

Auftragsbearbeitungsvertrag

Stand 15. Oktober 2026

zwischen

DATA Security AG

Wilenstrasse 42

CH-8832 Wilen b. Wollerau

(nachfolgend: "DATA Security AG" / "Auftragnehmerin" genannt)

und

Nutzer von DATA Security Software

(nachfolgend: "Auftraggeber" genannt)



Inhalt

Geltungsbereich der aktuellen Beauftragung	4
Betroffene Anwendungen des Auftraggebers	4
Schweizer Datenschutzprüfung der ausgewählten Produkte	6
DS Datenschutz+KI	6
DS MS365 / Compliance 365	6
DS Sign	6
DS Identity / DS KYC	6
Auslandbearbeitung und weitere Auftragsbearbeiter	7
Auftragsbearbeitung	8
1 Präambel	8
2 Definitionen, Begriffsbestimmungen	8
3 Dauer und Laufzeit des Auftrags	8
4 Kategorien von betroffenen Personen	9
5 Arten der Personendaten	9
6 Ort der Bearbeitung	9
7 Kontrollechte des Auftraggebers	10
8 Weisungsbefugnisse des Auftraggebers	11
9 Pflichten des Auftragnehmers	11
9.1 Bearbeitungspflichten	11
9.2 Duldungspflichten bei Kontrollen	12
9.3 Informationspflichten	12
9.4 Mitwirkungs- und Unterstützungspflichten	13
9.5 Organisationspflichten	13
10 Wahrung der Vertraulichkeit und sonstiger Geheimnisse	13
10.1 Allgemeine Vertraulichkeit	13
10.2 Anwaltsgeheimnis	14
11 Unterauftragsverhältnisse	15
12 Mitteilungspflichten bei Störungen und Datensicherheitsverletzung	15
13 Rechte der Betroffenen	16
14 Technische und organisatorische Massnahmen	16
15 Verfahren nach Beendigung des Auftrags	17
16 Vertragsdauer und Kündigung	18
17 Wirksamkeit der Vereinbarung	18
18 Haftung	18
19 Anwendbares Recht und Gerichtsstand	19
Anlage 1: Technische und organisatorische Massnahmen (TOM)	20
1 Zutrittskontrolle	20
2 Zugangskontrolle	21
3 Zugriffskontrolle	22
4 Weitergabekontrolle	24
5 Eingabekontrolle	25
6 Auftragskontrolle	26



7	Verfügbarkeitskontrolle	27
8	Trennungskontrolle (Trennungsgebot)	29
9	Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung	30
9.1	Massnahmen zum Datenschutzmanagement	30
9.2	Massnahmen zum Incident-Response-Management	31
10	Schweizer Rechtsrahmen und Geltung	32
Anlage 2 –	Verpflichtung zur Wahrung des Berufsgeheimnisses	33
1	Zweck und Anwendungsbereich	33
2	Berufsgruppen und gesetzlicher Schutz	33
3	Stellung der Auftragnehmerin und der eingesetzten Personen	34
4	Konkrete Verpflichtungen	34
5	Dauer, Rangfolge und Verhältnis zum Datenschutz	35



Geltungsbereich der aktuellen Beauftragung

Dieser Auftragsbearbeitungsvertrag gilt als Gesamtvertrag für sämtliche nachstehend aufgeführten Lösungen der DATA Security AG, soweit und solange der Auftraggeber sie im Rahmen der jeweiligen Beauftragung bezieht. Bezieht der Auftraggeber zu einem späteren Zeitpunkt eine weitere aufgeführte Lösung, gilt dieser Vertrag ohne Weiteres auch für diese; ein neuer Auftragsbearbeitungsvertrag ist nicht erforderlich.

Massgeblich ist der für die jeweils bezogene Lösung dokumentierte Funktions-, Personen- und Datenumfang. Die blossе Aufführung einer Lösung begründet keine Bearbeitung von Personendaten. Für jede Lösung gelten die nachstehend konkretisierten Voraussetzungen des Schweizer DSG und der DSV.

Betroffene Anwendungen des Auftraggebers

DS Datenschutz+KI	KI-Selbstcheck, strukturierte Fragen zu Verantwortlichkeiten, Risikobewertung, Datenverarbeitung, Rechtsgrundlagen und Schulungen; ausserdem CH-DSG-Fragenkatalog, Aufgabenliste, Verzeichnis der Verarbeitungstätigkeiten, Schulungsmodul, Siegelnachweis, TOM-Checklisten, Vorlagen, Risikoanalyse und Dokumentation von Datenschutzpannen. CH-Status: Bestandteil bei Bezug – Datenschutzprüfung und KI-Governance nach schweizerischem DSG; keine personenbezogene Bewertung. CH-DSG: Art. 5–9 DSG; bei Auslandsbekanntgabe zusätzlich Art. 16–17 DSG; besondere Moduldaten nur nach Prüfung und Freigabe.
DS MS365 / Compliance 365	Compliance-Bewertung für Microsoft 365, Prüfung von Lizenzbedarf, Tenant-, Teams-, Exchange-, SharePoint- und OneDrive-Konfiguration, MFA/RBAC/Verschlüsselung, automatische Aufgabenliste, M365-spezifische CH-DSG-Vorlagen, Schulungen für Mitarbeitende, Verarbeitungsbeispiele, ISO-27001-basierte Risikoanalyse und Datenschutzverletzungs-Reporting. CH-Status: Bestandteil bei Bezug – Erweiterte Tenant-Analysen nur nach freigegebenem Rollen-, Rechte-, Datenfeld- und Transferkonzept. CH-DSG: Art. 5–9 DSG; bei Auslandsbekanntgabe zusätzlich Art. 16–17 DSG; besondere Moduldaten nur nach Prüfung und Freigabe.
DS Sign	DS Sign ist eine eigenständige Lösung, mit der Kunden beliebige Dokumente elektronisch unterzeichnen und unterzeichnen lassen können –



	wahlweise mit einfacher, fortgeschrittener oder qualifizierter elektronischer Signatur. Die Nutzung ist sowohl separat als auch über die Schnittstelle in DS KYC möglich. Bearbeitet werden Identitäts- und Kontaktdaten der Nutzenden und der Unterzeichnenden, die vom Auftraggeber bereitgestellten Dokumentinhalte sowie die erforderlichen Signatur-, Status-, Zeitstempel- und Nachweisdaten; bei fortgeschrittenen und qualifizierten Signaturen zusätzlich die für die Identifizierung der Unterzeichnenden erforderlichen Daten. CH-Status: Bestandteil bei Bezug – separat oder über die Schnittstelle in DS KYC nutzbar; einfache, fortgeschrittene oder qualifizierte elektronische Signatur. CH-DSG: Art. 5–9 DSG; bei Auslandsbekanntgabe zusätzlich Art. 16–17 DSG; besondere Moduldaten nur nach Prüfung und Freigabe.
DS Identity	Identitätsprüfung natürlicher Personen als Bestandteil von KYC-Prozessen, namentlich Prüfung von Ausweisdokumenten und Videoidentifikation. DS Identity ist verfügbar, jedoch ausschliesslich im Zusammenspiel mit DS KYC nutzbar und nicht als eigenständige Lösung beziehbar. CH-Status: Verfügbar – ausschliesslich in Verbindung mit DS KYC. CH-DSG: Art. 5–9 DSG; bei Auslandsbekanntgabe zusätzlich Art. 16–17 DSG; besondere Moduldaten nur nach Prüfung und Freigabe.
DS KYC	Lösung zur Durchführung und Dokumentation von Sorgfaltspflichten bei der Prüfung von Kunden und Geschäftspartnern (KYC/KYB), insbesondere Identifizierung von Vertragspartnern, Feststellung wirtschaftlich berechtigter Personen, Abfragen von Unternehmens- und Registerinformationen, Abgleich mit Sanktions- und weiteren Prüflisten sowie Dokumentation der Prüfergebnisse; je nach Funktionsumfang in Verbindung mit DS Identity und DS Sign. CH-Status: Freigegeben seit 1. September 2026 – Bestandteil bei Bezug. CH-DSG: Art. 5–9 DSG; bei Auslandsbekanntgabe zusätzlich Art. 16–17 DSG; besondere Moduldaten nur nach Prüfung und Freigabe.



Schweizer Datenschutzprüfung der ausgewählten Produkte

Produkt- und Aktivierungsregel: Die Aufnahme in die Übersicht ist keine Erlaubnis, Personendaten zu bearbeiten. Es gelten ausschliesslich die vom Auftraggeber bezogenen, in der Beauftragung bezeichneten und durch eine dokumentierte Verarbeitungsspezifikation freigegebenen Funktionen.

Die DATA Security AG prüft vor Aktivierung je Produkt die Rolle nach Art. 5 lit. j (Verantwortlicher) bzw. k (Auftragsbearbeiter) und Art. 9 DSG, die vorgesehenen Personendaten, betroffenen Personen, Bearbeitungszwecke, Empfänger und Unterauftragsbearbeiter, Speicher- und Zugriffsstandorte, Aufbewahrungs- und Löschfristen sowie das Schutzniveau nach Art. 8 DSG und Art. 1–3 DSV.

