Auftragsverarbeitungsvertrag nach DSG bzw. analog DSGVO

zwischen der ALSO Schweiz AG

- Verantwortlicher / Auftragsverarbeiter - nachstehend Auftraggeber genannt -

und dem/der

Lieferanten

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftragsverarbeitungsvertrages ist die Durchführung der Aufgaben durch den Auftragnehmer gemäss Individualvertrag, insbesondere:

- Technischer Support und Wartung
- Auftragsabwicklung
- IT-Dienstleistungen
- Kundenservice wie Reparatur und allfällige Garantieleistungen
- Cloud-Services, jeweils im Rahmen des entsprechenden Produkt-, Dienstleistungs-, Kauf- und/oder Werkvertrages.

(2) Dauer

Die Dauer dieses Auftragsverarbeitungsvertrages (Laufzeit) entspricht der Laufzeit des Individualvertrages (hiernach Individualvertrag).

(3) Abschluss

Dieser Auftragsverarbeitungsvertrag tritt in Kraft mit Unterzeichnung, rückwirkend auf den 1. September 2023.

(4) Umfang

Dieser Auftragsverarbeitungsvertrag ist ausschliesslich anwendbar für den Fall, da der Auftragnehmer im Auftrag des Kunden als Auftragsverarbeiter Personendaten bearbeitet. Dies ist ausschliesslich der Fall im Zusammenhang mit den unter Ziff. 1 (1) genannten Aufgaben.

Für die übrigen Bearbeitungen, wo keine Auftragsverarbeitung vorliegt, publiziert der Auftragnehmer seine Grundsätze der Bearbeitung von Personendaten sowie allfällige Aktualisierungen im Internet unter URL einfügen (Datenschutzerklärung Auftragnehmer).

Der Auftragnehmer und der Auftraggeber halten bei der Bearbeitung von Personendaten (wie im DSG definiert) das anwendbare schweizerische Datenschutzrecht (Schweizerisches Datenschutzgesetz, DSG

und dessen Ausführungsverordnungen) ein. Wo auf Endkunden des Auftraggebers das europäische Datenschutzrecht (Verordnung (EU) 2016/679 (Datenschutzgrundverordnung, DSGVO)) anwendbar ist, hält der Auftragnehmer die DSGVO analog ein.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Auftraggeber ergeben sich konkret aus dem eingegangenen Individualvertrag und dessen Anhängen.

Art der Verarbeitung	Zweck der Datenverarbeitung
Technischer Support, Auftragsabwicklung, IT-Dienstleistungen, Kundenservice, Cloudservices	Auftragsabwicklung, technischer Support, IT-Dienstleistungen, Kundenservice, Cloud-Services

Die Erbringung der vertraglich vereinbarten Datenbearbeitung findet ausschliesslich in der Schweiz oder in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem Land für das es von der Europäischen Kommission bzw. vom Schweizerischen Bundesrat eine Adäquanzentscheidung gemäss Anhang 1 der DSV gibt statt.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

☒ Personenstammdaten

☒ Kommunikationsdaten (z.B. Telefon, E-Mail)

☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☒ Kundenhistorie

☒ Vertragsabrechnungs- und Zahlungsdaten

☒ Planungs- und Steuerungsdaten

☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Mitarbeiter des Auftraggebers
- ☐ Lieferanten des Auftraggebers
- ☒ Kunden des Auftraggebers
- ☐ Handelsvertreter/Reseller
- ☐ Ansprechpartner
- ☐ ……

3. Pflichten des Auftraggebers

(1) Der Auftraggeber ist dafür verantwortlich, in den Vertragsverhältnissen mit Dritten und mit seinen Endkunden angemessene Datenschutzregelungen zu treffen und die betroffenen Dritten über die Bearbeitung, Speicherung und Weitergabe von Daten und gegebenenfalls über die Datenbearbeitung durch den Auftragnehmer zu informieren. Der Auftraggeber ist dafür verantwortlich, die dafür notwendigen Einwilligungen der betroffenen Dritten, soweit gesetzlich erforderlich, einzuholen und dem Auftragnehmer auf Verlangen vorzulegen.
(2) Der Auftraggeber ermächtigt den Auftragnehmer, die Personendaten des Auftraggebers und/oder seiner Endkunden die im Zusammenhang mit der Individualvereinbarung bearbeitet werden, gleichgültig, ob diese vom Auftraggeber oder von Dritten stammen, im Sinne der Datenschutzgesetze zu bearbeiten.
(3) Der Auftraggeber nimmt zur Kenntnis, dass der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten, detaillierte Angaben über Produkte, Mengen, Umsätze sowie Namens- und Adressdaten des Auftraggebers und seiner Endkunden an seine Lieferanten weitergeben darf (Sell-Out-Reporting).

