Vereinbarung zur Auftragsverarbeitung

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

ALSO Deutschland GmbH – Lange Wende 43 – 59494 Soest

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Technischer Support, Auftragsabwicklung, IT-Dienstleistungen, Kundenservice, Cloud-Services.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung im Rahmen der jeweiligen Produkt-, Dienstleistungs-, Kauf- und/oder Werkverträge.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Art der Daten	Zweck der Datenverarbeitung	Kreis der Betroffenen
Personenbezogene Daten: - Name - Adressdaten - Kontaktdaten - Vertragsstammdaten - Kundenhistorie - Vertragsabrechnungs- und Zahlungsdaten - Auskunftsangaben - Systemkonfigurationen - Speicherdaten des Auftragnehmers - Verkehrs- und Nutzungsdaten	- Auftragsabwicklung - Technischer Support - IT-Dienstleistungen - Kundenservice - Cloud-Services	- Mitarbeiter des Auftraggebers - Geschäftspartner - Kunden - Interessenten - Lieferanten - Abonnenten - Beschäftigte - Kunden des Auftragnehmers

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich 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 eine Adäquanzentscheidung gibt statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in einem Drittland wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs 2 lit c und d DSGVO)

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien: Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen), Verkehrs- und Nutzungsdaten im Rahmen der Nutzung des Clouddienste, Information über Systemkonfigurationen und Kundenumgebungen sowie im Rahmen des technischen Supports sämtlich Datenkategorien, die der Auftraggeber innerhalb der betreuten Systeme speichert.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Mitarbeiter des Auftraggebers, Geschäftspartner, Kunden, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Ansprechpartner sowie im Rahmen des technischen Supports sämtliche Personenkreise, zu denen der Auftraggeber Daten innerhalb der betreuten Systeme speichert.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, 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 gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 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 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 [Einzelheiten in Anlage 1].
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, 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.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten-Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
   Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Carsten Rohlfs, TÜV Rheinland Industrie Services GmbH, Alfredstraße 81, 45130 Essen, +4916090151429, carsten.rohlfs@de.tuv.com bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 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 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) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

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

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 Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung 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 Auftragsverarbeitung 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 Verarbeitung 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 Ziffer 7 dieses Vertrages.

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, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Weitergabe von Aufträgen im Rahmen der im Auftrag vereinbarten Tätigkeiten an Subunternehmer ist zulässig. Der Auftragnehmer wird Subunternehmer nach deren Eignung, insbesondere auf die Anforderungen der DSGVO, sorgfältig auswählen und regelmäßig prüfen. Des Weiteren wird der Auftragnehmer mit den Subunternehmern eine dieser Vereinbarung entsprechende Vereinbarung zu Auftragsverarbeitung vereinbaren. Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen diese Änderung Einspruch zu erheben. Erfolgt kein Einspruch innerhalb von 14 Tagen ab Bekanntgabe, gilt die Zustimmung zur Änderung als erteilt.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	**Anschrift**	**Leistung**
keine		

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

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durch einen zur Berufsverschwiegenheit verpflichteten oder durch im Einzelfall zu benennende 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. 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 Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, 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 Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten 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
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(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 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 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 der Leistungsvereinbarung – 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 datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

_____, den _____	_____, den _____
Auftraggeber:	**Auftragnehmer:**
_____	_____
_____	_____
(Unterschrift / Firmenstempel)	(Unterschrift/ Firmenstempel)
_____	_____
(Funktion des Unterzeichners)	(Funktion des Unterzeichners)
_____	_____
(Name des Unterzeichners in Klarschrift)	(Name des Unterzeichners in Klarschrift)

Anhang 1: Technisch-Organisatorische-Maßnahmen

Gesellschaft: ALSO Deutschland GmbH

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

Zutrittskontrolle:
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.

Zweck:
Diese Maßnahmen sollen gewährleisten, dass unbefugten der „körperliche" Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden verwehrt wird.