DS|Datenschutz+KI

Der CH-DSG-Fragenkatalog, das Verzeichnis der Bearbeitungstätigkeiten, TOM-Checklisten, Datenschutzvorfall- und Risiko-Dokumentation sind auf das Schweizer Recht ausgerichtet. Im Grundumfang sind nur Organisations- und Nutzerinformationen vorgesehen. Für besonders schützenswerte Personendaten oder persönlichkeitsbezogenes Profiling ist eine separate Freigabe samt allfälliger DSFA nach Art. 22 DSG erforderlich.

DS|MS365 / Compliance 365

Erweiterte Analysen von Microsoft-365-Tenant-, Exchange-, Teams-, SharePoint- oder OneDrive-Konfigurationen können Metadaten und personenbezogene Inhalte oder Administrationszugriffe betreffen. Eine Aktivierung setzt ein produktbezogenes Rollen-, Rechte-, Datenfeld- und Transferkonzept sowie die Prüfung etwaiger Auslandsbekanntgaben nach Art. 16–17 DSG voraus.

DS|Sign

DS|Sign ermöglicht die Unterzeichnung beliebiger Dokumente durch interne und externe Unterzeichnende, separat oder über die Schnittstelle in DS|KYC. Signatur-, Identitäts-, Zeitstempel- und Nachweisdaten werden ausschliesslich zweckgebunden für den jeweiligen Signaturvorgang und dessen Nachweis bearbeitet. Die Dokumentinhalte bestimmt der Auftraggeber; enthalten sie besonders schützenswerte Personendaten oder Berufsgeheimnisse, gelten die Ziffern 5 und 10 der Auftragsbearbeitung sowie Anlage 2. Für fortgeschrittene und qualifizierte elektronische Signaturen sind die Anforderungen des ZertES und für die qualifizierte elektronische Signatur Art. 14 Abs. 2bis OR zu beachten. Wird hierfür ein Anbieter von Zertifizierungsdiensten beigezogen, ist dessen datenschutzrechtliche Rolle zu bestimmen und er, soweit er als Auftragsbearbeiter tätig ist, in der Liste der Unterauftragsbearbeiter auszuweisen.

DS|Identity / DS|KYC

DS|Identity ist ausschliesslich im Zusammenspiel mit DS|KYC verfügbar. Bearbeitet werden je nach Funktionsumfang Identifikations- und Ausweisdaten, Angaben zu wirtschaftlich berechtigten Personen, Unternehmens- und Registerinformationen sowie Listen- und Trefferinformationen. Der



produktive Einsatz erfordert eine dokumentierte Verarbeitungsspezifikation mit Bearbeitungszwecken, Datenfeldern sowie Speicher- und Löschfristen; es gelten die über den Link nach Ziffer 11 abrufbaren Unterauftragsbearbeiter. Werden bei der Identitätsprüfung biometrische Daten zur eindeutigen Identifizierung bearbeitet, handelt es sich um besonders schützenswerte Personendaten nach Art. 5 lit. c Ziff. 4 DSG; in diesem Fall ist eine Datenschutz-Folgenabschätzung nach Art. 22 DSG zu prüfen.

Auslandbearbeitung und weitere Auftragsbearbeiter

Für sämtliche Module sind Speicherorte, Backup-Standorte und Fernzugriffe unter Art. 16–17 DSG einschliesslich Anhang 1 DSV zu prüfen. Den Beizug von Unterauftragsbearbeitern (weiteren Auftragsbearbeitern) hat der Auftraggeber nach Art. 9 Abs. 3 DSG und Art. 7 DSV gemäss Ziffer 11 allgemein genehmigt. Weder die Bezeichnung EU/EWR noch der Sitz eines Cloud-Anbieters ersetzt die konkrete Beurteilung des Ziellands und der Zugriffskonstellation.



Auftragsbearbeitung

1 Präambel

DATA Security AG ist Anbieter von Lösungen im Bereich IT und Compliance. Für die Nutzung von DATA Security Lösungen und Inanspruchnahme von Dienstleistungen regeln die jeweilige Beauftragung sowie die AGB und der Verhaltenskodex der DATA Security AG die Rechte und Pflichten der Parteien. Ein separater Hauptvertrag besteht nicht. Mit diesem Vertrag sollen zusätzlich die Vorgaben des Bundesgesetzes über den Datenschutz (DSG) hinsichtlich Art. 9 DSG geregelt werden.

2 Definitionen, Begriffsbestimmungen

- a. Der Gegenstand des Auftrages ist in der jeweiligen Beauftragung beschrieben. Massgebend sind ausschliesslich die vom Auftraggeber bezogenen und freigegebenen Lösungen, Funktionen und Datenfelder; Produktbeschreibungen und Funktionslisten begründen keine zusätzliche Bearbeitungserlaubnis.
- b. Der Auftragnehmer bearbeitet Personendaten des Auftraggebers. Bei dem Vertragsgegenstand handelt es sich deshalb um eine Auftragsbearbeitung. Die Parteien sind sich darin einig, dass auf diesen Vertrag die Vorschriften des Bundesgesetzes über den Datenschutz (DSG), insbesondere die Vorschriften über die Datenbearbeitung im Auftrag, anzuwenden sind. Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Leistungen nach Massgabe des Art. 9 DSG ordnungsgemäss durchzuführen. Dieser Vertrag gilt nur, soweit der Auftragnehmer als Auftragsbearbeiter im Sinne von Art. 5 lit. k DSG tätig wird. Bearbeitungen, die der Auftragnehmer als Verantwortlicher vornimmt, namentlich Vertragsadministration, Rechnungsstellung, gesetzliche Aufbewahrung und eigene Rechtsverteidigung, fallen nicht unter diesen Vertrag.
- c. Im Sinne von Art. 9 DSG regelt dieser Vertrag die datenschutzrechtlichen Massnahmen und die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der datenschutzrechtlichen Anforderungen.

3 Dauer und Laufzeit des Auftrags

Die Dauer und Laufzeit dieses Vertrags richtet sich nach der Laufzeit der jeweiligen Beauftragung für die Nutzung von DATA Security Lösungen und Inanspruchnahme von Dienstleistungen.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 9 DSG abgeleiteten Pflichten stellt einen schweren Verstoß dar



4 Kategorien von betroffenen Personen

Die Datenbearbeitung betrifft folgende Kategorien von natürlichen Personen:

- Mitarbeitende und Familienangehörige
- Dienstleister und deren Mitarbeitende
- Geschäftspartner und deren Mitarbeitende
- Kunden/Mandanten und deren Geschäftspartner/Mitarbeitende
- Wirtschaftlich berechtigte Personen, Organe und Vertretungsberechtigte von Kunden und Geschäftspartnern (DS|KYC, DS|Identity)
- Unterzeichnende von Dokumenten (DS|Sign)
- Ggf. andere Personen

5 Arten der Personendaten

Welche Personendaten im Rahmen dieses Vertrags bearbeitet werden, richtet sich nach den beauftragten Modulen und deren Nutzung durch den Auftraggeber. Massgebend ist die Beschreibung der Datenarten im Verzeichnis der Bearbeitungstätigkeiten. Freitexte und Uploadfelder erweitern die Freigabe nicht; werden Daten ausserhalb der Freigabe übermittelt, beschränkt der Auftragnehmer den Zugriff und stimmt Löschung oder Rückgabe mit dem Auftraggeber ab. Betroffen sein können unter anderem folgende Arten von Personendaten:

- Stammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Kundenhistorien
- Vertragsdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Identifikations- und Ausweisdaten, Angaben zu wirtschaftlich berechtigten Personen sowie Register-, Listen- und Trefferinformationen (DS|KYC, DS|Identity)
- Signatur-, Zeitstempel- und Nachweisdaten (DS|Sign)
- Besonders schützenswerte Personendaten (Art. 5 lit. c DSGVO) und Daten, die einem Berufsgeheimnis unterliegen, nur soweit das beauftragte Modul dies vorsieht und die Beauftragung sie freigibt

6 Ort der Bearbeitung

Die Datenbearbeitung, einschliesslich Hosting, Backup, Administration, Support und Fernzugriffen, findet ausschliesslich auf dem Gebiet der Schweiz oder innerhalb der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes statt.



Eine Bearbeitung in anderen Staaten ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit der Bundesrat für den Zielstaat einen angemessenen Schutz festgestellt hat (Art. 16 Abs. 1 DSG i.V.m. Anhang 1 DSV), geeignete Garantien nach Art. 16 Abs. 2 DSG bestehen oder ausnahmsweise die Voraussetzungen von Art. 17 DSG erfüllt und dokumentiert sind. Ausserdem ist bei einem Datentransfer ins Ausland nach Art. 19 DSG das Zielland stets zu benennen.

Den Nachweis für das Bestehen der Garantien und eines angemessenen Schutzniveaus führt der Auftragnehmer. Zertifizierungen nach Art. 13 DSG können ergänzende Nachweise zur Datenschutzorganisation liefern; sie ersetzen weder die Prüfung der Voraussetzungen nach Art. 16 und 17 DSG noch die vertraglich vereinbarten Garantien. Der Auftragnehmer verpflichtet sich, die Einhaltung der Garantien und eines angemessenen Schutzniveaus sicherzustellen. Der Auftraggeber behält sich vor, das Vorliegen der Garantien und die Einhaltung eines angemessenen Schutzniveaus im Rahmen seiner Audit- und Kontrollrechte jederzeit zu überprüfen. Standarddatenschutzklauseln werden, soweit erforderlich, an das Schweizer Recht angepasst und um risikoadäquate Zusatzmassnahmen ergänzt. Auskunftersuchen ausländischer Behörden teilt der Auftragnehmer dem Auftraggeber, soweit rechtlich zulässig, unverzüglich mit.

