Auftragsverarbeitungsvertrag

„LD connect für DATEV Rechnungswesen“

Erstellt am	06.05.2020
Letzte Änderung am	06.05.2020
Aktuelle Version	1.0

L & D – Lion and Deer GmbH

Heinz-Fröling-Straße 15
51429 Bergisch Gladbach
Tel. +49 (0) 2204 76797-295
info@liondeer.de

Inhalt

Auftragsverarbeitungsvertrag 2
Präambel 3
§ 1 Gegenstand/Umfang der Beauftragung 3
a. Zweck der Verarbeitung 3
b. Kategorien betroffener Personen 4
c. Kategorien personenbezogener Daten 4
§ 2 Weisungsbefugnisse des Auftraggebers 5
§ 3 Schutzmaßnahmen des Auftragnehmers 5
§ 4 Informations- und Unterstützungspflichten des Auftragnehmers 6
§ 5 Sonstige Verpflichtungen des Auftragnehmers 6
§ 6 Subunternehmerverhältnisse 7
§ 7 Kontrollrechte 7
§ 8 Rechte Betroffener 7
§ 9 Laufzeit und Kündigung 8
§ 10 Löschung und Rückgabe nach Vertragsende 8
§ 11 Haftung 8
§ 12 Schlussbestimmungen 9
Anlage TOM 10

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

Zwischen dem

Nutzer von „LD connect für DATEV Rechnungswesen“

als Verantwortliche/r - nachfolgend "**Auftraggeber**" genannt

und

L & D – Lion and Deer GmbH

Heinz-Fröling-Straße 15

51429 Bergisch Gladbach

als Auftragsverarbeiter/in - nachfolgend "**Auftragnehmer**" genannt

- Auftraggeber und Auftragnehmer nachfolgend jeder auch "Partei" und gemeinsam "Parteien" -

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen gemäß dem zwischen ihnen geschlossenen Vertrag (im Folgenden: "**Hauptvertrag**"). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("**DSGVO**"). Zur Erfüllung der Anforderungen der DSGVO an derartige Konstellationen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag, der mit Unterzeichnung des Hauptvertrages zustande kommt.

§ 1 Gegenstand/Umfang der Beauftragung

(1) Im Rahmen der Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages hat der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "**Auftraggeberdaten**"). Diese Auftraggeberdaten verarbeitet der Auftragnehmer im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

(2) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt in der folgenden Art sowie in dem dort spezifizierten Umfang und Zweck. Der Kreis der von der Datenverarbeitung betroffenen Personen wird dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

a. Zweck der Verarbeitung

- Unterstützung bei der Durchführung von Verträgen oder Aufträgen
- Vertrieb oder Versand von Waren oder Erbringung von Leistungen
- Betreuung von Kunden und Geschäftspartnern
- Kundenbefragungen im Rahmen von Markt- und Meinungsforschung
- Gewährleistung der ordentlichen und gesetzeskonformen Buchhaltung
- Rechnungsstellung für Waren oder Leistungen
- Pflege und Verwaltung von Beschäftigtendaten
- Angestelltenentwicklungsplanung
- Dokumentation von Arbeitszeiten
- Zahlung von Gehältern und Löhnen
- Planung und Verwaltung von Fortbildungs- und Trainingsmaßnahmen
- Beschäftigtenbeurteilung oder Leistungsbewertung
- Überwachung betrieblicher Einrichtungen
- Gewährleistung des Zutrittsschutzes
- Ermöglichung der Verfolgung von Straftaten
- Wahrnehmung des Hausrechts
- Gewährleistung der ordnungsgemäßen Akten- und Datenträgervernichtung
- Kommunikation mittels elektronischer Medien
- Ermöglichung der Kontaktierung von Beschäftigten
- Dokumentation von Terminen von Beschäftigten
- Zugangsverwaltung hinsichtlich Technik (einschließlich Telekommunikation, Netzwerk)
- Verwaltung von Berechtigungen
- Verwaltung von Lizenzen / Software Asset Management
- Telekommunikationskostenabrechnung
- Pflege und Verbesserung von Kommunikationsprozessen
- Reisebuchung und Reisekostenabrechnung