4. Technisch-organisatorische Massnahmen

(1) Der Auftraggeber und der Auftragnehmer gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit. Diese richtet sich nach Anlage 1, welche den Vorgaben gemäss Art. 3 DSG bzw. analog Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 1- 4 DSV bzw. analog Art. 5 Abs. 1, Abs. 2 DSGVO entsprechen.
(2) Zur Gewährleistung einer angemessenen Datensicherheit müssen der Auftraggeber und der Auftragnehmer den Schutzbedarf der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen (Art. 1 DSV und analog Art. Art. 32 Abs. 1 DS-GVO). Der Auftraggeber und der Auftragnehmer müssen technische und organisatorische Massnahmen treffen, damit die bearbeiteten Daten ihrem Schutzbedarf entsprechend nur Berechtigten zugänglich sind (Vertraulichkeit), verfügbar sind, wenn sie benötigt werden (Verfügbarkeit), nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität), nachvollziehbar bearbeitet werden (Nachvollziehbarkeit). Einzelheiten ergeben sich aus Anlage 1.
(3) Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate oder bessere Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert.

4. Berichtigung, Einschränkung und Löschung von Personendaten
(1) Der Auftragnehmer darf die Personendaten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten, sofern für den Auftragnehmer ersichtlich ist, dass der Endkunde dem Auftraggeber zuzuordnen ist.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer gewährleistet insbesondere die Einhaltung folgender Vorgaben (analog Art. 28 bis 33 DSGVO):

a) Der Auftragnehmer hat einen Datenschutzberater bestellt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Der Auftragnehmer gewährleistet die Wahrung der Vertraulichkeit zwischen den Parteien gemäss Art. 3 Abs. 1 DSV bzw. analog Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 personenbezogenen Daten hat, dürfen diese Daten ausschliesslich entsprechend der Weisung des Auftraggebers verarbeiten einschliesslich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, soweit gesetzlich zulässig. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) 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 Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

f) Der Auftragnehmer kontrolliert die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person dem Risiko entsprechend gewährleistet wird.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen. Hingegen gehören dazu sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmassnahmen zu ergreifen.

(2) Der Auftraggeber erteilt hiermit eine allgemeine Genehmigung, dass der Auftragnehmer Daten auch an einen Dritten transferieren darf, sofern dieser die Personendaten in der Schweiz oder in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem Land für das es von der Europäischen Kommission bzw. vom Schweizerischen Bundesrat eine Adäquanzentscheidung gemäss Anhang 1 der DSV bearbeitet. Liegt kein Adäquanzentscheid vor, trifft der Auftragnehmer die geeigneten und erforderlichen Massnahmen gemäss Art. 16 Abs. 2 DSG bzw. Art. 46 DSG-VO. Der Auftragnehmer teilt dem Auftraggeber mit, wer der Dritte ist und wo die Datenbearbeitung stattfindet und welche Massnahmen er getroffen hat, wenn er den Datentransfer auf Art. 16 Abs. 2 DSG bzw. Art. 46 DSG-VO abstützt.

(3) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen innert 14 Tagen ab Bekanntgabe begründet Einspruch zu erheben, andernfalls gilt die Unterbeauftragung als genehmigt. Die Information an den Auftraggeber erfolgt durch E-Mail-Mitteilung. Widerspricht der Auftraggeber und ist die Wahl eines anderen Auftragsverarbeiters nicht möglich, kann der Auftraggeber den Auftragsverarbeitungsvertrag sowie den Individualvertrag ausserordentlich beenden ohne Anrecht auf jegliche Rückerstattungsansprüche.