7 Kontrollechte des Auftraggebers

Der Auftraggeber ist allein verantwortlich für die Beurteilung der Zulässigkeit der Bearbeitung der Personendaten sowie für die Ausführung der Rechte der Betroffenen. Bei einer Datenbearbeitung im Auftrag arbeitet der Auftraggeber gem. Art. 9 DSG nur mit Auftragsbearbeitern zusammen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen zur Erfüllung der Anforderungen der DSG eingerichtet sind. Dazu gehört auch die Prüfung, ob gesetzliche oder vertragliche Geheimhaltungspflichten, namentlich Berufsgeheimnisse, der Übertragung der Bearbeitung entgegenstehen (Art. 9 Abs. 1 lit. b DSG).

Der Auftraggeber ist danach verpflichtet und befugt, vor Beginn der Datenbearbeitung und nach seinem Ermessen auch wiederholt nach vorheriger Abstimmung während der üblichen Geschäftszeiten im erforderlichen Umfang die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere der vom Auftragnehmer getroffenen technischen und organisatorischen Massnahmen, zu kontrollieren.

Der Auftraggeber ist befugt hierzu, schriftliche Auskünfte und die Vorlage von Nachweisen über die eingerichteten Datenschutzmassnahmen sowie über die Art und Weise ihrer technischen und organisatorischen Umsetzung zu verlangen, das Grundstück und die Betriebsstätten des Auftragnehmers zu betreten, nach seinem Ermessen Prüfungen und Besichtigungen vorzunehmen und im erforderlichen Umfang in bearbeitungsrelevante Unterlagen, Bearbeitungs- und Ablaufprotokolle, Systeme und gespeicherte Daten und in Regelungen, Richtlinien und Handbücher zur Regelung der beauftragten Datenbearbeitung einzusehen.



Hierzu gehören auch Nachweise über die Verpflichtung der Mitarbeitenden auf die Wahrung der Vertraulichkeit und technische und organisatorische Konzepte, z.B. Datenschutzhandbuch, einschlägige Verfahrensanweisungen und auch Verträge mit Unterauftragnehmern.

Die gleichen Rechte besitzen auch Beauftragte des Auftraggebers, z.B. Gutachter oder Sachverständige, soweit sie besonders zur Verschwiegenheit verpflichtet sind oder strafbewehrten berufsständischen Schweigepflichten unterliegen.

Die Rechte des Auftraggebers bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus diesem Vertrag, mindestens jedoch solange der Auftraggeber Personendaten aus den beauftragten Bearbeitungen speichert.

Die Prüfung erfolgt nach vorheriger Anmeldung. In Fällen, in denen Bearbeitungsprobleme bestehen, meldepflichtige Vorfälle aufgetreten sind oder aufsichtsrechtliche Massnahmen anstehen oder eingeleitet worden sind, kann die Prüfung ausnahmsweise auch ohne vorherige Anmeldung erfolgen.

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8 Weisungsbefugnisse des Auftraggebers

Der Auftragnehmer bearbeitet die Daten ausschliesslich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Weisungen erfolgen in Textform, beispielsweise per E-Mail. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen anwendbare Datenschutzvorschriften verstösst, informiert er den Auftraggeber unverzüglich. Er ist berechtigt, deren Ausführung bis zur Klärung auszusetzen. Rechtswidrige Weisungen werden nicht ausgeführt.

9 Pflichten des Auftragnehmers

9.1 Bearbeitungspflichten

Der Auftragnehmer führt den Auftrag ausschliesslich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Ohne separate dokumentierte Vereinbarung nutzt er die Daten insbesondere nicht für Produktentwicklung, das Training von KI-Modellen, Profiling, Marketing, Benchmarking oder Datenanreicherung.

Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Auftraggebers nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrages oder zur Gewährleistung einer ordnungsgemässen Datenbearbeitung erforderlich ist oder eine gesetzliche oder sonstige Aufbewahrungspflicht besteht. Eventuell hergestellte Auszüge, Kopien oder Duplikate sind nach Abschluss der



Bearbeitung oder Nutzung vom Auftragnehmer unverzüglich sicher zu löschen bzw. datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenbearbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeitende des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.

Der Auftragnehmer verpflichtet sich, nur solche Software, Daten oder Datenträger einzusetzen, die zuverlässig auf Freiheit von schädlicher Software geprüft sind, um ein Einschleusen von Viren etc. zu vermeiden.

9.2 Duldungspflichten bei Kontrollen

Der Auftragnehmer verpflichtet sich, in Prüfungen durch den Auftraggeber die Einhaltung der getroffenen technischen und organisatorischen Massnahmen nachzuweisen, Auskünfte zu erteilen und die entsprechenden Unterlagen vorzulegen bzw. Einsicht in die erforderlichen Unterlagen und Systeme zu gewähren und nach vorheriger Abstimmung entsprechende Prüfungen des Auftraggebers vor Ort zu dulden und zu unterstützen. Er verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.

Der Nachweis angemessener technischer und organisatorischer Massnahmen kann auch durch Vorlage von Testaten oder Zertifikaten oder durch eine Zertifizierung bzw. ein Datenschutzaudit einer unabhängigen Einrichtung bzw. eines autorisierten Sachverständigen geführt werden. Unabhängig von diesen Nachweisen ist der Auftragnehmer verpflichtet, Kontrollen durch den Auftraggeber gem. §7 dieser Vereinbarung zu dulden.

9.3 Informationspflichten

Der Auftragnehmer ist verpflichtet, wesentliche Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmässigkeit der Durchführung der Auftragsleistungen herabsetzen, unaufgefordert dem Auftraggeber zu melden. Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten für den Datenschutz und über eventuelle Massnahmen und Auflagen zum Schutz der Personendaten. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Er informiert den Auftraggeber unverzüglich über das Erlöschen oder den Widerruf von Zertifikaten oder von Massnahmen gem. Art. 13 DSG. Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten und Änderungen in der Person des betrieblichen Datenschutzberaters oder, wenn keine Bestellpflicht besteht, den Namen und die Kontaktdaten der sonstigen zuständigen Stelle namentlich die Geschäftsführung.



9.4 Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 9 DSG, die für das Verzeichnis von Bearbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

9.5 Organisationspflichten

Der Auftragnehmer verpflichtet sich zur Einrichtung von Massnahmen und Dokumentationen, die eine Kontrolle und Nachvollziehbarkeit aller mit der Auftragsbearbeitung zusammenhängenden Tätigkeiten und Bearbeitungsprozesse im Sinne einer Auftragskontrolle und der Ordnungsmässigkeit der Datenbearbeitung ermöglichen.

Datenschutzvorfälle und sonstige sicherheitsrelevante Störungen der Bearbeitung sind einschliesslich ihrer Auswirkungen und der ergriffenen Abhilfemassnahmen zu dokumentieren und dem Auftraggeber zu melden. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen. Wird die Bearbeitung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, ist der Auftraggeber darüber zu informieren. Der Auftragnehmer verpflichtet sich, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Bearbeitung im gleichen Masse zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung vom Ort des Auftragnehmers aus dem Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.

10 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

10.1 Allgemeine Vertraulichkeit

- (1) Personen- und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der Personendaten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrages bekannt werdenden Personendaten und sonstige unternehmensinterne Umstände, Daten und Informationen (Betriebsgeheimnisse) vertraulich zu behandeln sowie die im Rahmen dieses Vertrages tätig werdenden Mitarbeitenden auch über die Beendigung des Beschäftigungsverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Bearbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.



- (2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er für die Durchführung der Arbeiten nur eigenes Personal sowie nach Ziffer 11 beigezogene Unterauftragsbearbeiter einsetzt und die mit der Auftragsdurchführung beschäftigten Mitarbeitenden mit den für sie massgebenden Bestimmungen des Datenschutzes vertraut macht und einer regelmässigen Schulung unterzieht.
- (3) Der Auftragnehmer verpflichtet sich zur Beachtung aller sonstigen Geheimnisse, soweit diese für die Bearbeitung einschlägig sind, wie des Fernmeldegeheimnisses und sonstiger Berufsgeheimnisse sowie zur Verpflichtung und Belehrung der Beschäftigten zur Sicherstellung der Wahrung dieser Geheimnisse.
- (4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über administrative Zugangsdaten und Datensicherheitsmassnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen. Von den ihm eingeräumten Zugriffsrechten darf der Auftragnehmer nur in dem Umfang Gebrauch machen, der für die Durchführung der Datenbearbeitung erforderlich ist. Die Verpflichtung zur Wahrung der Vertraulichkeit und der sonstigen Geheimnisse gilt auch über die Beendigung dieses Vertrages hinaus.

