Vertrag zur Auftragsbearbeitung gemäss Art. 9 DSG (CH) / 28 DSGVO (EU)

Vereinbarung

zwischen

Kunden der Dreier AG

Verantwortliche – nachstehend Auftraggeber genannt –

und

Dreier AG Transport•Logistik
Bahnhofstrasse 1A
5034 Suhr
Schweiz

Auftragsbearbeiter – nachstehend Auftragnehmer genannt

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der in ihren Einzelheiten beschriebenen Auftragsdatenbearbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit Personendaten des Auftraggebers in Berührung kommen können.

Auftragsdatenbearbeitungsvertrag (AV)

§ 1 Definitionen

(1) Hauptvertrag

Unter dem Hauptvertrag wird der Vertrag zwischen dem Auftraggeber und dem Auftragnehmer verstanden, welcher die Leistungserbringung des Auftragsnehmer regelt. Untenstehend auch Leistungsvertrag genannt.

(2) Unterauftragnehmer

Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

(3) Definitionen nach Datenschutzgesetz

Es gelten allgemein die Definitionen nach DSG Art. 5

§ 2 Gegenstand und Dauer der Bearbeitung

(1) Gegenstand

Der Gegenstand der Vereinbarung ergibt sich aus dem aktuell gegenständlichen Leistungsvertrag und allen folgenden Leistungsverträgen, die zwischen dem Auftragnehmer und Auftraggeber zukünftig zum vergleichbaren Vertragsgegenstand geschlossen werden.

(2) Dauer

Die Dauer dieser Vereinbarung entspricht der Laufzeit der Leistungsvereinbarung gemäss dem unterzeichneten Hauptvertrag.

§ 3 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer bearbeitet Personendaten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmässigkeit der Datenbearbeitung allein verantwortlich.

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Die Weisungen sind vom Auftragnehmer, sowie vom Auftraggeber schriftlich zu dokumentieren.

(3) Der Auftragnehmer muss gewährleisten, dass sich die zur Bearbeitung der Personendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf Personendatendes Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit mit Wirkung für die Zukunft fortbesteht.

(4) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu bearbeitenden Daten, für die die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze, verantwortlich.

§ 4 Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die weisungsberechtigten Personen sind in Anlage 2 aufgeführt.

(2) 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.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 19 bis 24 des DSG und 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit der Personendaten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Massnahmen, die die Umstände und Zwecke der Bearbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

b. die Verpflichtung, Verletzungen der Personendaten unverzüglich an den Auftraggeber zu melden.

c. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

(2) Auf Anfrage des Auftraggebers stellt der Auftragsbearbeiter dem Auftraggeber alle Angaben zur Verfügung, die zur Führung eines Verzeichnisses von Bearbeitungstätigkeiten benötigt werden

a. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

b. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kommt der Auftraggeber seiner Unterstützungspflicht nach. Der Auftragnehmer muss auf jeden Fall in Vorleistung gehen.

(4) Die Erhebung, Bearbeitung oder Nutzung von Daten ausserhalb fest umschlossener Räumlichkeiten einer Niederlassung des Auftragnehmers ist nicht gestattet. Hiervon ausgenommen ist die E-Mail- Kommunikation im Rahmen der üblichen Geschäftskorrespondenz (Handels- und Geschäftsbriefe, auch Anweisungen in Textform).

(5) Sollten die Personendaten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschliesslich beim Auftraggeber als „verantwortliche Stelle“ im Sinne der DSG / DSGVO liegen.

§ 6 Technische und organisatorische Massnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Massnahmen vor Beginn der Bearbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Massnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit nach DSG oder DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Massnahmen um Massnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Bearbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

(3) Die Festlegung des Schutzniveaus obliegt dem Auftraggeber und wird anhand der Kriterien in Anlage 1 festgelegt.

(4) 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.

