Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO - OCB

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

Auftraggeber

nachstehend „Auftraggeber“ genannt
MentalSolutions.net
Natural-Lifestream GmbH
Huswisenstrasse 6
8426 Lufingen

und

Hulk AG

geschäftsansässig

Birkentraße 47

6343 Rotkreuz, Schweiz

Registernr.: CHE-473.773.896

nachstehend als "Auftragnehmer"

beide zusammen „Parteien“ genannt

Präambel

Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Rahmen der Bereitstellung der Software "OneClickBusiness" als Software as a Service. Dieser Vertrag enthält eine Reihe von Anlagen, die die vom Auftragnehmer für den Auftraggeber zu erbringenden Leistungen im Einzelnen spezifizieren – insgesamt als „Vertragsverhältnis“ bezeichnet. Bei der Erbringung dieser Leistungen werden personenbezogene Daten des Auftraggebers durch den Auftragnehmer verarbeitet. Die Verarbeitung der personenbezogenen Daten durch den Auftraggeber findet derzeit ausschließlich in der Bundesrepublik Deutschland bzw. der Europäischen Union oder im Europäischen Wirtschaftsraum statt.

Die Parteien wollen ihren wechselseitigen datenschutzrechtlichen Verpflichtungen nach Art. 28 DSGVO im Rahmen ihres Vertragsverhältnisses Rechnung tragen und schließen deswegen nachstehende Vereinbarung zur Auftragsverarbeitung:

§ 1 - Gegenstand und Dauer

(1) Gegenstand

(a) Inhaltlicher Geltungsbereich

Diese Vereinbarung zur Auftragsverarbeitung ergänzt und konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem Vertragsverhältnis. Diese Vereinbarung zur Auftragsverarbeitung gilt für sämtliche Tätigkeiten im Zusammenhang mit dem Vertragsverhältnis, bei denen Beschäftigte und/oder – soweit gemäß nachstehendem § 7 zulässig – Subunternehmer des Auftragnehmers personenbezogene Daten des Auftraggebers verarbeiten.

(b) Räumlicher Geltungsbereich

Nach dieser Vereinbarung zur Auftragsverarbeitung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer nur im Gebiet der Bundesrepublik Deutschland sowie der Europäischen Union und des Europäischen Wirtschaftsraumes zulässig. Dem Auftragnehmer ist es ohne vorherige Abstimmung mit dem Auftraggeber nicht gestattet, die Verarbeitung personenbezogener Daten des Auftraggebers in Drittländer außerhalb des Gebietes der Europäischen Union bzw. des Europäischen Wirtschaftsraumes zu verlagern. Wenn und soweit der Auftragnehmer künftig beabsichtigt, seine Leistungserbringung und damit einhergehend die Verarbeitung personenbezogener Daten des Auftraggebers ins außereuropäische Ausland zu verlagern, hat er den Auftraggeber umgehend zu unterrichten.

Eine solche Verarbeitung außerhalb der EU und des EWR darf nur erfolgen, wenn der Auftraggeber dieser vorher schriftlich oder in einem dokumentierten elektronischen Format zugestimmt hat und wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO durch eine der nachfolgend aufgeführten Maßnahmen erfüllt sind. Das angemessene Schutzniveau

- ist festgestellt durch einen Angemessenheitsbeschluss
- der Kommission (Art. 45 Abs. 3 DSGVO);

- wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b in Verbindung mit Art. 47 DSGVO);
- wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO);
- wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e in Verbindung mit Art. 40 DSGVO);
- wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f in Verbindung mit Art. 42 DSGVO);
- wird hergestellt durch sonstige Maßnahmen: (Art. 46 Abs. 2 lit. a, Abs. 3 lit. a und b DSGVO)

(2) Dauer

Diese Vereinbarung tritt mit Bestätigung des Auftraggebers im Backend der Software "OneClickBusiness" statt und endet mit der Beendigung des Vertragsverhältnisses.