10.2 Anwaltsgeheimnis

Soweit der Auftraggeber oder für ihn tätige Personen dem anwaltlichen Berufsgeheimnis (Anwaltsgeheimnis) nach Art. 13 des Bundesgesetzes über die Freizügigkeit der Anwältinnen und Anwälte (BGFA) und Art. 321 StGB unterliegen, behandelt der Auftragnehmer sämtliche ihm im Rahmen dieses Vertrags bekannt werdenden oder zugänglichen Mandatsinformationen, namentlich Informationen über Mandate, Klientinnen und Klienten und deren Angelegenheiten sowie mandatsbezogene Dokumente und Korrespondenz, als Geheimnisse und schützt sie vor unbefugter Kenntnisnahme und Offenbarung. Er bearbeitet sie ausschliesslich, soweit dies für die vereinbarten Leistungen erforderlich ist, und beschränkt den Zugriff nach dem Need-to-know-Prinzip.

Diese Pflichten gelten auch für alle Mitarbeitenden sowie für Unterauftragsbearbeiter und deren Mitarbeitende, die Zugriff auf solche Informationen haben oder erhalten können; der Auftragnehmer verpflichtet diese Personen vor ihrem Einsatz nachweisbar zur Wahrung des Anwaltsgeheimnisses und weist sie auf die Folgen einer unbefugten Offenbarung nach Art. 321 StGB und Art. 62 DSG hin.

Die Einzelheiten, auch zu weiteren Berufsgeheimnissen, regelt Anlage 2, die Bestandteil dieses Vertrags ist. Die Verantwortung des Auftraggebers, die Zulässigkeit des Beizugs des Auftragnehmers nach Art. 9 Abs. 1 lit. b DSG und dem anwendbaren Berufsrecht zu beurteilen, bleibt unberührt.



11 Unterauftragsverhältnisse

Der Auftraggeber erteilt dem Auftragnehmer mit Vertragsabschluss die allgemeine Genehmigung, weitere Auftragsbearbeiter zur Erbringung der vereinbarten Leistungen beizuziehen.

Die jeweils eingesetzten Unterauftragsbearbeiter sind mit ihren Leistungen und Bearbeitungsorten in der aktuellen [Liste der Unterauftragsbearbeiter](#) aufgeführt. Diese Liste ist Bestandteil dieser Vereinbarung und wird vom Auftragnehmer aktuell gehalten. Eine Aktualisierung erfordert keine Neuausstellung dieses Vertrags.

Der Auftragnehmer verpflichtet die Unterauftragsbearbeiter vertraglich zur Einhaltung gleichwertiger Datenschutzpflichten, wie sie ihm selbst aus dieser Vereinbarung obliegen, und stellt angemessene Datenschutz- und Datensicherheitsmassnahmen sicher. Er bleibt gegenüber dem Auftraggeber für die Einhaltung dieser Pflichten durch die Unterauftragsbearbeiter verantwortlich.

Der Auftragnehmer ist berechtigt, Unterauftragsbearbeiter ohne erneute ausdrückliche Zustimmung des Auftraggebers hinzuzuziehen oder zu ersetzen, sofern ein mindestens gleichwertiges Datenschutzniveau gewährleistet bleibt. Die gesetzlichen Rechte und Pflichten der Parteien bleiben unberührt.

12 Mitteilungspflichten bei Störungen und Datensicherheitsverletzung

- (1) Bei einer Störung der Bearbeitung oder einer Datensicherheitsverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Massnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und für den Auftraggeber ein.
- (2) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über Verstösse gegen Vorschriften zum Schutz der Personendaten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz von Personendaten oder andere Unregelmässigkeiten beim Umgang mit Personendaten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können.
- (3) Zu den Datensicherheitsverstössen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne dieses Vertrages.
- (4) Die Meldung an den Auftraggeber umfasst alle Informationen, die für den Auftraggeber erforderlich sind, um den Vorfall nach Art. 24 DSG beurteilen zu



können und ggfs. die Betroffenen zu informieren. Die Meldung an den Auftraggeber umfasst insbesondere Angaben zur Art des Vorfalls und der Verletzung der Sicherheit von Personendaten, eine Beschreibung der wahrscheinlichen Risiken für die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen und eine Beschreibung der bereits eingeleiteten Massnahmen zur Behebung bzw. Reduzierung eines möglichen Schadens oder sonstiger Risiken für die Betroffenen und den Auftraggeber. Noch nicht verfügbare Angaben liefert der Auftragnehmer unverzüglich nach.

- (5) Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 24 DSGVO und unternimmt alle in seinen Verantwortungsbereich fallenden Massnahmen zur Minderung nachteiliger Folgen für die Betroffenen sowie zur Aufklärung des Vorfalls und dessen Folgen. Dies gilt auch nach Beendigung des Vertragsverhältnisses. Die Meldung an den EDÖB und die Information betroffener Personen obliegen dem Auftraggeber (Art. 24 Abs. 1 und 4 DSGVO).

13 Rechte der Betroffenen

- (1) Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zu-ständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen, namentlich bei Auskunft (Art. 25 DSGVO), Datenherausgabe oder -übertragung (Art. 28 DSGVO) sowie Berichtigung und Löschung (Art. 32 DSGVO).
- (2) Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarten Kontaktpersonen erteilt werden.

14 Technische und organisatorische Massnahmen

Der Auftragnehmer sichert ein dem Risiko für die Rechte und Freiheiten der Betroffenen adäquates Schutzniveau der Personendaten zu. Zu diesem Zweck verpflichtet sich der Auftragnehmer, seine innerbetriebliche Organisation und die erforderlichen technischen und organisatorischen Massnahmen unter Berücksichtigung des jeweiligen Stands der Technik, der Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Bearbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen so zu gestalten und laufend zu aktualisieren, dass diese den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten.

Die technischen und organisatorischen Massnahmen umfassen insbesondere:



- Die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Bearbeitung der Daten
- Die rasche Wiederherstellung der Verfügbarkeit der Personendaten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls
- Die Einführung und das Vorhalten von Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung.

Der Auftragnehmer sichert die Einhaltung der genannten Massnahmen und Regelungen zu. Diese Massnahmen gelten als vereinbart. Die Einzelheiten der technischen und organisatorischen Massnahmen sind in **Anlage 1** beschrieben, die integraler Bestandteil dieses Vertrages ist.

Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber vorab mitzuteilen.

Der Auftragnehmer kann die Eignung der nach Art. 8 DSG in Verbindung mit Art. 1–3 DSV zu treffenden technisch-organisatorischen Massnahmen durch die Einhaltung genehmigter Verhaltensregeln oder eines Datenschutzsiegels oder Prüfzeichen nachweisen, dass für die vertragsgegenständlichen Bearbeitungsverfahren und Orte erteilt und für die unter diese Vereinbarung fallenden Bearbeitungsverfahren relevant ist. Der Auftragnehmer hat Veränderungen am Zertifikat oder dessen Ablauf dem Auftraggeber unverzüglich mitzuteilen. Die Kontroll- und Auditrechte des Auftraggebers bleiben unberührt.

15 Verfahren nach Beendigung des Auftrags

- (1) Nach Abschluss der Bearbeitung, spätestens nach Beendigung dieses Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Bearbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten Personen- oder sonstige vertrauliche Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers diesem in einem gängigen, nutzbaren Format auszuhändigen oder datenschutzgerecht zu vernichten oder sicher zu löschen. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen. Diese Verpflichtung gilt in gleichem Masse auch für eventuell beauftragte Unterauftragnehmer. Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismässig hohen Aufwand verursachen würde, sowie Kopien, die zum Nachweis der Ordnungsmässigkeit der Datenbearbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.



- (2) Für diese Daten ist die Bearbeitung einzuschränken. Die Daten dürfen durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden und sind nach Ablauf der Aufbewahrungsfrist unverzüglich sicher zu löschen. Der Auftraggeber ist über Art und Umfang dieser gespeicherten Daten zu unterrichten. Der Auftragnehmer kann diese Daten zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.
- (3) Der Auftragnehmer hat dem Auftraggeber nach Beendigung dieses Vertrages die sichere Löschung bzw. die sichere Vernichtung aller in seinem Besitz befindlichen Unterlagen schriftlich zu bestätigen. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Datensicherungen werden im Rahmen des dokumentierten Sicherungszyklus gelöscht.

16 Vertragsdauer und Kündigung

Die Vertragsdauer richtet sich nach Ziffer 3; für die ordentliche Kündigung gelten die AGB der DATA Security AG.

Wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, kann der Auftraggeber den Vertrag jederzeit ohne Einhaltung einer Frist kündigen. Gleiches gilt, wenn der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

Eine Kündigung des Vertrags kann nur schriftlich erfolgen.

17 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Bei datenschutzrechtlichen Widersprüchen gilt folgende Rangfolge:

- (1) Zwingendes Schweizer Datenschutzrecht
- (2) Dieser Auftragsbearbeitungsvertrag einschliesslich Anlage 2 (Berufsgeheimnis); strengere Geheimhaltungsvorkehrungen der Anlage 2 gehen nach deren Ziffer 5 vor
- (3) Anlage 1 TOM
- (4) Individuell genehmigte Verarbeitungsspezifikation und die über den Link nach Ziffer 11 abrufbare Liste der Unterauftragsbearbeiter, soweit diese den Schutz nicht absenken
- (5) Beauftragung und AGB

18 Haftung

Für die Haftung gelten die Regelungen den einschlägigen Bestimmungen des Schweizer Rechts; die Art. 60 ff. DSG enthalten Strafbestimmungen und bilden keine allgemeine zivilrechtliche Haftungsregel.

