Auftragsbearbeitungsvertrag

zwischen

Auftragnehmer

DATA Security AG

Färberstrasse 9

CH-8832 Wollerau

(nachfolgend «Auftragnehmer» genannt)

und

Auftraggeber

Anwender von DATA Security Manager

(nachfolgend «Auftraggeber» genannt)

Stand: 18.08.2023

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 besteht ein Hauptvertrag zwischen dem Auftraggeber und Auftragnehmer. Im Hauptvertrag sind die jeweiligen Rechte und Pflichten geregelt. Darüber hinaus gelten die AGB und Verhaltenskodex der DATA Security AG. Mit diesem Vertrag sollen zusätzlich die Vorgaben des Bundesgesetzes über den Datenschutz (DSG) hinsichtlich Art. 9 DSG geregelt werden.

2. Definitionen, Begriffsbestimmungen

1. Der Gegenstand des Auftrages ist im jeweiligen Hauptvertrag beschrieben.
2. 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.
3. 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 des Hauptvertrags 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:

- Mitarbeiter und Familienangehörige
- Dienstleister und deren Mitarbeiter
- Geschäftspartner und deren Mitarbeiter
- Kunden/Mandanten und deren Geschäftspartner/Mitarbeiter
- Ggf. andere Personen

5. Arten der Personendaten

Gegenstand der Erhebung, Bearbeitung und/oder Nutzung von Personendaten sind Datenarten/-kategorien, entsprechend der Beschreibung der Datenarten im Verzeichnis der Bearbeitungstätigkeiten.

- Stammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Kundenhistorien
- Vertragsdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Daten höherer Kategorien

6. Ort der Bearbeitung

Die Datenbearbeitung 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 so weit ein Angemessenheitsbeschluss hierzu vorliegt oder durch andere geeignete Garantien i.S.v. Art. 16 DSG ein angemessenes Datenschutzniveau sichergestellt ist. 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. Nach Art. 13 DSG kann der Nachweis durch Vorlage eines entsprechenden Zertifikates einer akkreditierten Zertifizierungsstelle geführt werden. 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.

7. Kontrollechte des Auftraggebers

1. 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.
2. 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.

3. 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.
4. 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.
5. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Weisungsbefugnisse des Auftraggebers

1. Die Verarbeitung der Daten erfolgt ausschliesslich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über Art, Umfang und Verfahren der Datenverarbeitung sowie über Änderungen der Verarbeitung vor.
2. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
3. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Weisungsberechtigte Personen des Auftraggebers sind nachfolgende Personenkreise:

   - Geschäftsleitung:
     - Herr Slobodan Mikulovic, +41 44 552 23 55, info@data-security.ch

4. Änderungen der weisungsberechtigten Personenkreise sind unverzüglich schriftlich mitzuteilen.

9. Pflichten des Auftragnehmers

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.

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.

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.

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.

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.

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

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 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 Sozialgeheimnisses, 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.

11. Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post- /Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsbearbeiter im Sinne des Art. 9 DSG in Anspruch zu nehmen.
3. Die jeweils aktuell eingesetzten, weiteren Auftragsverarbeiter kann der Auftraggeber unter: https://www.data-security.ch/upload/Liste_der_Dienstleister.pdf abrufen. Diese Liste wird, falls sich Änderungen ergeben, quartalsweise aktualisiert.
4. Der Auftragnehmer informiert den Auftraggeber, wenn eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt wird. Die Änderungen kann der Auftraggeber unter: https://www.data-security.ch/upload/Liste_der_Dienstleister.pdf abrufen. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.
5. Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrechtlichen Grund erhoben werden. Der Einspruch ist innerhalb von 4 Wochen nach Bereitstellung der Information gegenüber dem Auftragnehmer in Schriftform zu erheben. Im Fall eines begründeten Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung oder den gesamten Vertrag gegenüber dem Auftraggeber innerhalb von 4 Wochen nach Zugang des Einspruchs kündigen.
6. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Die volle Verantwortung für die von Auftragnehmer eingeschalteten Subunternehmer bleibt beim Auftragnehmer.

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.
   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.
3. 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.
4. Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 19 DSG 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.

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.
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

1. 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 DSG entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten.

   Die technischen und organisatorischen Massnahmen umfassen insbesondere:

   a) die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Bearbeitung der Daten,

   b) die rasche Wiederherstellung der Verfügbarkeit der Personendaten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls und

   c) 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.

2. Der Auftragnehmer sichert die Einhaltung der genannten Massnahmen und Regelungen zu. Diese Massnahmen gelten als vereinbart und die Beschreibung der Massnahmen wird Bestandteil dieses Vertrages.

3. 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.

4. Der Auftragnehmer kann die Eignung der nach Art. 8 DSG 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.
5.

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, dem Auftraggeber auszuhändigen oder in Abstimmung mit

dem Auftraggeber 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.