(4) Der Auftragnehmer wird Subunternehmer nach deren Eignung, insbesondere auf die Anforderungen des DSG, sorgfältig auswählen und regelmässig prüfen. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(5) Davon unberührt ist die Datenweitergabe an eigenständige Verantwortliche (wie z.B. Lizenzgeber) im Sinne des DSG, insbesondere dann, wenn Sie mit Endkunden einen eigenen Vertrag abschliessen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Leistungen gemäss Leistungsumfang des Hauptvertrages, im Einvernehmen mit dem Auftragnehmer zu überprüfen bzw. überprüfen zu lassen durch einen zur Berufsverschwiegenheit verpflichteten oder durch im Einzelfall zu benennende Prüfer ein Mal pro Kalenderjahr während maximal 2 Tagen während den üblichen Geschäftszeiten durchführen zu lassen (Audit). Er hat das Recht, sich durch Stichprobenkontrollen, die mindestens 10 Tage vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Nachweis der Einhaltung der technischen und organisatorischen Massnahmen , die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch Zertifizierung nach einem genehmigten Zertifizierungsverfahren, aktuelle Testate, Berichte oder Berichtsauszüge aus Audits durch unabhängige Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.
(3) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Soweit eine Prüfung/ein Audit des Auftraggebers einen

Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die Kosten gehen dabei zu Lasten des Auftragnehmers, wenn es sich nicht um branchenspezifische Vorgaben handelt.

8. Mitteilung bei Verstössen

(1) Beide Parteien unterstützen sich bei der Einhaltung der gesetzlichen Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und -verlust, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

a) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich, schnellstmöglich seit Entdeckung an die andere Partei mittels des Meldeformulars in Anlage 2 zu melden;
b) die Verpflichtung, dem der anderen Partei im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
c) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung; und
d) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Individualvertrages enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber erteilt Weisungen schriftlich. 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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich und beauftragt worden sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Individualvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung unwiderruflich zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem Auftraggeber vorzulegen.

(3) Geschäftsrelevante Dokumentation und Korrespondenz, die dem Nachweis der auftrags- und ordnungsgemässen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen gesetzlichen Archivierungs- bzw. Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Schlussbestimmungen

(1) Die Haftung des Auftragnehmers richtet sich ausschliesslich nach der Leistungsvereinbarung im Rahmen des jeweiligen Individualvertrages.

(2) Verrechnung wird ausgeschlossen.

(3) Anwendbar ist ausschliesslich materielles Schweizer Recht unter Ausschluss des Internationalen Privatrechts (IPRG, SR 291) und multinationalem Kollisionsrecht.

(4) Ausschliesslicher Gerichtsstand ist Emmen.

_____, den _____ _____, den _____

Auftraggeber: **Auftragnehmer:**

_____ _____

(Unterschrift / Firmenstempel) (Unterschrift/ Firmenstempel)

_____ _____

(Funktion des Unterzeichners) (Funktion des Unterzeichners)

_____ _____

(Name des Unterzeichners in Klarschrift) (Name des Unterzeichners in Klarschrift)

Anlage 1 – Technisch und organisatorische Massnahmen

1. Vertraulichkeit (Art. 2 lit. a DSV, analog Art. 32 Abs. 1 lit. b DS-GVO)

Physische Zugangskontrollen

Kein unbefugter Zugriff auf Datenverarbeitungssysteme.

Zweck: Diese Massnahmen sollen sicherstellen, dass Unbefugten der "physische" Zugang zu Datenverarbeitungsanlagen, die zur Verarbeitung personenbezogener Daten verwendet werden, verweigert wird.

Im Unternehmen ergriffene Massnahmen:

Bestehend	Messen
X	Zutrittskontrollsystem (Ausweisleser, Schliesssystem)
X	Massnahmen zur Objektsicherheit
X	Sicherheitstüren, Sicherheitsfenster
X	Protokollierung der Besucher
X	Überwachung
X	Lichtschranken, Bewegungsmelder
X	Türsicherung (Schliessanlage, Codeschloss, biometrisches Zutrittsschloss, Sicherheitsschlösser)
X	Schlüsselverwaltung / Dokumentation der Schlüsselbelegung
X	Sicherheit auch ausserhalb der Arbeitszeit durch Alarmanlage und/oder Anlagensicherheit
X	Regelungen für Gäste / Besucher / Personen ausserhalb des Unternehmens
X	Besucherausweise
X	Besondere Schutzmassnahmen des Serverraums (Wasseralarmanlage)
X	Mitarbeiter- und Berechtigungskarten (Tragepflicht)
X	Eingeschränkte Bereiche für externe Besucher und interne Mitarbeiter
X	Sorgfältige Auswahl des Reinigungspersonals
X	Dokumentation der Zutrittsskontroll-Massnahmen
X	Monitoring der Zugänge

Physische Zugangskontrolle: Kein unbefugter Systemzugriff.