Zusätzlich gelten für die Haftung die Regelungen der AGB der DATA Security AG.



19 Anwendbares Recht und Gerichtsstand

Es gilt das Recht der Schweiz unter Ausschluss des UN-Kaufrechts.

Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevante Streitigkeiten ist der Sitz der DATA Security AG, Wilen b. Wollerau.

Gesetzliche Regelungen über ausschliessliche Zuständigkeiten bleiben hiervon unberührt.



Anlage 1: Technische und organisatorische Massnahmen (TOM)

1 Zutrittskontrolle

Massnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Massnahmen
• Geschäfts- und Büroräume sind mit einem manuellen Schliesssystem gesichert • Besonders schutzbedürftige Bereiche sind mit Sicherheitsschlössern ausgestattet • Der Zugang wird über eine Klingel- oder Gegensprechanlage kontrolliert • Server-, Technik- und Archivräume werden, soweit vorhanden, verschlossen gehalten • Unterlagen und Datenträger mit Personendaten werden in abschliessbaren Schränken oder Rollcontainern aufbewahrt • Der Zugang zu besonders schutzbedürftigen Bereichen wird, soweit erforderlich, mechanisch oder elektronisch beschränkt
Organisatorische Massnahmen
• Eine Schlüsselregelung einschliesslich Ausgabe, Rückgabe und Verlustmeldung ist dokumentiert und wird angewendet • Eine Schlüsselliste oder sonstige Zugangsberechtigungsliste wird geführt • Schlüssel- und Zutrittsberechtigungen sind auf berechtigte Personen beschränkt • Die bestehenden Zutrittsberechtigungen werden regelmässig überprüft • Besuchende werden über Empfang, Anmeldung oder eine zuständige Ansprechperson gesteuert • Besuchende werden in nicht öffentlich zugänglichen Bereichen von Mitarbeitenden begleitet • Unbekannte Personen werden in nicht öffentlich zugänglichen Bereichen angesprochen • Die Bereiche, die externe Dienstleister wie Reinigungs-, Wartungs- oder Handwerkspersonal betreten dürfen, sind begrenzt • Externe Dienstleister mit Zutritt zu Geschäftsräumen oder schutzbedürftigen Bereichen werden sorgfältig ausgewählt • Externe Dienstleister werden auf Vertraulichkeit verpflichtet, soweit sie Zugang zu Bereichen mit Personendaten erhalten können • Türen zu nicht öffentlich zugänglichen Bereichen werden ausserhalb der Geschäftszeiten verschlossen



Organisatorische Massnahmen

- Interne Verantwortlichkeiten für die Kontrolle von Zutritt, Schlüsselverwaltung und Besucherregelungen sind festgelegt

2 Zugangskontrolle

Massnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten verwendet werden können.

Technische Massnahmen

- Die Authentifizierung erfolgt mittels individueller Benutzerkennung und Passwort
- Administrative Zugriffe, Cloud-Dienste und Remote-Zugriffe sind, soweit angemessen, durch Mehr-Faktor-Authentifizierung geschützt
- Interne Systeme und Netzwerke sind durch eine Firewall geschützt
- Auf Servern ist Endpoint Protection bzw. Malware-Schutz installiert
- Auf Clients ist Endpoint Protection bzw. Malware-Schutz installiert
- Remote-Zugriffe erfolgen über VPN
- Mobile Endgeräte wie Notebooks, Tablets und Smartphones sind verschlüsselt
- Externe Datenträger werden verschlüsselt, soweit Personendaten darauf gespeichert werden
- Bildschirme werden nach einer definierten Inaktivitätszeit automatisch gesperrt
- Mitarbeitende können den Bildschirm manuell sperren
- Benutzer und Identitäten werden, soweit vorhanden, zentral verwaltet
- Benutzerkonten werden nach Austritt oder Rollenwechsel technisch gesperrt oder deaktiviert
- Sicherheitsrelevante Anmeldeereignisse, insbesondere fehlgeschlagene Login-Versuche, werden protokolliert
- Benutzerkonten werden nach mehrfach fehlgeschlagenen Anmeldeversuchen gesperrt
- Sicherheitsupdates und Patches für Betriebssysteme, Anwendungen und Sicherheitssoftware werden regelmässig eingespielt

Organisatorische Massnahmen

- Benutzerberechtigungen werden nach dem Need-to-know- und Least-Privilege-Prinzip verwaltet
- Rollenbasierte Benutzerprofile wurden erstellt und werden gepflegt
- Ein Prozess zur Einrichtung, Änderung und Deaktivierung von Benutzerkonten ist dokumentiert und wird angewendet
- Bestehende Benutzerkonten und Zugangsberechtigungen werden regelmässig überprüft



Organisatorische Massnahmen

- Benutzerkonten werden zentral mit sicherem Initialpasswort oder über ein geregeltes Passwort-Reset-Verfahren vergeben
- Eine Richtlinie zur sicheren Passwortverwendung ist erlassen und wird angewendet
- Vorgaben zum Einsatz von Mehr-Faktor-Authentifizierung, insbesondere bei Remote-, Cloud- und Administrationszugriffen, sind festgelegt
- Eine allgemeine Richtlinie zu Datenschutz und Informationssicherheit ist erlassen
- Eine Mobile Device Policy regelt den sicheren Einsatz mobiler Endgeräte
- Die Nutzung privater Geräte ist geregelt, soweit diese zugelassen sind
- Clean-Desk- und Clear-Screen-Regelungen sind festgelegt und werden angewendet
- Mitarbeitende sind zur manuellen Bildschirmsperre angeleitet
- Mitarbeitende werden zum sicheren Umgang mit Zugangsdaten sensibilisiert
- Verantwortlichkeiten für Benutzerverwaltung, Passwort-Reset und Rechtevergabe sind festgelegt
- Änderungen an Benutzerkonten und Zugangsrechten werden nachvollziehbar dokumentiert

3 Zugriffskontrolle

Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und die personenbezogenen Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt verwendet werden können.

Technische Massnahmen

- Zugriffe innerhalb der eingesetzten Anwendungen und Systeme werden rollen- und berechtigungsbasiert kontrolliert
- Es werden individuelle Benutzerkonten anstelle gemeinsamer Sammelkonten vergeben
- Zugriffe werden nach dem Need-to-know- und Least-Privilege-Prinzip technisch beschränkt
- Benutzer-, Administratoren- und Servicekonten sind getrennt
- Administrative Berechtigungen sind auf hierfür autorisierte Personen beschränkt
- Zugriffe auf Dateiablagen, Datenbanken, Fachanwendungen und Cloud-Dienste sind technisch beschränkt
- Daten werden innerhalb der eingesetzten Systeme, soweit erforderlich, nach Mandanten, Kunden oder Projekten getrennt
- Relevante Zugriffe auf Anwendungen und Datenbestände werden protokolliert



Technische Massnahmen

- Eingabe, Änderung, Export und Löschung von Personendaten werden protokolliert, soweit technisch möglich und angemessen
- Export-, Download-, Kopier- und Druckfunktionen werden, soweit erforderlich, technisch beschränkt
- Datenbestände, Datenträger und mobile Endgeräte werden verschlüsselt, soweit Personendaten betroffen sind
- Sitzungen werden nach einer definierten Inaktivitätszeit automatisch gesperrt
- Rechte werden standardisiert über Berechtigungsgruppen vergeben
- Aktive Benutzerkonten und Berechtigungen werden regelmässig technisch überprüft
- Nicht mehr benötigte Benutzerkonten werden technisch deaktiviert oder gesperrt

Organisatorische Massnahmen

- Ein Berechtigungskonzept für Systeme, Anwendungen und Datenbestände ist dokumentiert und wird angewendet
- Zugriffsrechte werden nach dem Need-to-know- und Least-Privilege-Prinzip vergeben
- Rollenbasierte Berechtigungsprofile sind festgelegt
- Einrichtung, Änderung und Entzug von Zugriffsrechten durchlaufen einen Genehmigungsprozess
- Bestehende Zugriffsrechte und Benutzerkonten werden regelmässig überprüft
- Zugriffsrechte werden bei Rollenwechsel, Aufgabenänderung oder Austritt zeitnah angepasst oder entzogen
- Rechte werden durch hierfür benannte Systemadministratoren oder verantwortliche Stellen verwaltet
- Die Anzahl administrativer Berechtigungen ist auf das erforderliche Mass beschränkt
- Vergabe, Änderung und Entziehung von Zugriffsrechten werden dokumentiert
- Fachliche Freigabe und technische Rechtevergabe sind getrennt, soweit organisatorisch möglich
- Der Umgang mit Administratorenrechten und privilegierten Konten ist geregelt
- Mitarbeitende werden zum zulässigen Zugriff auf Personendaten sensibilisiert
- Zugriffsprotokolle werden regelmässig kontrolliert, soweit erforderlich und angemessen
- Eskalationswege bei unberechtigten Zugriffen oder auffälligen Zugriffsmustern sind festgelegt