16. Vertragsdauer und Kündigung

1. Die Vertragsdauer und die Kündigung wird im Hauptvertrag bzw. den AGB beschrieben. 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.
2. 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.

18. Haftung

Für die Haftung gelten die Regelungen des Art. 60 ff. DSG.

Zusätzlich gelten für die Haftung die Regelungen des Hauptvertrags.

19. Anwendbares Recht und Gerichtsstand

1. Es gilt das Recht der Schweiz unter Ausschluss des UN-Kaufrechts.
2. Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevante Streitigkeiten ist der Sitz der DATA Security AG, Wollerau.

Gesetzliche Regelungen über ausschliessliche Zuständigkeiten bleiben hiervon unberührt.

20. Anlage 1 Beschreibung der vereinbarten technischen und organisatorischen Massnahmen (TOM)

DATA Security AG, Färberstrasse 9, CH-8832 Wollerau - i.S.d. Art. 7 DSG

Unternehmen, die selbst oder als Dienstleister (nach Art. 9 DSG) Personendaten bearbeiten oder Zugriff darauf haben, müssen technische und organisatorische Massnahmen treffen und umsetzen, welche die Einhaltung der Datenschutzgrundsätze, sowie die Sicherheit der Bearbeitung von Personendaten gewährleisten.

1. Zutrittskontrolle

Massnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Personendaten verarbeitet oder genutzt werden, zu versperren.

Technische Massnahmen

- Manuelles Schliesssystem
- Sicherheitsschlösser
- Klingelanlage

Organisatorische Massnahmen

- Schlüsselregelung / Liste
- Empfang
- Besucher in Begleitung durch Mitarbeiter
- Sorgfalt bei Auswahl Reinigungsdienste
- Ansprache unbekannter Personen
- Begrenzung der Bereiche, die externe Dienstleister (z.B. Reinigungs- und Wartungspersonal) aufsuchen können

2. Zugangskontrolle

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

Technische Massnahmen

- Login mit Benutzername + Passwort
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung von Datenträgern
- Automatische Desktopsperre
- Verschlüsselung von Notebooks/Tablets

Organisatorische Massnahmen

- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe

- Personenkontrolle beim Empfang
- Richtlinie „Sicheres Passwort“
- Richtlinie „Clean Desk“
- Allg. Richtlinie Datenschutz und Sicherheit
- Mobile Device Policy
- Anleitung „Manuelle Desktopsperre“

3. Zugriffskontrolle

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

Technische Massnahmen

- Aktenschredder (mind. Stufe 3, cross cut)
- Externer Aktenvernichter (DIN 32757)
- Physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung von Datenträgern

Organisatorische Massnahmen

- Einsatz Berechtigungskonzepte
- Verwaltung der Rechte durch einen Systemadministrator
- Minimale Anzahl an Administratoren
- Protokollierung der Vernichtung von Datenträgern

4. Weitergabekontrolle

Massnahmen, die gewährleisten, dass Personendaten 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-Mail-Verschlüsselung
- Einsatz von VPN
- Protokollierung der Zugriffe und Abrufe
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https

Organisatorische Massnahmen

- Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen

5. Eingabekontrolle

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

Technische Massnahmen

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatisierte Kontrolle der Protokolle

Organisatorische Massnahmen

- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder
- gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Klare Zuständigkeit für Löschungen

6. Auftragskontrolle

Massnahmen, die gewährleisten, dass Personendaten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Organisatorische Massnahmen

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmassnahmen
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

7. Verfügbarkeitskontrolle

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

Technische Massnahmen

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Serverraum klimatisiert
- USV
- Schutzsteckdosenleisten Serverraum
- RAID- System/ Festplattenspiegelung

- Videoüberwachung Serverraum
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum

Organisatorische Massnahmen

- Backup & Recovery-Konzept
- Kontrolle des Sicherungsvorgangs
- Regelmässige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten

8. Trennungskontrolle (Trennungsgebot)

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

Technische Massnahmen

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme/Datenbanken/Datenträger)
- Logische Mandantentrennung (softwareseitig)

Organisatorische Massnahmen

- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten

9. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management (Massnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.)

- Regelmässige Schulung der Mitarbeiter zum Datenschutz
- Ein Verzeichnis der Verarbeitungstätigkeiten ist vorhanden, vollständig und aktuell.
- Es bestehen Standards für die IT-Sicherheit
- Die Aufbewahrung der elektronischen Protokolle ist geregelt
- Es gibt Regelungen über die Sicherung des Datenbestands
- Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden
- Ein Datenschutzkonzept ist vorhanden
- Datenschutz- und Datensicherungsmassnahmen werden gelegentlich unvermutet kontrolliert

Incident-Response-Management (Massnahmen, die gewährleisten, dass im Falle einer Datenpanne eine unmittelbare Information an den Auftraggeber erfolgt.

- Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne
- Es existiert ein internes Incident-Response-Management-Konzept
- Es gibt ein Konzept zur Meldung von Daten-pannen an den Auftraggeber