(3) Kündigung

Beide Parteien sind berechtigt, diese Vereinbarung jederzeit aus wichtigem Grund zu kündigen. Ein solcher wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn

- der Auftragnehmer trotz Abmahnung durch den Auftraggeber die zur Verarbeitung der personenbezogenen Daten des Auftraggebers befugten Personen nicht zur Vertraulichkeit oder auf das Datengeheimnis nach § 53 BDSG verpflichtet hat und diese keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- der Auftragnehmer den Auftraggeber entgegen § 9 Abs. 2 nicht oder nicht unverzüglich über Verletzungen des Schutzes personenbezogener Daten informiert (Art. 33 Abs. 2 DSGVO);
- der Auftragnehmer den Auftraggeber im Rahmen seiner Meldepflicht gegenüber der Aufsichtsbehörde und den betroffenen Personen nach Art. 33, 34 DSGVO nicht oder nicht unverzüglich oder nicht vollständig über die Art der Verletzung des Schutzes personenbezogener Daten, der Anzahl der betroffenen Personen und betroffenen Kategorien personenbezogener Daten und die wahrscheinlichen Folgen der Verletzung personenbezogener Daten für die betroffenen Personen informiert hat;
- der Auftragnehmer dem Auftraggeber oder einem von ihm beauftragten Prüfer den Zutritt zu seinen Räumlichkeiten und den Zugang zu den IT-Anlagen zwecks Durchführung der Kontrollen nach Art. 28 Abs. 3 lit. h DSGVO trotz zweifacher Aufforderung nicht ermöglicht und/oder nicht alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten des Art. 28 DSGVO zur Verfügung stellt, ohne dass hierfür ein wichtiger Grund vorliegt;
- der Auftragnehmer technische und organisatorische Maßnahmen ohne Abstimmung mit dem Auftraggeber entgegen § 4 Abs. 3 ändert und hierbei das nach Art. 32 DSGVO erforderliche Datenschutz- und Datensicherheitsniveau, insbesondere der Stand der Technik, nicht eingehalten wird;
- der Auftragnehmer Weisungen des Auftraggebers nicht ausführen kann oder will.

§ 2 - Verantwortungsbereiche

Beide Parteien verpflichten sich, die zur Anwendung kommenden Datenschutzgesetze (insbesondere die Bestimmungen der DSGVO und des BDSG) einzuhalten. Die Parteien gehen davon aus, dass der Auftragnehmer als Auftragsverarbeiter im Sinne des Art. 28 DSGVO für den Auftraggeber tätig wird. Wenn und soweit der Auftragnehmer jetzt oder künftig Leistungen erbringen soll, die nicht nach dieser Vereinbarung privilegiert sind, werden die Parteien schriftlich ergänzende Bestimmungen zum Datenschutz treffen, insbesondere diese Vereinbarung ergänzen oder eine neue Vereinbarung zur Auftragsverarbeitung abschließen.

Auf Anfrage der Aufsichtsbehörde arbeiten Auftraggeber und Auftragnehmer bei der Erfüllung ihrer Aufgaben zusammen (Art. 31 DSGVO).

Im Rahmen der Durchführung dieser Vereinbarung gelten nachfolgende Verantwortungsbereiche:

(1) Verantwortung des Auftraggebers

(a) Der Auftraggeber bestimmt die Zwecke und die Ziele der Verarbeitung der personenbezogenen Daten. Dies geschieht durch die in § 1 (1) (a) spezifizierten Vertragsdokumente und deren Anlagen sowie ergänzend durch die nach Maßgabe dieser Vereinbarung durch den Auftraggeber dem Auftragnehmer nach § 10 zu erteilenden Weisungen.

(b) Der Auftraggeber ist im Hinblick auf das Vertragsverhältnis und die in dessen Durchführung vom Auftragnehmer zu verarbeitenden Daten für die Einhaltung sämtlicher einschlägiger Datenschutzvorschriften, insbesondere der DSGVO und des BDSG, verantwortlich. Der Auftraggeber ist insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung und die Zulässigkeit der Datenverarbeitung nach Art. 6 DSGVO sowie die Wahrung der Rechte der betroffenen Personen nach Art. 12–22 DSGVO verantwortlich.

(c) Der Auftraggeber behält die volle Kontrolle über die vom Auftragnehmer zu verarbeitenden Daten. Sämtliche verarbeiteten Daten stehen ausschließlich dem Auftraggeber zu.

(2) Verantwortung des Auftragnehmers

(a) Der Auftragnehmer wird personenbezogene Daten, die er im Rahmen dieser Vereinbarung im Auftrag für den Auftraggeber verarbeitet, ausschließlich zur Erfüllung des im Vertrag und seinen Leistungsscheinen sowie in etwaigen nach Maßgabe dieser Vereinbarung zu erteilenden Weisungen beschriebenen Zwecken verarbeiten.

(b) Verlangt der Auftraggeber seine Daten – egal aus welchem Grund – heraus, ist der Auftragnehmer verpflichtet, dem Auftraggeber sämtliche Daten in einem strukturierten, gängigen und maschinenlesbaren Format für die automatisierte Übernahme oder direkte Einspielung herauszugeben. Zurückbehaltungsrechte – egal welcher Art – stehen dem Auftragnehmer an diesen Daten nicht zu.