Im Unternehmen getroffenen Maßnahmen:

vorh.	Maßnahme
X	Zutrittskontrollsystem (Ausweisleser, Schließsystem)
X	Maßnahmen zur Objektsicherung
X	Zaunanlagen
X	Sicherheitstüren, Sicherheitsfenster
X	Werkschutz, Pförtner
X	Personenkontrolle beim Pförtner, Empfang
X	Protokollierung der Besucher
X	Videoüberwachung
X	Türsicherung (Schließsystem, Codesperre, biometrische Zugangssperre, Sicherheitsschlösser)
X	Schlüsselverwaltung / Dokumentation der Schlüsselvergabe
X	Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz
X	Regelung für Gäste / Besucher / Firmenfremde Personen
X	Besucherausweise
X	Spezielle Schutzvorkehrungen des Serverraums
X	Sperrbereiche
X	Sorgfältige Auswahl des Reinigungspersonals

Zugangskontrolle:
Kein unbefugter Systemzugang.

Zweck:
Diese Maßnahmen sollen gewährleisten, dass nur befugten Personen die Datenverarbeitungssysteme zugänglich sind und ausschließlich von ihnen benutzt werden können.

Im Unternehmen getroffene Maßnahmen:

vorh.	Maßnahme
X	Persönlicher und individueller User-Log-In bei Anmeldung am System, bzw. Unternehmensnetzwerk
X	Kennwortverfahren (Kennwortrichtlinie)
X	Multi-Faktor Anmeldung
X	BIOS-Passwortschutz
X	Zusätzlicher System-Log-in für bestimmte Anwendungen
X	Automatische Sperrung des Clients nach gewissem Zeitablauf ohne Useraktivität (auch Passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
X	Elektronische Dokumentation sämtlicher Passwörter (keine User-Passwörter) und Verschlüsselung dieser Dokumentation zum Schutz vor unbefugtem Zugriff
X	Personalisierte Chipkarten
X	Einsatz von Intrusion-Detection-Systemen
X	Einsatz von Anti-Viren-Software/Anti-Malware-Software
X	Einsatz von Firewall-Systemen
X	Einsatz von VPN-Technologie
X	Einsatz von Verschlüsselungsmechanismen für Dateien
X	Verschlüsselung von mobilen Datenträgern sowie Datenträger in mobilen Geräten (Notebooks, Smartphones, etc.)
X	Kein Gerät ohne Passwort oder Sperrcode mit Zugriff auf Firmendaten
X	Verpflichtung auf das Datengeheimnis nach Art 28 Abs. 3 lit. b EU-DSGVO
X	Ordnungsgemäße Vernichtung von Datenträgern
X	Richtlinie zur privaten Nutzung des IT-Equipments
x	Richtlinie mobiler Arbeitsplatz (z.B. Notebook)

Zugriffskontrolle:
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.
Z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Zweck:
Diese Maßnahmen sollen gewährleisten, dass nur die zur Nutzung des Datenverarbeitungssystems Berechtigten den Zugriff haben und der Zugriff sich ausschließlich auf diese personenbezogenen Daten beschränkt, die dieser Zugriffsberechtigung unterliegen, s. d. Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Im Unternehmen getroffenen Maßnahmen:

vorh.	**Maßnahme**
X	Verwaltung von Berechtigungen
X	Differenzierte Berechtigungen
X	Profile
X	Rollen
X	Dokumentation von Berechtigungen
X	Genehmigungsverfahren zur Berechtigungsvergabe
X	Auswertungen/Protokollierung
X	Prüfung/Auditierung
X	Segregation of Duties
X	Aufgabenbezogene Berechtigungsprofile
X	Reduzierung der Personen mit Administratorenberechtigungen auf ein Minimum
X	Löschung von Datenträgern vor Wiederverwertung
X	Einsatz von Aktenvernichtern bzw. Dienstleistern zur Aktenvernichtung
X	Sichere Aufbewahrung von Datenträgern
X	Ordnungsgemäße Vernichtung von Datenträgern
X	Protokollierung der Vernichtung
X	Regelmäßige Überprüfung der Berechtigungen
X	Aufzeichnung und Auswertung von Protokollen (erfolglose und erfolgreiche Authentifizierungsversuche)
X	Abwesenheitsregelung (Zugang zum Datenbestand des Abwesenden)

Trennungskontrolle:
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. (z.B. Sandboxing, Mandantenfähigkeit)

Zweck:
Zweckbezogene Verarbeitung personenbezogener Daten soll technisch sichergestellt werden. D.h. zu unterschiedlichen Zwecken erhobene Daten sollen auch entsprechend getrennt verarbeitet werden.

Im Unternehmen getroffene Maßnahmen:

vorh.	Maßnahme
X	Getrennte Systeme
X	Getrennte Datenbanken
X	Zugriffsberechtigungen
X	Trennung durch Zugriffsregelungen

Sonstiges:
Pseudonymisieren: (Art. 32 Abs. 1 lit a DSGVO, Art 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzliche Information gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterlag.