Zweck: Diese Massnahmen sollen sicherstellen, dass nur autorisierte Personen auf die Datenverarbeitungssysteme zugreifen können und nur von Ihnen genutzt werden können.

Im Unternehmen ergriffene Massnahmen:

Bestehend	Messen
X	Persönliche und individuelle Benutzeranmeldung bei der Anmeldung am System- oder Firmennetzwerk
X	Kennwortprozedur (Kennwortrichtlinie)
X	Multi-Faktor-Authentifizierung
X	BIOS-Kennwortschutz
X	Zusätzlicher System-Login für spezifische Anwendungen

X	Zuordnung einzelner Clients und Identifikatoren nur für bestimmte Funktionen
X	Automatische Sperrung des Clients nach einer gewissen Zeit ohne Benutzeraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenumschaltung)
X	Elektronische Dokumentation aller Passwörter (keine Benutzerpasswörter) und Verschlüsselung dieser Dokumentation zum Schutz vor unbefugtem Zugriff
X	Personalisierte Chipkarten
X	Gehäuseverriegelung
X	Einsatz von Intrusion Detection Systemen
X	Verwendung von Antivirensoftware/Anti-Malware-Software
X	Einsatz von Firewall-Systemen
X	Netzwerk-Zugriffskontrolle
X	Zuordnung von Benutzerprofilen zu IT-Systemen
X	Einsatz der VPN-Technologie
X	Verwendung von Verschlüsselungsmechanismen für Dateien
X	Verschlüsselung mobiler Festplatten Datenträger in mobilen Endgeräten (Notebooks, Smartphones, etc.) Externe Speichermedien (USB-Sticks, Speicherkarten, etc.)
X	Kein Gerät ohne Passwort oder Sperrcode mit Zugriff auf Unternehmensdaten
X	Verpflichtung zum Datengeheimnis gemäss nDSG
X	Ordnungsgemässe Zerstörung von Festplatten
X	Leitfaden für die private Nutzung von IT-Geräten
X	BYOD-Richtlinie (Bring your own device)
X	Richtlinie für mobile Workstations (z.B Notebook)
X	Hintergrundsprüfung von Mitarbeitern mit privilegiertem Zugang zu Information
X	Zugang zu externen Websiten wird gemonitoried
X	Beschränkter Zugang zu Archiv-Informationen
X	Zugangskontrolle zu Software-Sourcecode
X	Dokumentierte Zugangskontrollen

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Ändern oder Entfernen innerhalb des Systems.
E.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Zweck:
Mit diesen Massnahmen soll sichergestellt werden, dass nur Personen Zugriff auf das Datenverarbeitungssystem haben und dass der Zugriff ausschliesslich auf diese personenbezogenen Daten beschränkt ist, die dieser Zugriffsberechtigung unterliegen, so dass Daten während der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Im Unternehmen ergriffene Massnahmen:

Bestehend	Messen
X	Berechtigungen verwalten
X	Fein abgestufte Berechtigungen
X	Profile

X	Rollen
X	Dokumentation von Berechtigungen
X	Genehmigungsverfahren für die Vergabe von Berechtigungen
X	Auswertungen/Protokollierung
X	Auditierung/Auditierung
X	Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (z.B. über Betriebssystem, Safeguard, PGP, Veracrypt, etc.)
X	Vier-Augen-Prinzip
X	Trennung der Verantwortlichkeiten
X	Aufgabenbezogene Berechtigungsprofile
X	Reduzierung von Personen mit Administratorrechten auf ein Minimum
X	Löschung von Datenträgern vor dem Recycling
X	Einsatz von Aktenvernichtern oder Dienstleistern zur Dokumentenvernichtung
X	Sichere Aufbewahrung von Datenträgern
X	Ordnungsgemässe Zerstörung von Festplatten
X	Protokollierung der Zerstörung
X	Regelmässige Überprüfung der Berechtigungen
X	Aufzeichnung, Auswertung und Monitoring von Protokollen (erfolglose und erfolgreiche Authentifizierungsversuche)
X	Dokumentiertes On- und Offboarding von Mitarbeitern
X	Abwesenheitskontrolle (Zugriff auf die Daten des Abwesenden)
X	Dokumentierte Zugangskontrollen