§ - 3 Art, Ziel und Zweck der Verarbeitung personenbezogener Daten

(1) Art und Zweck der Datenverarbeitung

Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung sind die Nutzung der Software "OneClickBusiness".

(2) Art der Daten der Datenverarbeitung

Gegenstand der Verarbeitung personenbezogener Daten unter dem Vertragsverhältnis dieser Vereinbarung zur Auftragsverarbeitung sind folgende Verarbeitungsvorgänge:

- das Erheben
- das Erfassen
- die Organisation
- das Ordnen
- die Speicherung
- das Auslesen
- das Abfragen
- die Verwendung
- die Offenlegung durch Übermittlung
- die Verbreitung oder eine andere Form der Bereitstellung
- den Abgleich oder die Verknüpfung
- die Einschränkung der Verarbeitung

Im Rahmen des Vertragsverhältnisses verarbeitet der Auftragnehmer folgende Arten von Daten:

- Personenstammdaten
- Kommunikationsdaten (zum Beispiel Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkte- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, zum Beispiel Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen

Der Kreis der durch die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung betroffenen Personen umfasst:

- Kunden

§ 4 - Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Nachweis der technischen und organisatorischen Maßnahmen

Vor Abschluss dieser Vereinbarung zur Auftragsverarbeitung und vor Beginn der Verarbeitung personenbezogener Daten durch den Auftragnehmer hat dieser dem Auftraggeber die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen, insbesondere hinsichtlich der konkreten Auftragsdurchführung nach Maßgabe dieser Vereinbarung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die so dokumentierten Maßnahmen Grundlage dieses Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und zu dokumentieren.

(2) Gewährleistung eines angemessenen Schutzniveaus

Der Auftragnehmer wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleisten. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Maßnahmen das Risiko auf Dauer eingedämmt wird. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Beschreibung der technisch-organisatorischen Maßnahmen

Zur Gewährleistung einer dem Risiko der Datenverarbeitung nach dem Vertrag und den Leistungsscheinen angemessenen Schutzniveau hat der Auftragnehmer die in seinem (Daten-)Sicherheitskonzept aufgeführten technischen und organisatorischen Maßnahmen gem. Art. 24, 32 DSGVO getroffen. Das (Daten-)Sicherheitskonzept wird als verbindlich festgelegt und als Anlage zu dieser Vereinbarung zur Auftragsverarbeitung genommen. Die darin beschriebenen Maßnahmen sind passend zum ermittelten Risiko der Verarbeitung unter Berücksichtigung der Schutzziele nach Stand der Technik und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse spezifiziert.

Dieses beinhaltet im Wesentlichen folgende technische und organisatorische Maßnahmen:

- Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO).
- Maßnahmen zur Gewährleistung der Fähigkeit, die Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO), Integrität (Art. 32 Abs. 1 lit. b DSGVO), Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO) im Zusammenhang mit der Verarbeitung auf

Dauer sicherzustellen.
- Maßnahmen zur Gewährleistung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO).
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO).

(4) Technischer Fortschritt und Änderung der technisch-organisatorischen Maßnahmen

Die in dieser Vereinbarung zur Auftragsverarbeitung/der Anlage1 zu dieser Vereinbarung zur Auftragsverarbeitung beschriebenen technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragnehmer ist es deshalb gestattet, alternative adäquate Maßnahmen umzusetzen, wenn und soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird dem Auftraggeber die technischen und organisatorischen Maßnahmen sowie sämtliche Änderungen zur Verfügung stellen, damit dieser seiner Dokumentations- und Nachweisverpflichtung nach Art. 5 Abs. 2 DSGVO nachkommen kann.

(5) Informationspflicht des Auftragnehmers

Der Auftragnehmer wird den Auftraggeber betreffend technischer und organisatorischer Maßnahmen sowie Ereignisse, die für die Sicherheit oder Vertraulichkeit der verarbeiteten und genutzten Daten von Bedeutung sind, regelmäßig unterrichten. Bei Störungen oder Unregelmäßigkeiten wird der Auftragnehmer den Auftraggeber unverzüglich unterrichten.

§ 5 - Berichtigung, Löschung und Sperrung von Daten

(1) Die im Auftrag des Auftraggebers verarbeiteten Daten darf der Auftragnehmer nur nach Weisung des Auftraggebers berichtigen, löschen, übertragen oder ihre Verarbeitung einschränken. Wenn sich eine betroffene Person zu diesem Zweck direkt an den Auftragnehmer wendet, hat dieser ein solches Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.