§ 7 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Angaben hinsichtlich der Bestellung eines Datenschutzbeauftragen, der Ansprechpartner und den weisungsberechtigten Personen finden sich in Anlage 2.

b) Die Wahrung der Vertraulichkeit gemäss DSG / DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu Personendaten hat, dürfen diese Daten ausschliesslich entsprechend der Weisung des Auftraggebers bearbeiten einschliesslich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Bearbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Massnahmen [siehe Anlage 4].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer ist jedoch verpflichtet, vor Tätigwerden eine schriftliche Zustimmung durch den Auftraggeber einzuholen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Bearbeitung Personendaten bei der Auftragsbearbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsbearbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmässig die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Bearbeitung in seinem

Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 6 dieses Vertrages.

i) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 8 Unterauftragsverhältnisse

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, die im Hauptvertrag und/oder im Anhang benannten, weitere Auftragsbearbeiter (Unterauftragnehmer) einschaltet. Über eine Änderung der genannten Unterauftragnehmer wird der Auftragnehmer den Auftraggeber informieren und ihm die Möglichkeit geben, gegen derartige Änderungen einen Einspruch zu erheben.

(2) Im Übrigen ist die Beauftragung von Unterauftragnehmern durch den Auftragnehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig. Die Zustimmung darf nur aus wichtigem, dem Auftragnehmer nachzuweisendem Grund verweigert werden. Im Fall der Einschaltung von mit dem Auftragnehmer nahestehenden Personen (Unternehmen) als Unterauftragnehmer, erteilt der Auftraggeber hiermit schon jetzt ausdrücklich seine Zustimmung.

(3) Der Auftragnehmer wird weiteren Auftragsbearbeitern vertraglich dieselben Pflichten wie nach diesem Vertrag auferlegt, einschliesslich hinreichender Garantie dafür, dass die geeigneten technischen und organisatorischen Massnahmen so durchgeführt werden, dass die Bearbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten, datenschutzbezogenen Vertragsunterlagen. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

§ 9 Kontrollrecht des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 9 DSG oder 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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß DSG / DSGVO.

§ 10 Berechtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag bearbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Bearbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den

Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt und sind streng untersagt. Hierfür bedarf es einer vorherigen schriftlichen Genehmigung des Auftraggebers. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenbearbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(4) Nach Abschluss der Erbringung der Bearbeitungsleistungen muss der Auftragnehmer alle Personendaten nach Wahl des Auftraggebers entweder löschen oder diesem zurückgeben, sofern nicht nach dem schweizerischen Recht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der Personendaten besteht. Gleiches gilt für alle Daten, die Betriebs- oder Geschäftsgeheimnisse des Auftraggebers beinhalten. Das Protokoll der Löschung ist auf Anforderung vorzulegen und dauerhaft aufzubewahren.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Datenbearbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(6) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostentragung.

(7) Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

(8) Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer

a) sämtliche im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger,

b) erstellte Bearbeitungsergebnisse,

c) Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen

dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

§ 11 Leistungsort

(1) Die Erbringung der vertraglich vereinbarten Datenbearbeitung findet ausschliesslich in der Schweiz, einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung in einen Drittstaat, ausserhalb der EU/EWR, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die gesetzlichen Voraussetzungen erfüllt sind.

(2) Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

(4) Wird die Datenbearbeitung nach dieser und den gesetzlichen Vorgaben zur Bearbeitung der Personendaten im Auftrag bzw. zur Übermittlung der Personendaten in das Ausland ausserhalb der Schweiz erbracht, ist der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei grenzüberschreitendem Datenverkehr verantwortlich.

§ 12 Haftung

(1) Eine zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsbearbeitung, ausser soweit ausdrücklich etwas anderes vereinbart.

(2) Der Auftragnehmer haftet dabei ausschliesslich für Schäden, die auf einer von ihm durchgeführten Bearbeitung beruhen, bei der

a) er den aus dem DSG / DSGVO resultierenden und speziell für Auftragsbearbeiter auferlegten Pflichten nicht nachgekommen ist oder

b) er unter Nichtbeachtung der rechtmässig erteilten Anweisungen des Auftraggebers handelte oder

c) er gegen die rechtmässig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Ebenso haftet der Auftragnehmer für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

(4) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer nur dann vorbehalten, wenn ein Verschulden des Auftragnehmers nachweislich vorliegt.

§ 13 Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschliesslich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt.

§ 14 Salvatorische Klausel

(1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(2) 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.

(3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedacht Werdens vereinbart worden wären.

(4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter § 13 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Personendaten im Sinne dieses Vertrages am besten gewährleistet.