Trennkontrolle:
Getrennte Verarbeitung von Daten, die für verschiedene Zwecke erhoben werden. (Z.B. Sandboxing, Mandantenfähigkeit)

Zweck:
Die zweckgebundene Verarbeitung personenbezogener Daten sollte technisch sichergestellt sein. Das bedeutet, dass Daten, die für unterschiedliche Zwecke erhoben werden, entsprechend auch getrennt verarbeitet werden sollten.

Im Unternehmen ergriffene Massnahmen:

Bestehend	Messen
X	Separate Systeme
X	Separate Datenbanken
X	Erlaubnisse
X	Trennung durch Zugangsregelungen
X	Separierung von Test, Produktions-, Entwicklungs- und Archiv-Systemen

Andere:
Die Verarbeitung personenbezogener Daten erfolgt so, dass die Daten ohne die Nutzung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert gespeichert werden und geeignete technische und organisatorische Massnahmen getroffen wurden.

2. Integrität (Art. 2 lit. b DSV, analog Art. 32 Abs. 1 lit. b DS-GVO)
Freigabesteuerung

Kein unbefugtes Lesen, Kopieren, Ändern oder Entfernen während des Transports oder der elektronischen Übertragung. (z.B Verschlüsselung, VPN, Signatur, etc.)

Zweck:
Mit diesen Massnahmen soll sichergestellt werden, dass der Datenträger während des Transports oder der elektronischen Übermittlung nicht ohne Genehmigung gelesen, kopiert, verändert oder entfernt werden kann, oder die Massnahmen sollen überprüfen und feststellen, wo die Übermittlung personenbezogener Daten mittels Datenübertragungsmöglichkeiten vorgesehen ist. Insofern werden die Transport- und Datenträgersteuerungen durch die Übergabesteuerung kombiniert.

Im Unternehmen ergriffene Massnahmen:

Bestehend	Messen
X	Klassifizierung von Informationen
X	Verschlüsselung von E-Mails
X	Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (z.B. über Betriebssystem, Safeguard, PGP, Veracrypt, etc.)
X	Verschlüsselte Datenverbindungen (VPN)
X	Protokollierung (Audit-Protokollierung)
X	Gesichertes Wi-Fi
X	SSL-Verschlüsselung für den Webzugriff
X	Verordnung über die Vernichtung von Datenträgern
X	Ordnungsgemässe Zerstörung von Festplatten
X	Sorgfältige Auswahl des Transportpersonals für den manuellen Transport
X	Übersicht über regelmässige Abruf- und Zustellvorgänge
X	Verfahren zur Erkennung und zum Schutz vor Malware
X	Gesicherte Rechenzentrumseingabe
X	Datenträgerverwaltung
X	Separate Sperrung vertraulicher Datenträger
X	Kontrollierte Vernichtung von Datenträgern (z.B. Druckfehler)
X	Löschung von Datenträgern vor Ersatz
X	Gesicherter Ausdruck
X	Unterhalt von Software, Hardware + Appliances

Eingabekontrolle:
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt wurden, z.B. Protokollierung, Dokumentenmanagement

Zweck:
Diese Massnahmen sollen die Überprüfbarkeit eines Verarbeitungsvorgangs (Eingabe, Änderung, Löschung) personenbezogener Daten sicherstellen. Das bedeutet, dass Autor, Inhalt und Zeitpunkt der Datenspeicherung ermittelt werden sollten.

Im Unternehmen ergriffene Massnahmen:

Bestehend	Messen
X	Zugriffsrechte / Berechtigungskonzept
X	Systemseitige Protokollierung
X	Sicherheit/Protokollierungssoftware
X	Funktionale Verantwortlichkeiten
X	Multi-Eye-Prinzip
X	Verpflichtung zum Informations- und Datenschutz sowie Wahrung von Geschäfts- und Berufsgeheimnissen.

3. Verfügbarkeit und Belastbarkeit

Mengenverfügbarkeitskontrolle

Schutz vor versehentlicher oder mutwilliger Zerstörung oder Verlust, z.B.: Backup-Konzept (online/offline, onsite/offsite), unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldekanäle, Notfallpläne.