(2) Der Ansprechpartner des Auftraggebers wird das Ersuchen prüfen und dem Auftragnehmer schriftlich mitteilen, ob es berechtigt war oder nicht und den Auftragnehmer anweisen, die Berichtigung, Löschung, Übertragung oder Einschränkung der Verarbeitung vorzunehmen. Die Weisung ist von beiden Parteien zu dokumentieren.

§ 6 - Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung zur Auftragsverarbeitung folgende gesetzliche Pflichten nach Art. 28–33 DSGVO:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38, 39 DSGVO ausüben kann;
- dem Auftraggeber auf Anforderung die Angaben nach Art. 30 Abs. 1 DSGVO zur Verfügung zu stellen;
- die zur Verarbeitung der personenbezogenen Daten befugten Personen des Auftragnehmers zur Vertraulichkeit gemäß Art. 28 Abs. 3 Satz 2 lit. b DSGVO bzw. zum Datengeheimnis gemäß § 53 BDSG zu verpflichten;
- den Auftraggeber im Rahmen des rechtlich und tatsächlich Möglichen mit technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrung der Rechte der betroffenen Personen (Art. 12–22 DSGVO) nachzukommen (Art. 28 Abs. 3 Satz 2 lit. e DSGVO);
- den Auftraggeber bei den in Art. 32–36 DSGVO genannten Pflichten zu unterstützen; insbesondere den Auftraggeber unverzüglich über Verletzungen des Schutzes personenbezogener Daten zu informieren (Art. 28 Abs. 3 lit. f in Verbindung mit Art. 33 Abs. 2 DSGVO) und bei der Datenschutzfolgenabschätzung gemäß Art. 35, 36 DSGVO unterstützen und dem Auftraggeber hierfür alle, ihm vorliegenden relevanten Informationen zur Verfügung zu stellen;
- für Zwecke der Auswahl durch den Auftraggeber und der Kontrollen und Überprüfungen seines Verhaltens, nachzuweisen, dass er die von dem Auftraggeber geforderten hinreichenden Garantien (Art. 28 Abs. 1 DSGVO) bieten kann, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO erfolgt und dass der Schutz der Rechte der betroffenen Person gewährleistet wird (Art. 28 Abs. 3 lit. h DSGVO);
- den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf die Auftragsverarbeitung beziehen, informieren; auch soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei dem Auftragsverarbeiter ermittelt;
- soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person, eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, nach besten Kräften bei der Abwehr solcher Haftungsansprüche zu unterstützen und insbesondere sämtliche hierfür erforderlichen Informationen zur Verfügung zu stellen;
- soweit der Auftragnehmer seinen Sitz außerhalb der EU hat, hat er schriftlich einen Vertreter zu benennen (Art. 27 Abs. 1 DSGVO) und dem Auftraggeber den Vornamen, Namen, die Organisationseinheit, Telefonnummer und die E-Mail-Adresse des Vertreters mitzuteilen.

§ 7 - Einschaltung von Subunternehmern

(1) Grundsätze für die Einschaltung von Subunternehmern

Die Einschaltung von Subunternehmern ist nur mit vorheriger schriftlicher Genehmigung des Auftraggebers gestattet. In diesem Fall wird der Auftragnehmer mit dem Subunternehmer eine Vereinbarung nach Maßgabe des Art. 28 Abs. 2–4 DSGVO abschließen. Auf Verlangen des Auftraggebers wird der Auftragnehmer diesem eine Kopie dieser Vereinbarung vorlegen. Der Auftraggeber wird die Genehmigung nicht unbillig verweigern.

(2) Anforderungen an die Einschaltung von Subunternehmern

Schaltet der Auftragnehmer mit Zustimmung des Auftraggebers oder aufgrund der allgemeinen schriftlichen Genehmigung des Auftraggebers Subunternehmer ein, so wird der Auftragnehmer seine vertraglichen Vereinbarungen mit den Subunternehmern so gestalten und entsprechend dokumentieren, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit wie sie im Verhältnis zwischen dem Auftragnehmer und dem Auftraggeber bestehen, entsprechen (Art. 28 Abs. 4 DSGVO). Zudem sind ihm die gleichen Pflichten aufzuerlegen, die dem Auftragnehmer nach den gesetzlichen Vorschriften und nach den Regelungen dieser Vereinbarung zur Auftragsverarbeitung treffen. Insbesondere hat er den Subunternehmer im Falle, dass dieser seinerseits ein weiteres Unterauftragsverhältnis eingeht, dazu zu verpflichten, seine Zustimmung und die Zustimmung des Verantwortlichen, einzuholen.