4 Weitergabekontrolle

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

Technische Massnahmen
• E-Mails mit Personendaten werden, soweit erforderlich, verschlüsselt übermittelt • Personendaten werden über verschlüsselte Verbindungen bereitgestellt, insbesondere HTTPS, SFTP oder vergleichbare sichere Übertragungswege • Remote-Zugriffe und standortübergreifende Verbindungen erfolgen über VPN • Mobile Datenträger und Speichermedien werden verschlüsselt • Dateien und Archive werden bei elektronischer Übermittlung, soweit erforderlich, mit Passwort geschützt oder verschlüsselt • Zugangsdaten und verschlüsselte Inhalte werden getrennt über unterschiedliche Kommunikationskanäle übermittelt • Export-, Download- und Weiterleitungsfunktionen werden, soweit erforderlich, technisch beschränkt • Relevante Datenübermittlungen, Abrufe, Downloads und Exporte werden protokolliert • Zugriffe auf bereitgestellte Übermittlungsplattformen oder Datenaustauschbereiche werden protokolliert • Soweit vorhanden, werden sichere Dateiübertragungs- oder Kundenportale eingesetzt • Download-Links und Freigaben werden zeitlich begrenzt • Der Zugriff auf bereitgestellte Daten wird durch individuelle Berechtigungen beschränkt • Übermittelte Daten werden, soweit erforderlich, durch geeignete Integritätsmechanismen vor Veränderung geschützt • Bereitgestellte Daten werden nach Ablauf des Übermittlungszwecks sicher gelöscht oder gesperrt

Organisatorische Massnahmen
• Verbindliche Vorgaben zur zulässigen Übermittlung von Personendaten sind erlassen • Zulässige Kommunikations- und Übertragungswege sind für unterschiedliche Datenkategorien festgelegt • Vor jeder Datenübermittlung werden Empfänger, Zweck, Berechtigung und Rechtsgrundlage geprüft



Organisatorische Massnahmen

- Ein Empfänger- und Berechtigungskonzept ist dokumentiert und wird angewendet
- Es ist festgelegt, welche internen oder externen Stellen Personendaten erhalten dürfen
- Besonders sensible, umfangreiche oder risikobehaftete Datenübermittlungen erfolgen, soweit angemessen, nach dem Vier-Augen-Prinzip
- Mitarbeitende werden zum sicheren Datentransfer geschult und sensibilisiert
- Zur Vermeidung von Fehlversand werden insbesondere Empfängeradresse, Anhänge und Verteilerlisten vor dem Versand geprüft
- Der Versand von Personendaten per E-Mail ist einschliesslich Verschlüsselung und Passwortübermittlung geregelt
- Der Transport physischer Datenträger und Papierunterlagen mit Personendaten ist geregelt
- Relevante Datenübermittlungen werden nachvollziehbar dokumentiert
- Verantwortlichkeiten für Freigabe, Durchführung und Kontrolle von Datenübermittlungen sind festgelegt
- Bestehende Empfänger, Verteiler und Datenfreigaben werden regelmässig überprüft
- Nicht mehr benötigte Freigaben und Austauschbereiche werden beendet oder gelöscht
- Bei Fehlversand, unzulässiger Übermittlung oder Verlust von Datenträgern wird ein festgelegtes Eskalations- und Meldeverfahren angewendet

5 Eingabekontrolle

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

Technische Massnahmen

- Die Eingabe von Personendaten wird technisch protokolliert
- Die Änderung von Personendaten wird technisch protokolliert
- Die Löschung von Personendaten wird technisch protokolliert
- Der jeweilige Zeitpunkt der Eingabe, Änderung oder Löschung wird protokolliert
- Das individuelle Benutzerkonto, über das die Eingabe, Änderung oder Löschung erfolgt ist, wird protokolliert
- Es werden individuelle Benutzerkonten anstelle gemeinsam genutzter Sammelkonten verwendet
- Protokolldaten sind vor unbefugter Veränderung oder Löschung geschützt
- Der Zugriff auf Protokolldaten ist auf berechtigte Personen beschränkt
- Administrative Eingriffe in Personendatenbestände werden protokolliert



Technische Massnahmen
• Relevante Protokolldaten können, soweit erforderlich, technisch ausgewertet werden • Auffällige Eingaben, Änderungen oder Löschungen lösen, soweit angemessen, automatisierte Hinweise oder Alarmierungen aus • Für Protokolldaten sind, soweit systemseitig möglich, technische Aufbewahrungsfristen festgelegt

Organisatorische Massnahmen
• Eine Übersicht darüber, mit welchen Programmen Personendaten eingegeben, geändert oder gelöscht werden können, wird geführt • Es ist festgelegt, welche Rollen oder Personen zur Eingabe, Änderung oder Löschung von Personendaten berechtigt sind • Eingaben, Änderungen und Löschungen sind über individuelle Benutzerkonten nachvollziehbar • Vergabe, Änderung und Entziehung von Berechtigungen für eingabe- und änderungsrelevante Systeme sind geregelt • Zuständigkeiten für Löschungen von Personendaten sind klar festgelegt • Vorgaben zur Durchführung und Freigabe von Löschungen sind dokumentiert und werden angewendet • Relevante Protokolle werden regelmässig oder anlassbezogen kontrolliert, soweit erforderlich und angemessen • Verantwortlichkeiten für die Kontrolle von Protokolldaten sind festgelegt • Festgestellte Auffälligkeiten bei Eingaben, Änderungen oder Löschungen werden dokumentiert • Bei unberechtigten oder auffälligen Eingaben, Änderungen oder Löschungen wird ein festgelegtes Eskalationsverfahren angewendet • Mitarbeitende werden zur Nutzung individueller Benutzerkonten und zur Nachvollziehbarkeit von Verarbeitungsvorgängen geschult und sensibilisiert

6 Auftragskontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können.

Technische Massnahmen
• Zugriffe von Unterauftragsverarbeitern werden rollen- und berechtigungsbasiert beschränkt • Relevante Zugriffe, Änderungen, Exporte und Löschungen werden protokolliert • Kundendaten werden durch Mandanten-, Datenbank- oder Systemtrennung technisch getrennt



Technische Massnahmen
• Systeme werden entsprechend den dokumentierten Weisungen des Kunden konfiguriert • Export-, Kopier- und Downloadfunktionen werden beschränkt und protokolliert • Personendaten werden bei Übertragung und Speicherung verschlüsselt • Administrative Zugriffe sind durch MFA und individuelle Admin-Konten abgesichert • Daten werden nach Auftragsende über festgelegte technische Verfahren zurückgegeben, gesperrt oder gelöscht • Sicherheitsrelevante Ereignisse und unzulässige Zugriffe werden überwacht

Organisatorische Massnahmen
• Die vom Unterauftragsverarbeiter getroffenen Sicherheitsmassnahmen werden vorab geprüft • Unterauftragsverarbeiter werden unter Sorgfaltsgesichtspunkten ausgewählt (gerade in Bezug auf Datenschutz und Datensicherheit) • Mit Unterauftragsverarbeitern wurde die notwendige Vereinbarung zur Auftragsverarbeitung bzw. wurden vom EDÖB anerkannte Standarddatenschutzklauseln nach Art. 16 Abs. 2 lit. d DSGVO abgeschlossen • Weisungen an den Unterauftragsverarbeiter werden in Textform erteilt • Die Mitarbeitenden des Unterauftragsverarbeiters sind auf die Vertraulichkeit nach Art. 9 DSGVO verpflichtet • Der Unterauftragsverarbeiter ist zur Benennung einer zuständigen Datenschutz-Ansprechperson verpflichtet; Art. 10 DSGVO sieht für private Verantwortliche eine freiwillige Datenschutzberatung vor • Gegenüber dem Auftragnehmer sind wirksame Kontrollrechte vereinbart • Der Einsatz weiterer Subunternehmer ist vertraglich geregelt • Die Vernichtung von Daten nach Beendigung des Auftrags wird sichergestellt • Bei längerer Zusammenarbeit werden der Unterauftragsverarbeiter und sein Schutzniveau laufend überprüft

7 Verfügbarkeitskontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Massnahmen
• Kritische Systeme sind über eine unterbrechungsfreie Stromversorgung (USV) abgesichert • Server- und Netzwerkinfrastruktur sind mit Überspannungsschutz und abgesicherter Stromversorgung ausgestattet



Technische Massnahmen

- Server- bzw. Technikräume werden klimatisiert; Temperatur und Luftfeuchtigkeit werden überwacht
- Brandfrüherkennung, Rauchmeldeanlagen und geeignete Feuerlöschvorrichtungen sind installiert
- Kritische Bereiche sind vor Wasserschäden geschützt, insbesondere durch geeignete Standortwahl und Vermeidung wasserführender Leitungen
- Es werden redundante Speichersysteme eingesetzt, z. B. RAID oder Festplattenspiegelung
- Für kritische Infrastruktur werden, soweit angemessen, redundante Systeme oder Komponenten eingesetzt
- Kritische Systeme, Speicherkapazitäten, Dienste und Verfügbarkeiten werden überwacht
- Systemausfälle, Kapazitätsengpässe und sicherheitsrelevante Störungen lösen automatisierte Benachrichtigungen aus
- Daten werden regelmässig nach einem festgelegten Sicherungskonzept gesichert
- Sicherungskopien werden verschlüsselt gespeichert, soweit Personendaten betroffen sind
- Backups werden getrennt von den Produktivsystemen gespeichert, z. B. offsite, offline oder georedundant
- Sicherungskopien sind gegen unbefugte Veränderung oder Löschung geschützt, z. B. durch Zugriffsbeschränkungen oder unveränderbare Backup-Speicher