§ 15 Rechtswahl, Gerichtsstand

(1) Es gilt Schweizer Recht

(2) Gerichtsstand ist der Kanton Aargau, Sitz des Auftragnehmers

Anlagen

Anlage 1: Art und Schutzniveau der betroffenen Daten

Anlage 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Anlage 3: Unterauftragsverhältnis beim Auftragnehmer

Anlage 1: Auftragsspezifizierung

1. Datenarten

Folgende Datenarten sind Gegenstand dieses Auftrags (*die massgeblichen Datenarten sind von der verantwortlichen Person des Auftraggebers anzukreuzen bzw. zu ergänzen*):

☒ Abrechnungsdaten
☒ Adressdaten
☐ Arbeitszeitendaten
☒ Bankverbindungsdaten & Kontodaten
☒ E-Mails
☒ Finanzdaten
☒ Gesprächshistorie
☒ Kontaktdaten
☐ Mitarbeiterdaten
☐ Nutzerkennung
☐ Passwörter
☒ Telefonnummern
☐ Transaktionsdaten
☒ Vertragsdaten
☐ Videoaufzeichnungen
☒ Zahlungsdaten

Weitere:
☐
☐
☐
☐
☐

2. Betroffene

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags (*die massgeblichen Kreise von Betroffenen sind von der verantwortlichen Person des Auftraggebers anzukreuzen bzw. zu ergänzen)*:

☐ Auszubildende
☒ Kunden
☐ Mitarbeitende

Weitere:
☐
☐
☐

Anlage 2: Technische und organisatorische Massnahmen

Im Folgenden werden, die auf dem Datenschutzgesetz basierenden technischen und organisatorischen Massnahmen beschrieben, die konkret vom Auftragnehmer im Zusammenhang mit der Bearbeitung der Personendaten und der Erfüllung seiner Verpflichtungen gemäss dem Hauptvertrag einschliesslich diesem Vertrag als Mindestvorkehrungen zu ergreifen sind, um ein dem Risiko angemessenes Schutzniveau hinsichtlich des Datenschutzes und der Datensicherheit der überlassenen Daten zu gewährleisten. Auf Verlangen des Auftraggebers muss der Auftragnehmer seien technische und organisatorischen Massnahmen aufzeigen.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Massnahmen, die gewährleisten, dass der Zutritt für Unbefugte in die Räumlichkeiten der Datenbearbeitungsanlagen, mit denen Personendaten bearbeitet oder genutzt werden, verwehrt sind:

Technische Massnahmen	Organisatorische Massnahmen
▪ Alarmanlage ▪ Elektronisches Schliesssystem ▪ Manuelles Schliesssystem ▪ Sicherheitsschlösser ▪ Datenschutzkonforme Videoüberwachung	▪ Besucher nur in Begleitung mit einem Mitarbeitenden ▪ Besucheranmeldung mit Empfangspersonal ▪ Schlüssel- und Chipkartenregelung (Schlüssel-/Chipausgabe und -vergabe, etc.) ▪ Sorgfalt bei der Auswahl des Reinigungsdienst

1.2. Zugangskontrolle

Massnahmen, die gewährleisten, dass Datenbearbeitungssysteme (Computer, Laptop) nicht von Unbefugten genutzt werden können.

Technische Massnahmen	Organisatorische Massnahmen
▪ Anti-Viren-Software ▪ Einsatz von einer sicheren VPN-Verbindung bei Remote-Zugriffen ▪ Automatische Desktopsperre ▪ Verschlüsselung von Datenträgern und mobilen Endgeräten ▪ Sperrung von USB-Anschlüssen und anderen externen Schnittstellen ▪ Authentifikation mittels Passworteingabe	▪ Richtlinie «Sicheres Passwort» (Passwortlänge, enthaltene Zeichen, Passwortwechsel) ▪ Erstellen von Benutzerprofilen ▪ Zuordnung von Benutzerprofilen ▪ Allgemeine Richtlinien zu PC- und Smartphone-Benutzung

1.3. Zugriffskontrolle

Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenbearbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen könne, und dass Personendaten bei der Bearbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Massnahmen	Organisatorische Massnahmen
▪ Datenschutzkonforme Vernichtung von Datenträgern (Akten, Laufwerke etc.) ▪ Sichere Aufbewahrung von Datenträgern ▪ Verschlüsselung von Datenträgern und mobilen Endgeräten ▪ Protokollierung der Zugriffe auf Anwendungen und Systemen	▪ Passwortregeln ▪ Berechtigungskonzepte ▪ Verwaltung der Benutzerrechte durch Administratoren ▪ Minimale Anzahl von Administratoren in den Systemen ▪

1.4. Trennungskontrolle

Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Datengetrennt bearbeitet werden können.