(3) Kontrollrechte des Auftraggebers

Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung zur Auftragsverarbeitung zur Feststellung, ob der Subunternehmer geeignete technische und organisatorische Maßnahmen ergriffen hat, die sicherstellen, dass die Datenverarbeitung durch ihn den Anforderungen der DSGVO entspricht, einzuräumen. Der Auftraggeber ist zu diesem Zweck berechtigt, Auskunft über den Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen. Der Auftragnehmer kann dem Auftraggeber die Umsetzung geeigneter technischer und organisatorischer Maßnahmen zur Erfüllung der Anforderungen der DSGVO auch durch Einhaltung von genehmigten Verhaltensregeln im Sinne von Art. 40 DSGVO und/oder Zertifizierungen im Sinne von Art. 42 DSGVO nachweisen.

(4) Weitergabe personenbezogener Daten an den Subunternehmer

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Leistungen außerhalb der EU/des EWR

Erbringt der Subunternehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

§ 8 - Kontroll- und Zutrittsrechte des Auftraggebers, Mitwirkungspflichten des Auftragnehmers

(1) Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen

Im Hinblick auf die Nachweispflichten des Auftraggebers nach Art. 5 Abs. 2 DSGVO und dessen Überprüfungsrechte nach Art. 28 Abs. 3 Satz 2 lit. h DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit dieser Vereinbarung zur Auftragsverarbeitung stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

(2) Überprüfungen beim Auftragnehmer

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die dem Auftragnehmer rechtzeitig anzukündigen sind, von der Einhaltung dieser Vereinbarung zur Auftragsverarbeitung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur die konkrete Auftragsverarbeitung betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (zum Beispiel Wirtschaftsprüfer, Revision, Datenschutzbeauftragter);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (zum Beispiel nach BSI-Grundschutz).

(3) Zutrittsrechte

Der Auftragnehmer verpflichtet sich, dem betrieblichen Datenschutzbeauftragten des Auftraggebers jederzeit Zutritt zu den Datenverarbeitungsanlagen zu gewähren und ihm zu ermöglichen, die Einhaltung der Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung und der datenschutzrechtlichen Bestimmungen zu überprüfen.

§ 9 - Mitzuteilende Verstöße

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 33, 34 DSGVO genannten Pflichten zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde (Art. 33 DSGVO) und zur Benachrichtigung der betroffenen Personen (Art. 34 DSGVO).

Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten durch ihn oder durch die bei ihm beschäftigten Personen unverzüglich, sobald ihm diese bekannt werden. Der Auftragnehmer hat ein Data Breach Notification Management

System implementiert, das eine unverzügliche Meldung an den Auftraggeber sicherstellt.

(2) Dem Auftragnehmer ist bekannt, dass nach Art. 33 Abs. 2 DSGVO Informationspflichten im Falle einer Verletzung personenbezogener Daten bestehen. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Insbesondere ist der Auftragnehmer verpflichtet, unverzüglich die Ursache für die Verletzung des Schutzes personenbezogener Daten zu beseitigen. Soweit den Auftraggeber Pflichten nach Art. 33 Abs. 1 oder 34 Abs. 1 DSGVO treffen, wird der Auftragnehmer ihn hierbei vollumfänglich unterstützen, insbesondere dem Auftraggeber eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie eine Beschreibung der von ihm ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen geben, damit der Auftraggeber seinen gesetzlichen Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO gegenüber der Aufsichtsbehörde und den betroffenen Personen nachkommen kann. Der Auftraggeber als Verantwortlicher bleibt gegenüber der Aufsichtsbehörde und den betroffenen Personen allein im Sinne der Art. 33, 34 DSGVO verantwortlich. Er entscheidet deswegen alleine, ob aufgrund der ihm vom Auftragnehmer über einen Vorfall zur Verfügung gestellten Informationen eine Benachrichtigung der Aufsichtsbehörde und ggf. der Betroffenen erfolgen muss oder im Ausnahmefall unterbleiben kann. Er ist allein für die Einhaltung der 72-Stunden-Frist des Art. 33 Abs. 1 DSGVO verantwortlich. Der Auftraggeber haftet alleine und vollumfänglich, sollte er eine erforderliche Meldung im vorgenannten Sinne trotz unverzüglicher Information durch den Auftragnehmer unterlassen oder die 72-Stunden-Frist versäumt haben.