Organisatorische Massnahmen

- Sicherungsintervalle, Aufbewahrungsfristen und Verantwortlichkeiten sind festgelegt
- Erfolgreiche Sicherungsvorgänge werden regelmässig kontrolliert und dokumentiert
- Die Datenwiederherstellung wird regelmässig getestet; die Ergebnisse werden protokolliert
- Wiederanlaufzeiten und Wiederherstellungspunkte sind, soweit erforderlich, festgelegt
- Für wesentliche Systeme und Prozesse ist ein Notfall- und Wiederanlaufplan dokumentiert
- Das Notfallkonzept wird regelmässig überprüft und aktualisiert
- Interne Melde- und Eskalationswege bei Systemausfällen oder Datenverlust sind festgelegt
- Kritische Infrastruktur, insbesondere USV, Klimatisierung, Brandmelde- und Sicherungssysteme, wird gewartet und regelmässig geprüft
- Störungen, Ausfälle und Wiederherstellungsmassnahmen werden dokumentiert



Organisatorische Massnahmen

- Beim Einsatz externer Dienstleister werden deren Verfügbarkeits-, Backup- und Wiederherstellungsmassnahmen auf Angemessenheit geprüft

8 Trennungskontrolle (Trennungsgebot)

Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Massnahmen

- Produktiv-, Test- und Entwicklungsumgebungen sind getrennt
- Systeme, Datenbanken oder Datenträger werden, soweit erforderlich, physisch getrennt
- Innerhalb der eingesetzten Anwendungen werden Mandanten bzw. Kunden logisch getrennt
- Personendaten werden, soweit erforderlich, nach Mandanten, Kunden, Projekten, Organisationseinheiten oder Verarbeitungsvorgängen getrennt
- Rollen- und berechtigungsbasierte Zugriffsbeschränkungen sind technisch umgesetzt
- Datenbankrechte sind festgelegt und technisch umgesetzt
- Für unterschiedliche Zwecke oder Mandanten werden getrennte Speicherbereiche, Verzeichnisse oder Datenräume genutzt
- Benutzer-, Administratoren- und Servicekonten sind getrennt
- Produktive Personendaten werden in Test- und Entwicklungsumgebungen, soweit möglich, nicht genutzt
- Testdaten werden anonymisiert oder pseudonymisiert, soweit personenbezogene Echtdaten für Tests nicht erforderlich sind
- Datenexporte zwischen getrennten Systembereichen oder Mandanten werden technisch beschränkt
- Es werden mandantenfähige Systeme mit getrennter Rechte-, Rollen- und Datenverwaltung eingesetzt
- Backup- oder Archivierungsbereiche werden getrennt geführt, soweit dies zur Zweck- oder Mandantentrennung erforderlich ist

Organisatorische Massnahmen

- Ein Berechtigungskonzept zur Trennung von Daten, Rollen und Verantwortlichkeiten ist dokumentiert und wird angewendet
- Es ist festgelegt, welche Personen oder Rollen auf welche Datenbestände zugreifen dürfen
- Organisatorische Vorgaben zur Trennung von Daten nach Zweck, Mandant, Kunde, Projekt oder Verarbeitungsvorgang sind festgelegt
- Die Systeme, Anwendungen und Datenbestände, in denen Personendaten getrennt verarbeitet werden, sind dokumentiert



Organisatorische Massnahmen

- Berechtigungen und Trennungsvorgaben werden regelmässig überprüft
- Die Zusammenführung, Übertragung oder Auswertung getrennter Datenbestände durchläuft einen Freigabeprozess
- Die Nutzung von Echtdaten in Test- und Entwicklungsumgebungen ist durch Vorgaben geregelt
- Die Anonymisierung oder Pseudonymisierung von Daten für Test-, Analyse- oder Schulungszwecke ist durch Vorgaben geregelt
- Zuständigkeiten für die Einrichtung, Änderung und Kontrolle von Mandanten-, Rollen- und Zwecktrennungen sind klar festgelegt
- Mitarbeitende werden zur zweckgebundenen Verarbeitung von Personendaten sensibilisiert
- Ausnahmen, bei denen getrennte Datenbestände zusammengeführt oder gemeinsam ausgewertet werden, werden dokumentiert
- Es wird regelmässig geprüft, ob bestehende Datenbestände noch dem vorgesehenen Zweck entsprechen

9 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

(Art. 8 DSG; Art. 1–3 DSV)

9.1 Massnahmen zum Datenschutzmanagement

Massnahmen, die gewährleisten, dass die Wirksamkeit der technischen und organisatorischen Massnahmen regelmässig überprüft, bewertet und bei Bedarf angepasst wird.

- Mitarbeitende werden regelmässig zu Datenschutz, Vertraulichkeit und Informationssicherheit geschult und sensibilisiert
- Ein Datenschutzkonzept mit Beschreibung wesentlicher Datenschutzprozesse, Verantwortlichkeiten und Kontrollmechanismen ist dokumentiert
- Ein vollständiges und aktuelles Verzeichnis der Verarbeitungstätigkeiten wird geführt
- Das Verzeichnis der Verarbeitungstätigkeiten wird regelmässig überprüft und aktualisiert
- Aufbewahrung, Löschung und Archivierung von Personendaten sind dokumentiert geregelt
- Sicherung und Wiederherstellung des Datenbestands sind dokumentiert geregelt
- Aufbewahrung und Auswertung elektronischer Protokolle sind geregelt
- Standards und Vorgaben zur IT-Sicherheit sind festgelegt und werden angewendet
- Die Mitarbeitenden sind nachweislich auf Vertraulichkeit verpflichtet



- Die bestehenden technischen und organisatorischen Massnahmen werden regelmässig überprüft
- Datenschutz- und Datensicherheitsmassnahmen werden risikoorientiert kontrolliert
- Bei wesentlichen Änderungen von Verfahren, Systemen oder Dienstleistern werden die Massnahmen anlassbezogen überprüft
- Durchgeführte Kontrollen und Prüfergebnisse werden dokumentiert
- Festgestellte Abweichungen und eingeleitete Korrekturmassnahmen werden dokumentiert
- Berechtigungskonzepte, Zugriffsrechte und Benutzerkonten werden regelmässig überprüft
- Die eingesetzten Dienstleister und Auftragsverarbeiter werden, soweit erforderlich, regelmässig überprüft
- Bei neuen oder geänderten Verfahren werden Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen berücksichtigt
- Datenschutz-Folgenabschätzungen werden durchgeführt, soweit gesetzlich erforderlich
- Interne Verantwortlichkeiten für Datenschutz, Informationssicherheit und Massnahmenkontrolle sind festgelegt
- Der zuständigen Leitungsebene wird, soweit angemessen, regelmässig Bericht erstattet

9.2 Massnahmen zum Incident-Response-Management

Massnahmen, die gewährleisten, dass Datenschutzvorfälle erkannt, bewertet, dokumentiert und bei Auftragsverarbeitung unverzüglich den Kunden gemeldet werden können.

- Mitarbeitende werden zum Erkennen von Datenschutzvorfällen geschult und sensibilisiert
- Ein internes Incident-Response-Management-Konzept ist dokumentiert und wird angewendet
- Interne Meldewege für Datenschutzvorfälle und Sicherheitsereignisse sind festgelegt
- Verantwortlichkeiten für Annahme, Bewertung und Bearbeitung von Datenschutzvorfällen sind festgelegt
- Ob eine Verletzung des Schutzes von Personendaten vorliegt, wird nach einem dokumentierten Verfahren bewertet
- Mögliche Risiken für betroffene Personen werden nach einem dokumentierten Verfahren bewertet
- Datenschutzvorfälle werden dem Kunden bei Auftragsverarbeitung nach einem dokumentierten Verfahren gemeldet
- Fristen und Eskalationswege für die interne und externe Meldung von Datenschutzvorfällen sind festgelegt



- Datenschutzvorfälle werden einschliesslich Sachverhalt, Zeitpunkt, betroffener Daten, betroffener Systeme, Ursache und ergriffener Massnahmen dokumentiert
- Datenschutzvorfälle werden nach einem festgelegten Verfahren eingedämmt und behoben
- Im Fall eines Vorfalls werden relevante Nachweise und Protokolldaten nach einem festgelegten Verfahren gesichert
- Kommunikationswege zum Kunden, zu internen Verantwortlichen und gegebenenfalls zu weiteren beteiligten Dienstleistern sind festgelegt
- Das Incident-Response-Konzept wird regelmässig überprüft und aktualisiert
- Datenschutzvorfälle werden nachbereitet, um technische und organisatorische Verbesserungsmassnahmen abzuleiten
- Der Incident-Response-Prozess wird, soweit angemessen, regelmässig getestet oder geübt

10 Schweizer Rechtsrahmen und Geltung

Diese Anlage ist Bestandteil des Auftragsbearbeitungsvertrags DATA Security AG nach Art. 9 DSG. Die Massnahmen dienen der risikoadäquaten Datensicherheit nach Art. 8 DSG sowie Art. 1–3 DSV; sie sind umgesetzt, soweit sie technisch bzw. organisatorisch einschlägig sind.