- Verwaltung von Kompetenzen und Qualifikationen der Beschäftigten
- Verwaltung von Bewerbungen / Onboarding
- Dokumentation und Festlegung von Compensations und Benefits für Beschäftigte
- Qualitätssicherung

b. Kategorien betroffener Personen

- Beschäftigte
- Auszubildende und Praktikanten
- Bewerber
- ehemalige Arbeitnehmer
- freie Mitarbeiter
- Gesellschafter, Organe der Gesellschaft
- Angehörige von Beschäftigten
- Kunden
- Interessenten
- Lieferanten und Dienstleister
- Mieter
- Geschäftspartner
- externe Berater
- Besucher
- Pressevertreter

c. Kategorien personenbezogener Daten

- Stammdaten (Adressen)
- Gesundheitsdaten
- Personal- und Identifikationsnummern
- Alter
- Kreditkartendaten
- Reisebuchungs- & Reiseabrechnungsdaten
- Arbeitszeitdaten
- Kundenverhaltensdaten
- Telekommunikationsabrechnungsdaten
- Audiodaten
- Lohn- und Gehaltsdaten
- Telekommunikationsverbindungsdaten
- Bankverbindung inkl. Zahlungsverkehr
- Mitarbeiterbewertungen
- Telefonnummern
- Bewerberdaten
- Beschäftigte (Qualifikationen)
- Vertragsdaten
- Bilddaten
- Namen
- Videodaten
- Hobbys
- Nutzerkennungen
- Zahlungsdaten
- E-Mails
- Passwörter
- Zugangsdaten

(3) Dem Auftragnehmer ist eine von den o.g. Festlegungen abweichende Verarbeitung von Auftraggeberdaten untersagt.

(4) Die Verarbeitung der Auftraggeberdaten findet grds. ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Sollte es eine Verlagerung der Auftragsverarbeitung in ein Drittland geben, bedarf dies der vorherigen Zustimmung des Auftraggebers und erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Der Auftraggeber stimmt bereits bei Abschluss dieses Auftragsverarbeitungsvertrages der Verarbeitung personenbezogener Daten durch die unten genannten Subunternehmen zu.

(5) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen. Gleiches gilt für alle Tätigkeiten, bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit Auftraggeberdaten in Berührung kommen.

§ 2 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten im Rahmen der Beauftragung und im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber hat das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "**Weisungsrecht**"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich oder in elektronischer Form (E-Mail ausreichend) erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer in elektronischer Form zu bestätigen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

§ 3 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden "**Mitarbeiter**" genannt), zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO). Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in **Anlage 1** zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der technischen und organisatorischen Maßnahmen nachweisen.

§ 4 Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte, wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 48 Stunden in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Diese Meldungen sollten jeweils zumindest die in Art. 33 Absatz 3 DSGVO genannten Angaben enthalten.

(2) Der Auftragnehmer wird den Auftraggeber im o.g. Falle bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Anforderung innerhalb angemessener Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

§ 5 Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist, sofern die Voraussetzungen des Art. 30 DSGVO auf ihn zutreffen, verpflichtet ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.

(3) Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat. Aufgrund der Unternehmsgröße ist dies momentan nicht notwendig. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber mitzuteilen.

(4) Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

§ 6 Subunternehmerverhältnisse

(1) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von Unterauftragsverhältnissen mit Subunternehmern ("**Subunternehmerverhältnis**") befugt. Der Auftragnehmer hat dafür Sorge zu tragen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den von ihm beauftragten Subunternehmen gelten, wobei dem Auftraggeber gegenüber dem Subunternehmer sämtliche Kontrollrechte gemäß dieses Vertrages einzuräumen sind.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

(3) Der Auftragnehmer hat mit folgenden Unternehmen Subunternehmerverhältnisse begründet, denen der Auftraggeber mit Abschluss dieses Auftragsverarbeitungsvertrages zustimmt:

- AWS, inc

§ 7 Kontrollrechte

(1) Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages zu überzeugen. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO. Er wird dem Auftraggeber unverzüglich, spätestens aber innerhalb von 14 Werktagen, die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftraggeber nicht selbst über die entsprechenden Informationen verfügt.