§ 10 - Weisungsbefugnisse

(1) Weisungen des Auftraggebers

Der Auftragnehmer wird Weisungen des Auftraggebers, die sich auf die Beachtung der einschlägigen datenschutzrechtlichen Bestimmungen sowie Zweck und Ziel der Verarbeitung beziehen, beachten. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person wird die personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers, einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, verarbeiten und nutzen. Etwas anderes gilt nur dann, wenn der Auftragnehmer durch das Recht der Union oder des Mitgliedsstaates, in dem er seinen Sitz hat, hierzu verpflichtet ist (Art. 28 Abs. 3 Satz 2 lit. a, Art. 29 DSGVO). In diesem Fall wird der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mitteilen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet, Art. 28 Abs. 3 Satz 2 lit. a DSGVO.

Der Auftraggeber behält sich im Rahmen der im Vertragswerk getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang, Ziele und Zweck der Datenverarbeitung vor. Dieses kann der Auftraggeber durch Einzelweisungen konkretisieren. Hinsichtlich der Mittel der Datenverarbeitung werden sich die Parteien abstimmen, ob und inwieweit die technisch-organisatorischen Maßnahmen durch oder mit dem Auftraggeber bestimmt werden. Weisungen, Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich oder in einem elektronischen Format zu dokumentieren (Art. 28 Abs. 3 Satz 2 lit. a, Art. 29 DSGVO). Auskünfte an Dritte oder betroffene Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung oder elektronischer Zustimmung des Auftraggebers erteilen. Die Zustimmung ist zu dokumentieren.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format bestätigen. Im Übrigen erteilt der Auftraggeber alle Aufträge, Teilaufträge und Weisungen grundsätzlich schriftlich oder in einem dokumentierten elektronischen Format. Der Auftragnehmer hat die Weisung des Auftraggebers zu dokumentieren und in geeigneter Weise festzuhalten. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Dem Auftragnehmer ist bekannt, dass er selbst als Verantwortlicher gilt, wenn er von der vertraglichen Vereinbarung oder den Weisungen des Verantwortlichen abweicht. Sollte er der Meinung sein, dass Weisungen des Auftraggebers rechtswidrig sind, gilt § 10 (3) unten.

(2) Hinweispflicht

Sofern der Auftragnehmer der Auffassung ist, dass die Ausführung von Weisungen des Auftraggebers, auch von solchen, in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, zu einer Verletzung von Datenschutzbestimmungen führen könnte oder rechtswidrig ist, ist er verpflichtet, den Auftraggeber hierauf unverzüglich, vor der Verarbeitung bzw. Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation hinzuweisen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen des Auftraggebers bestätigt oder geändert wird. Wenn und soweit die Aussetzung zu Unrecht erfolgte, behält sich der Auftraggeber vor, etwaigen ihm hieraus resultierenden Schaden geltend zu machen. Die Weisung des Auftraggebers und die Ablehnung des Auftragnehmers sind zu dokumentieren.

§ 11 - Rückgabe von Datenträgern und Löschung von Daten

(1) Löschung von Daten

Mit Beendigung des Auftrags oder vorher auf Verlangen des Auftraggebers ist der Auftragnehmer verpflichtet, dem Auftraggeber sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie die in Zusammenhang mit dem Vertragsverhältnis und dieser Vereinbarung zur Auftragsverarbeitung stehenden Datenbestände auszuhändigen oder nach vorheriger Zustimmung des

Auftraggebers datenschutzgerecht zu löschen oder zu vernichten (Art. 28 Abs. 3 Satz 2 lit. g DSGVO). Für Test- und Ausschussmaterial gilt dies nur dann, wenn der Auftraggeber dies ausdrücklich verlangt. Nach Beendigung des Auftragsverhältnisses dürfen keinerlei personenbezogene Daten bei dem Auftragnehmer verbleiben. Die Verpflichtung gilt nicht, sofern der Auftragnehmer nach dem Unionsrecht oder dem Recht des Mitgliedstaates, in dem er seinen Sitz hat, zur Aufbewahrung personenbezogener Daten verpflichtet ist. Das Protokoll der Löschung bzw. Vernichtung ist dem Auftraggeber vorzulegen. Entsprechendes gilt für die Versicherung der vollständigen Aushändigung sämtlicher in Zusammenhang mit dem Vertragsverhältnis und dieser Vereinbarung zur Auftragsverarbeitung stehenden Unterlagen sowie Verarbeitungs- und Nutzungsergebnisse.

(2) Aufbewahrungspflichten

Der Auftragnehmer ist berechtigt, Dokumentationen, die er benötigt, um die Auftrags- und ordnungsgemäße Datenverarbeitung nachweisen zu können, gemäß den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie dem Auftraggeber zu seiner Entlastung bei Vertragsende übergeben.