Schweizer Ergänzungen zur Wirksamkeitskontrolle

Der Schutzbedarf wird anhand Datenart, Zweck, Umfang und Umständen bestimmt und unter Berücksichtigung von Wahrscheinlichkeit, Schwere, Stand der Technik und Implementierungskosten regelmässig überprüft (Art. 1 DSV).

Schutzziele: Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit (Art. 2 DSV). Zugangs-, Zugriff-, Datenträger-, Speicher-, Transport-, Wiederherstellungs- und Überprüfungsmassnahmen richten sich nach Art. 3 DSV.

Auslandzugriffe, Cloud-Hosting und Backups unterliegen zusätzlich der Länder- und Empfängerprüfung nach Art. 16 und 17 DSG und Anhang 1 DSV.

Sicherheitsvorfälle werden dem Verantwortlichen so rasch als möglich gemeldet (Art. 24 Abs. 3 DSG); die Risikobeurteilung und allfällige Meldung an den EDÖB liegt beim Verantwortlichen (Art. 24 Abs. 1 DSG).



Anlage 2 – Verpflichtung zur Wahrung des Berufsgeheimnisses

Ergänzung zum Auftragsbearbeitungsvertrag nach Art. 9 DSG

1 Zweck und Anwendungsbereich

Diese Anlage schützt vertrauliche Informationen und Geheimnisse, die der Auftragnehmerin bei der Erbringung der vereinbarten Leistungen für Rechtsanwältinnen und Rechtsanwälte, Revisorinnen und Revisoren sowie Treuhänderinnen und Treuhänder bekannt werden oder zugänglich sein könnten. Sie ergänzt die Pflichten aus dem Auftragsbearbeitungsvertrag und konkretisiert insbesondere dessen Regelung zum Anwaltsgeheimnis in Ziffer 10.2. Sie erlaubt keine zusätzliche Datenbearbeitung und erweitert weder die bezogenen Lösungen noch die vereinbarten Datenkategorien.

Als Geheimnisse gelten insbesondere nicht öffentlich bekannte Informationen über Mandate, Klientinnen und Klienten, Prüfungsfeststellungen, wirtschaftliche Verhältnisse, Geschäftsabläufe sowie vertrauliche Dokumente und Zugangsdaten. Vertragsgemäss sind diese Informationen unabhängig davon zu schützen, ob sie im Einzelfall Personendaten darstellen oder unter einen besonderen strafrechtlichen Geheimnistatbestand fallen.

2 Berufsgruppen und gesetzlicher Schutz

- (1) **Rechtsanwältinnen und Rechtsanwälte:** Das anwaltliche Berufsgeheimnis ergibt sich aus Art. 13 des Bundesgesetzes über die Freizügigkeit der Anwältinnen und Anwälte (BGFA) und wird strafrechtlich durch Art. 321 StGB geschützt. Der Schutz erstreckt sich auf Geheimnisse aus der anwaltlichen Berufstätigkeit; die Anwältin bzw. der Anwalt hat dafür zu sorgen, dass Hilfspersonen das Geheimnis wahren. Eine vorsätzliche unbefugte Offenbarung durch die vom Straftatbestand erfassten Personen kann auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft werden.
- (2) **Revisorinnen und Revisoren:** Die Revisionsstelle unterliegt der Geheimhaltung nach Art. 730b Abs. 2 OR hinsichtlich ihrer Feststellungen und der Geschäftsgeheimnisse der geprüften Gesellschaft. Art. 321 StGB erfasst ausdrücklich die nach Obligationenrecht zur Verschwiegenheit verpflichteten Revisorinnen und Revisoren sowie ihre Hilfspersonen. Die genaue Reichweite richtet sich nach der tatsächlich ausgeübten Revisionsfunktion; die Bezeichnung "Revisor" allein genügt nicht für jede denkbare Beratungsleistung.
- (3) **Treuhänderinnen und Treuhänder:** Die Berufsbezeichnung "Treuhänderin" oder "Treuhänder" begründet für sich allein keine Zugehörigkeit zum abschliessend bezeichneten Personenkreis des Art. 321 StGB. Art. 62 DSG schützt geheime Personendaten, die im Rahmen einer Berufstätigkeit, welche deren Kenntnis erfordert, erlangt werden, vor vorsätzlicher unbefugter Offenbarung. Unter den Voraussetzungen dieser Bestimmung droht auf Antrag eine Busse bis CHF 250'000.



Daneben können vertragliche Geheimhaltungspflichten, auftragsrechtliche Treuepflichten und gegebenenfalls weitere spezialgesetzliche Pflichten bestehen. Diese Anlage vereinbart unabhängig von der Einordnung ein umfassendes vertragliches Stillschweigen.

3 Stellung der Auftragnehmerin und der eingesetzten Personen

Die Auftragnehmerin verpflichtet sich als Vertragspartei zur Vertraulichkeit. Ob eine bestimmte natürliche Person, etwa eine mit Support oder Administration befassete Mitarbeiterin oder ein Mitarbeiter, strafrechtlich als Hilfsperson nach Art. 321 StGB oder als mitwirkende Person nach Art. 62 Abs. 2 DSG erfasst ist, ergibt sich aus den gesetzlichen Voraussetzungen und ihrer konkreten Tätigkeit. Eine solche strafrechtliche Stellung wird nicht allein durch diese Vereinbarung begründet. Die Auftragnehmerin organisiert ihre Leistungserbringung so, dass auch ohne unmittelbare Strafbarkeit ein gleichwertiger vertraglicher Geheimnisschutz besteht.

4 Konkrete Verpflichtungen

- (1) Die Auftragnehmerin bearbeitet oder verwendet geschützte Informationen ausschliesslich, soweit dies für die dokumentiert vereinbarten Leistungen erforderlich und rechtlich zulässig ist. Eine Nutzung für eigene Zwecke, Produktentwicklung, Werbung oder das Training von KI-Modellen ist ausgeschlossen, sofern sie nicht gesondert wirksam vereinbart und zulässig ist.
- (2) Die Auftragnehmerin beschränkt den Zugang nach dem Need-to-know-Prinzip, setzt angemessene technische und organisatorische Massnahmen um und dokumentiert berechtigte Zugriffe, soweit dies nach Schutzbedarf und eingesetztem System erforderlich ist.
- (3) Sie verpflichtet alle Personen mit möglichem Geheimniszugang vor ihrem Einsatz nachweisbar zur Vertraulichkeit, informiert sie über die einschlägigen gesetzlichen und vertraglichen Folgen einer unbefugten Offenbarung und sichert die Fortgeltung der Verpflichtung über das Ende ihrer Tätigkeit hinaus.
- (4) Unterauftragsbearbeiter und andere Dritte mit tatsächlicher Zugriffsmöglichkeit auf geheimnisgeschützte Informationen werden nur nach Ziffer 11 des Auftragsbearbeitungsvertrags hinzugezogen; für Mandatsinformationen gilt zusätzlich dessen Ziffer 10.2. Die Auftragnehmerin stellt vor einem möglichen Zugriff einen mindestens gleichwertigen Geheimnisschutz, notwendige Zugriffsbeschränkungen und die Weitergabe der Verpflichtung an deren Mitarbeitende sicher.
- (5) Die Auftragnehmerin informiert den Auftraggeber unverzüglich über einen tatsächlichen oder begründet vermuteten unbefugten Zugriff oder eine unzulässige Offenbarung und unterstützt ihn bei der Eindämmung und rechtlichen Beurteilung des Vorfalls. Die Pflichten zur Meldung von Datensicherheitsverletzungen nach Art. 24 DSG bleiben unberührt.



- (6) Bei Herausgabeverlangen von Behörden, Gerichten oder Dritten prüft die Auftragnehmerin die rechtliche Verpflichtung und die mögliche Betroffenheit geschützter Geheimnisse. Sie informiert den Auftraggeber vorgängig, soweit rechtlich zulässig, ermöglicht dessen rechtliche Prüfung und beschränkt eine rechtlich zwingende Herausgabe auf den notwendigen Umfang. Gesetzlich verbindliche Offenlegungspflichten bleiben vorbehalten.

5 Dauer, Rangfolge und Verhältnis zum Datenschutz

Die Geheimhaltungspflicht besteht während der Vertragsdauer und nach Vertragsende fort, solange die betreffenden Informationen geheimhaltungsbedürftig sind oder eine gesetzliche Geheimhaltungspflicht fortbesteht. Gesetzliche Aufbewahrungs- oder Offenlegungspflichten bleiben vorbehalten. Soweit diese Anlage strengere Geheimhaltungsvorkehrungen vorsieht, gehen diese den allgemeinen Vertragsbestimmungen vor; zwingendes Recht und die ausdrücklich vereinbarte Begrenzung des Bearbeitungsumfangs bleiben unberührt.

Diese Anlage ersetzt weder eine bei einzelnen Mandaten erforderliche Prüfung der Zulässigkeit des Beizugs externer Dienstleister noch die datenschutzrechtliche Prüfung nach Art. 9 DSG. Der Auftraggeber bleibt für die Beurteilung seines Berufsgeheimnisses und der zulässigen Offenlegung im konkreten Mandatsverhältnis verantwortlich; die Auftragnehmerin bleibt für ihre eigenen vertraglichen und gesetzlichen Pflichten verantwortlich.