(2) Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DSGVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich, spätestens binnen einer Frist von 7 Werktagen zu berichtigen, löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

§ 9 Laufzeit und Kündigung

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragsnehmer für eine Dauer von 6 Monaten aufzubewahren und auf Verlangen an den Auftragsgeber herauszugeben.

(2) Der Auftragnehmer wird dem Auftraggeber die Löschung elektronisch bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

§ 11 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 12 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der elektronischen Form.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

Anlagen

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO)

Anlage TOM

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO

Die Parteien treffen zum Auftragsverarbeitungsvertrag und der DSGVO-Compliance der Subunternehmer ergänzend folgende Festlegungen über die vom Auftragnehmer umzusetzenden technischen und organisatorischen Maßnahmen:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu den Büroräumen des Auftragnehmers haben:

☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)

☐ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)

☐ Zaunanlagen

☐ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe

☐ Alarmanlage

☐ Videoüberwachung

☐ Spezielle Schutzvorkehrungen des Serverraums

☐ Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und anderen Datenträgern

☐ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Begleitung nach dem Besuch bis zum Ausgang)

Zugangskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu den Büroräumen des Auftragnehmers haben:

☐ Persönlicher und individueller Login bei Anmeldung am System/Netzwerk

☐ Autorisierungsprozess für Zugangsberechtigungen

☐ Begrenzung der befugten Benutzer

☐ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)

☐ Protokollierung des Zugangs

☐ Zusätzlicher Login für bestimmte Anwendungen

☐ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität

☐ Firewall

Zugriffskontrolle

Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

☐ Verwaltung und Dokumentation von differenzierten Berechtigungen

☐ Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von Daten Gegenstand der Leistung des Auftragnehmers ist.

☐ Auswertungen/Protokollierungen von Datenverarbeitungen

☐ Autorisierungsprozess für Berechtigungen

☐ Genehmigungsroutinen

☐ Profile/Rollen

☐ Verschlüsselung von Datenträgern

☐ Funktionstrennung (Segregation of Duties)

☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399

☐ Nicht-reversible Löschung von Datenträgern

Trennungskontrolle

Folgende stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken

☐ Verarbeitung auf mindestens logisch getrennten Systemen

☐ Zugriffsberechtigungen nach funktioneller Zuständigkeit

☐ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

☐ Mandantenfähigkeit von IT-Systemen

☐ Verwendung von Testdaten

☐ Trennung von Entwicklungs- und Produktionsumgebung

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung von Daten erfolgt so, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

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

Weitergabekontrolle

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

☐ Verschlüsselung von Datenträgern

☐ Gesicherter File Transfer oder sonstiger Datentransport

☐ Physikalische Transportsicherung

☐ Verpackungs- und Versandvorschriften

☐ Qualifizierte elektronische Signatur

☐ Verschlüsseltes WLAN

Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

☐ Zugriffsrechte

☐ Systemseitige Protokollierungen

☐ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

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

Durch folgende Maßnahmen ist sichergestellt, dass Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Kunden stets verfügbar sind:

☐ Sicherheitskonzept für Software- und IT-Anwendungen

☐ Backup-Verfahren

Des Weiteren verweisen wir hier auf die DSGVO Compliance von AWS (Amazon Webservices), welcher als Subunternehmer den Betrieb der Serverumgebung in der Region Frankfurt übernimmt.

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

Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

☐ Benennung eines Datenschutzbeauftragten, soweit erforderlich

☐ Verpflichtung der Mitarbeiter auf die Vertraulichkeit

☐ Hinreichende Schulungen der Mitarbeiter im Datenschutz

☐ Führen eines Verzeichnisses von Verarbeitungstätigkeiten, soweit erforderlich (Art. 30 DSGVO)

☐ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

☐ Externe Prüfung oder Auditierung

Management bei Datenschutzverletzungen

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)

☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber betroffenen Personen (Art. 34 DSGVO)

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Kunden verarbeitet werden:

☐ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien

☐ Prozess zur Erteilung und/oder Befolgung von Weisungen

☐ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung

☐ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter

☐ Unabhängige Auditierung der Weisungsgebundenheit

☐ Verpflichtung der Beschäftigten auf die Vertraulichkeit

☐ Vereinbarung von Vertragsstrafen für Verstöße gegen Weisungen

☐ formalisiertes Auftragsmanagement