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

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen während des Transportes oder Elektronischer Übertragung (z.B Verschlüsselung, VPN, Signatur, etc.).

Zweck:
Diese Maßnahmen sollen gewährleisten, dass Datenträger während des Transportes oder elektronischer Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, bzw. soll durch die Maßnahmen überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Insofern werden die Transport- und Datenträgerkontrollen durch die Weitergabekontrolle zusammengefasst.

Im Unternehmen getroffene Maßnahmen:

vorh.	Maßnahme
X	Verschlüsselung von email
X	Verschlüsselte Datenverbindungen (VPN)
X	Protokollierung (Auditlogging)
X	Gesichertes WLAN
X	SSL-Verschlüsselung bei Web-Access
X	Regelung zur Datenträgervernichtung
X	Ordnungsgemäße Vernichtung von Datenträgern
X	Sorgfältige Auswahl beim Transportpersonal bei manuellem Transport
X	Übersicht über regelmäßige Abruf- und Übermittlungsvorgänge
X	Verfahren zu Erkennung und Schutz von Schadsoftware
X	Gesicherter Datacenter-Eingang
X	Datenträger-Verwaltung
X	Gesonderter Verschluss vertraulicher Datenträger
X	Kontrollierte Vernichtung von Datenträgern (z.B. Fehldrucke,)
X	Löschung von Datenträgern vor Austausch

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

Zweck:
Durch diese Maßnahmen soll die Nachprüfbarkeit eines Verarbeitungsvorgangs (Eingabe, Änderung, Entfernung) personenbezogener Daten gewährleistet werden. D.h. Urheber, Inhalt und Zeitpunkt der Datenspeicherung sollen ermittelt werden.

Im Unternehmen getroffenen Maßnahmen:

vorh.	**Maßnahme**
X	Zugriffsrechte / Berechtigungskonzept
X	Systemseitige Protokollierungen
X	Sicherheits-/Protokollierungssoftware
X	Funktionelle Verantwortlichkeiten
X	Mehraugenprinzip
X	Verpflichtung auf das Datengeheimnis

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit b EU-DSGVO)
Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B. Backupkonzept (online/offline, onsite/offsite), unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldewege, Notfallpläne.

Zweck:
Es muss sichergestellt sein, dass die personenbezogene Daten nicht zufällig zerstört werden und vor Verlust geschützt sind. Es muss gewährleistet sein, das eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Im Unternehmen getroffene Maßnahmen:

vorh.	Maßnahme
X	Backupstrategie
X	Aufbewahrungskonzept von Backups
X	Serverräume nicht unterhalb von wasserführenden Anlagen/Einrichtungen
X	Unterbrechungsfreie Stromversorgung (Batterie, Diesel)
X	Temperatur- und Feuchtigkeitsüberwachung in Serverräumen
X	Viren/Bedrohungsschutz, Firewall
X	Klimaanlage in IT Räumen
X	Brand- und Löschschutz (Brandmeldeanlagen, Feuerlöscheinrichtungen)
X	Alarmanlage
X	Geeignete Archivierungsräumlichkeiten
X	Notfallplan
X	Notfallübung
X	Ausfall- und Wiederherstellungspläne, etc.
X	Redundantes Datacenter (inhouse/extern)
X	Redundante Datenanbindung der Datacenter an das Corporate Network
X	Redundante Hardware
X	Spiegeln von Daten

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

Auftragskontrolle:
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 EU-DSGVO ohne entsprechende Weisung des Auftraggebers, z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Zweck:
Der Auftragnehmer hat zu gewährleisten, dass die im Auftrag zu bearbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Mittelbar damit verbunden ist die Pflicht des Auftraggebers, Weisungen an Auftragnehmer zu erteilen.

Im Unternehmen gelten folgende Maßnahmen:

vorh.	**Maßnahme**
X	Schriftlicher Vertrag zur Auftragsdatenverarbeitung gem. EU-DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
X	Schulungen aller zugriffsberechtigten Mitarbeiter
X	Regelmäßig stattfindende Nachschulungen
X	Verpflichtung der Mitarbeiter zur Geheimhaltung und auf das Datengeheimnis
X	Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
X	Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag
X	Sorgfältige Auswahl des Auftragnehmers