§ 12 - Haftung, Freistellung und Vertragsstrafen

(1) Haftung der Parteien im Außenverhältnis

(a) Haftung

Im Verhältnis zu den betroffenen Personen haften der Auftraggeber und der Auftragnehmer für Schäden, die aus einer schuldhaften Verletzung von Datenschutzbestimmungen im Rahmen der Durchführung des Vertragsverhältnisses oder dieser Vereinbarung zur Auftragsverarbeitung durch den Auftragnehmer, die bei ihm beschäftigten Personen oder durch von ihm nach Maßgabe von § 7 eingeschalteten Subunternehmer entstehen.

(b) Freistellung durch den Auftragnehmer

Macht eine betroffene Person gegenüber dem Auftraggeber Schadensersatzansprüche wegen der Verletzung von Datenschutzbestimmungen, insbesondere der DSGVO oder des BDSG, oder einer ansonsten unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Vertragsverhältnisses der Parteien oder dieser Vereinbarung zur Auftragsverarbeitung geltend, stellt der Auftragnehmer den Auftraggeber bei einer schuldhaften Pflichtverletzung frei. Ist der Auftraggeber zum Schadensersatz verpflichtet, kann er bei dem Auftragnehmer Rückgriff nehmen. Der Auftragnehmer ist jedoch in einem solchen Fall zu dem Nachweis berechtigt, dass der den betroffenen Personen entstandene Schaden nicht durch eine Pflichtverletzung des Auftragnehmers, der bei ihm beschäftigten Personen oder von ihm nach Maßgabe von § 7 eingeschaltete Subunternehmer schuldhaft verursacht wurde.

(2) Haftung des Auftragnehmers

(a) Haftung des Auftragnehmers gegenüber betroffenen Personen

Im Verhältnis zu den betroffenen Personen haftet der Auftragnehmer für Schäden, die diesen aus einer schuldhaften Verletzung einer ihm speziell nach den Regelungen der DSGVO oder dieser Vereinbarung zur Auftragsverarbeitung auferlegten Pflicht, entstehen. Dies gilt weiter bei der Nichtbeachtung einer rechtmäßig erteilten Weisung des Auftraggebers oder wenn der Auftragnehmer entgegen einer Weisung des Auftraggebers gehandelt hat.

Der Auftragnehmer haftet auch gegenüber den betroffenen Personen, wenn einer der bei ihm beschäftigten Personen oder ein durch ihn beauftragter Subunternehmer schuldhaft eine auferlegte Pflicht verletzt und hierdurch ein Schaden für die betroffenen Personen entstanden ist.

(b) Haftung des Auftragnehmers gegenüber dem Auftraggeber

Dem Auftraggeber gegenüber haftet er, wenn er selbst oder die nach § 7 eingeschalteten Subunternehmer die ihnen obliegenden Pflichten nicht einhalten. Er stellt den Auftraggeber insoweit bei einer schuldhaften Pflichtverletzung von sämtlichen Schadensersatzansprüchen frei, die die betroffenen Personen gegenüber dem Auftraggeber wegen der Verletzung einer solchen Pflicht geltend machen. § 12 (1)(b) gilt entsprechend. Der Auftragnehmer ist jedoch berechtigt, nachzuweisen, dass der der betroffenen Person entstandene Schaden nicht durch eine Pflichtverletzung einer der bei ihm beschäftigten Personen oder eines von ihm nach Maßgabe des § 7 eingeschalteten Subunternehmers schuldhaft verursacht wurde.

(3) Haftung beider Parteien und Rückgriff im Innenverhältnis

Werden sowohl der Auftraggeber als auch der Auftragnehmer von einer betroffenen Person auf Schadensersatz wegen der Verletzung von Pflichten nach der DSGVO oder dem BDSG in Anspruch genommen, bestimmt sich die Haftung der Parteien im Innenverhältnis danach, inwieweit die eine und/oder die andere Partei den Schaden verursacht hat. Sie kann gegen die jeweils andere Partei in Höhe des von dieser verursachten Schadens Rückgriff nehmen, wenn und soweit sie den vollen Schadensersatz an die betroffene Person geleistet hat.