Zweck:
Es muss sichergestellt werden, dass die personenbezogenen Daten nicht versehentlich vernichtet und vor Verlust geschützt sind. Es muss sichergestellt sein, dass die eingesetzten Systeme im Störungsfall wiederhergestellt werden können.

Im Unternehmen ergriffene Massnahmen:

Bestehend	Messen
X	Backup-Strategie
X	Backup-Retention-Konzept
X	Serverräume, die nicht unter wasserführenden Systemen/Einrichtungen liegen
X	Unterbrechungsfreie Stromversorgung (Batterie, Diesel)
X	Temperatur- und Feuchteüberwachung in Serverräumen
X	Viren-/Bedrohungsschutz, Firewall
X	Klimatisierung in Computerräumen
X	Brand- und Löschschutz (Brandmeldeanlagen, Feuerlöschgeräte)
X	Alarm
X	Geeignete Archivierungsmöglichkeiten
X	Alternativplan
X	Notfallübung
X	Katastrophenpläne, BCM
X	Fehler- und Wiederherstellungspläne usw.
X	Redundantes Rechenzentrum (inhouse/extern)
X	Redundante Datenanbindung der Rechenzentren an das Unternehmensnetzwerk
X	Redundante Hardware
X	Spiegeln von Daten
X	Unterhalt von Software, Hardware + Appliances

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

Auftragssteuerung:

Keine Auftragsdatenverarbeitung ohne entsprechende Weisungen des Auftraggebers, z.B. klare Vertragsgestaltung, formalisierte Auftragsverwaltung, strenge Auswahl des Dienstleisters, Verpflichtung zur Vorkasse, Nachprüfungen.

Zweck:
Der Auftragnehmer hat dafür Sorge zu tragen, dass die im Auftrag zu verarbeitenden Daten nur nach Weisung des Auftraggebers verarbeitet werden. Indirekt damit verbunden ist die Weisungspflicht des Auftraggebers gegenüber Auftragnehmern.

Im Unternehmen gelten folgende Massnahmen:

Bestehend	Messen
X	Schriftlicher Vertrag zur Auftragsdatenverarbeitung mit Subunternehmern mit Bestimmungen über die Rechte und Pflichten des Auftragnehmers und Auftraggebers.
X	Regelmässige Kontrolle zur Einhaltung der Verpflichtungen der Subunternehmer aus den Auftragsdatenverarbeitungsverträgen.
X	Schulung aller autorisierten Mitarbeiter
X	Regelmässige Umschulung
X	Geheimhaltungs- und Datengeheimnis der Mitarbeiter
X	Regelmässige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
X	Ermittlung von Ansprechpartnern und verantwortlichen Projektleitern für den konkreten Auftrag.
X	Sorgfältige Auswahl des Auftragnehmers

Anlage 2 – zum Auftragsverarbeitungsvertrag: Meldeformular

Meldung an: den Datenschutz- bzw. Informationsschutzverantwortlichen des Auftraggebers / AUFTRAGNEHMERS

AUFTRAGNEHMER / AUFTRAGGEBER	
Zeitspanne/-datum des Vorfalles	
Zeitpunkt der Feststellung	
Beschreibung des Vorfalles	
Betroffene Datenkategorien	
Anzahl der betroffenen Personen	
Betroffene IT-Systeme	
Verantwortliche Abteilung beim AUFTRAGSVERABEITER	
Name und Kontaktdetails des Datenschutzbeauftragten oder -beraters	
Autor + Datum der Meldung	
Wer wurde von wem informiert (Datenschutzbehörden, betroffene Personen, Aufsichtsbehörden) und falls ja, was wurde kommuniziert	
Quelle der Information über die Datenschutzverletzung	
Beschreibung der Konsequenzen des Vorfalles	
Beschreibung der allenfalls bereits getroffenen Massnahmen durch den AUFTRAGSVERABEITER (unter Berücksichtigung, dass keine Beweise zerstört werden)	
Wurde eine Strafverfahren anhängig gemacht	
Beschreibung weitergehender zukünftiger technischer und organisatorischer Massnahme	
Massnahmen zur Mitigation des Schadens des Vorfalles	
Gesamtrisikobeurteilung	