Technische Massnahmen	Organisatorische Massnahmen
▪ Trennung von Produktiv- und Testumgebung	▪ Steuerung über Berechtigungen ▪ Festlegung von Datenbankrechten ▪ Mandantentrennung

1.5. Pseudonymisierung

Massnahmen, die sicherstellen, dass die Identifizierung der betroffenen Personen wesentlich erschwert wird, wie z.B. durch Trennung von Daten und Identifikationsmerkmalen.

Technische Massnahmen	Organisatorische Massnahmen
▪ Trennung von Kundenstammdaten und Kundenumsatzdaten.	▪ Interne Anweisung, Personendaten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Integrität

2.1. 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 der Personendaten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Massnahmen	Organisatorische Massnahmen
▪ E-Mail-Verschlüsselung ▪ Sichere VPN-Technologie ▪ Gesicherte Transportbehälter ▪ Elektronische Signatur	▪ Einsatz von vertrauenswürdigem Transportpersonal ▪ Weitergabe in anonymisierter oder pseudonymisierter Form

2.2. Eingangskontrolle

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

Technische Massnahmen	Organisatorische Massnahmen
▪ Anfertigung eines Protokolls bezüglich der Eingabe, Veränderung und Löschung von Daten ▪ Digitales Berechtigungskonzept	▪ Vergabe von Zugriffsberechtigungen ▪ Nachvollziehbarkeit von Eingaben, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) ▪ Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

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

Technische Massnahmen	Organisatorische Massnahmen
▪ Backups ▪ Diebstahlsicherungen ▪ Serverraum klimatisiert ▪ USV (Unterbrechungsfreie Stromversorgung) ▪ Feuer- und Rauchmelder ▪ Feuerlöscher ▪ Malwareschutz und Antivirus ▪ Firewall / IDS	▪ Alarmanlage ▪ Schutz des Serverraums vor Risiken wie Hochwasser, Brände oder gefährlich platzierten Sanitäranlagen (im, oberhalb oder daneben) ▪ Erstellung von Backups der Daten ▪ Zyklus der Backups-Anfertigung ▪ Tests für Datenwiederherstellung ▪ Backup und Recovery-Konzept ist aufgestellt

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Massnahmen

Technische Massnahmen	Organisatorische Massnahmen
▪ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeitende nach Bedarf/Berechtigung.	▪ Interner Datenschutzbeauftragter bestimmt. Rainer Schüpbach +41 76 674 95 74 rainer.schuepbach@dreier.ch ▪ Mitarbeitende werden geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet. ▪ Regelmässige Sensibilisierung der Mitarbeitenden (min. jährlich). ▪ Die DSFA wird bei Bedarf durchgeführt.

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Massnahmen	Organisatorische Massnahmen
▪ Einsatz von Firewall und regelmässige Aktualisierung. ▪ Einsatz von Spamfilter und regelmässige Aktualisierung.	

4.3. Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

Technische Massnahmen	Organisatorische Massnahmen
▪ Es werden nicht mehr Personendaten erhoben, als für den jeweiligen Zweck erforderlich sind.	

Anlage 3: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Nr.	Firma	Anschrift / Land	Bearbeitungstätigkeit / Leistung
1	Brabender System GmbH	Gewerbestrasse 5a 6314 Unterägeri Schweiz	▪ Transport Management System ▪ Lagerverwaltungssystem ▪ Transport Applikation
2	Leitwerk AG	Im Ettenbach 13a 77767 Appenweiler Deutschland	▪ IT-Infrastruktur ▪ Housting und Housing
3	Sage Schweiz AG	Platz 10 6039 Root D4 Schweiz	▪ Buchhaltungssoftware
4	Remira Group GmbH	Phoenixplatz 2 44263 Dortmund Deutschland	▪ Lagerverwaltungssystem
5	Kendox AG	Bahnhof-Strasse 7 9463 Oberriet SG Schweiz	▪ Digitales Dokumentenmanagement
6	Lobster DATA GmbH	Bräuhausstrasse 1 82327 Tutzing Deutshland	▪ Schnittstelle-Software
7	Microsoft Schweiz	The Circle 02 8058 Zürich-Flughafen Schweiz	▪ E-Mail ▪ Auswertungen