(4) Vertragsstrafen

Für Verstöße gegen die Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung, wie insbesondere gegen die Verpflichtung zur Bestellung eines Datenschutzbeauftragten nach § 6 Abs. 1 oder die Verpflichtung, gemäß § 6 Abs. 2 die mit der Datenverarbeitung im Sinne dieser Vereinbarung zur Auftragsverarbeitung bei ihm beschäftigten Personen auf das Datengeheimnis nach § 53 BDSG bzw. zur Vertraulichkeit zu verpflichten, oder bei Änderung der technisch-organisatorischen Maßnahmen nach § 4 Abs. 4 ohne die erforderliche Abstimmung mit dem Auftraggeber oder Beauftragung von Subunternehmern ohne Einhaltung der Anforderungen des § 7 sowie bei Nichtbeachtung von Weisungen des Auftraggebers zahlt der Auftragnehmer an den Auftraggeber eine Vertragsstrafe. Weitergehende Schadensersatzansprüche des Auftraggebers sowie das Recht, diese Vereinbarung in einem solchen Fall nach § 1 Abs. 3 fristlos zu kündigen, bleiben hiervon unberührt. Dem Auftragnehmer steht jedoch die Möglichkeit offen, nachzuweisen, dass die Ausführung von Weisungen des Auftraggebers zu einer Verletzung von Datenschutzbestimmungen geführt hätte oder rechtswidrig war und er den Auftraggeber hierauf unverzüglich nach § 10 (3) hingewiesen hat.

Ebenso ist der Auftragnehmer berechtigt, nachzuweisen, dass er die Daten nach dem Recht der Union oder dem Recht des Mitgliedstaates, in dem er seinen Sitz hat, verarbeitet hat, er hierzu verpflichtet war und er dies dem Auftraggeber nach § 10 (1) vor der Verarbeitung der personenbezogenen Daten mitgeteilt hat.

Anlage 1 - Technische und organisatorische Maßnahmen

Einleitung

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO der Digistore24 GmbH mit Stand 01.05.2018.

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1 - Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1a - Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische und organisatorische Maßnahmen
Der Zugang zum Büro ist nur mit einem Schlüssel möglich.
Schlüssel werden nur von berechtigten Personen verwaltet.
Schlüssel werden nur an berechtigte Personen vergeben.
Produkt-Server-Systeme unserer Anwendungen (intern und extern) stehen in gesicherten Rechenzentren bei Anexia.
Unsere Produkt-Email-Server stehen in gesicherten Rechenzentren bei HostEurope.

1b - Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische und organisatorische Maßnahmen
Login mit Benutzername + Passwort
Anti-Virus-Software Clients
Firewall
Rechner sind verschlüsselt
Auf Kundendaten kann nur per Remote Desktop zugegriffen werden
Einsatz VPN bei Remote-Zugriffen
Verwalten von Benutzerberechtigungen
Richtlinie „Sicheres Passwort“
Anleitung "PC-Einstellungen“

1c - Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische und organisatorische Maßnahmen
Aktenschredder (mind. Stufe 3, cross cut)
Verwaltung der Benutzerrechte durch Administratoren

1d - Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische und organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung
Physikalische Trennung (Systeme/Datenbanken/Datenträger)
Mandantenfähigkeit relevanter Anwendungen
Verwaltung der Benutzerrechte durch Administratoren

2 - Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2a - 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische und organisatorische Maßnahmen
Email-Verschlüsselung
Einsatz VPN bei Remote-Zugriffen
Ausschließliche Nutzung von verschlüsselten Verbindungen wie sftp, https
Sorgfältige Auswahl aller Dienstleister

2b - 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische und organisatorische Maßnahmen
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3 - Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3a - Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische und organisatorische Maßnahmen
Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
Backup & Recovery-Konzept
Kontrolle des Sicherungsvorgangs
Serverraum klimatisiert
Schutzsteckdosenleisten im Serverraum
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum
RAID System / Festplattenspiegelung
Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)

4 - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4a - Datenschutz-Management

Technische und organisatorische Maßnahmen
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (https://doc.digistore24-team.com)
Externer Datenschutzbeauftragter: Marion Albrecht, Rechtsanwältin und Fachanwältin für IT Recht von der Kanzlei activeLAW Klein.Offenhausen.PartmbB Hans-Böckler-Allee 26 D-30173 Hannover Email: datenschutz@digistore24.com

4b - Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische und organisatorische Maßnahmen
Einsatz von Virenscanner und regelmäßige Aktualisierung
Einsatz von Firewall und regelmäßige Aktualisierung
Einsatz von Spamfilter und regelmäßige Aktualisierung
Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)

4d - Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische und organisatorische Maßnahmen
Datenübermittlung an Auftragsverarbeiter erfolgt nur auf Grundlage einer gültigen Vereinbarung
Prüfung eines jeden Auftragsverarbeiter im Hinblick auf das Datenschutzniveau