Allgemeine Geschäftsbedingungen Datenschutz zur Auftragsverarbeitung

der

stratEDI Gesellschaft für Kommunikationskonzepte und -lösungen mbH
Lusebrink 9
58285 Gevelsberg

- nachfolgend **„Auftragnehmer“** -

- nachfolgend Vertragspartner und Auftragnehmer gemeinsam als **„Parteien“** bezeichnet -

PRÄAMBEL

Diese Bedingungen beschreiben die Verpflichtungen der Parteien zum Datenschutz. Der Vertragspartner - nachfolgend: Auftraggeber genannt - möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen vereinbaren die Parteien die nachfolgenden Regelungen, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 BEGRIFFSBESTIMMUNGEN

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die alleine oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels

Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 ANGABE DER ZUSTÄNDIGEN DATENSCHUTZ-AUFSICHTSBEHÖRDE

(1) Zuständige Aufsichtsbehörde für den Auftragnehmer ist Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

(2) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 VERTRAGSGEGENSTAND

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Rechnungserstellung im elektronischen Format. Grundlage dieser Leistungserbringung ist der Hauptvertrag.

Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung sowie den Anlagen des Hauptvertrages). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 WEISUNGSRECHT

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsempfangsberechtigten Personen ergeben sich aus **Anlage 5**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen wird der Auftragnehmer dem Auftraggeber unverzüglich einen Nachfolger bzw. Vertreter in Textform benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Bis zu einer Klärung ist er zur Ausführung der Weisung nicht verpflichtet. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 ART DER VERARBEITETEN DATEN, KREIS DER BETROFFENEN

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 2** dargestellt.

§ 6 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) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 3** aufgeführten Maßnahmen der

a) Zutrittskontrolle

b) Zugangskontrolle

c) Zugriffskontrolle

d) Weitergabekontrolle

e) Eingabekontrolle

f) Auftragskontrolle

g) Verfügbarkeitskontrolle

h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter/als Ansprechpartner für den Datenschutz

Herr Dipl. Inform. Olaf Tenti

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

als externer Datenschutzbeauftragter

Körnerstr. 45

58095 Hagen

Tel.: +49 (0) 2331 / 356832-0

E-Mail: datenschutz@gdi-mbh.eu

Internet: http://gdi-mbh.eu/

bestellt. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

§ 7 INFORMATIONSPFLICHTEN 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 personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und informiert hierüber den Auftraggeber.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten 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, 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 DS-GVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 KONTROLLRECHTE DES AUFTRAGGEBERS

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig in angemessenen Abständen von den technischen und organisatorischen Maßnahmen des Auftragnehmers. 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 nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang, höchstens einmal jährlich, durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(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.

(4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 EINSATZ VON SUBUNTERNEHMERN

(1) Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus der **Anlage 4** und ggf. dem Hauptvertrag. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

(2) Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von einem Monat zu kündigen.

(3) Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DS-GVO festgelegten Pflichten auferlegt sind.

(4) Unter Einhaltung der Anforderungen dieser Vereinbarung gelten die Regelungen in diesem § 9 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Sofern eine Einbeziehung eines weiteren Auftragsverarbeiters in einem Drittland erfolgt, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen weiteren Auftragsverarbeiter ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der jeweils gültigen EU-Standarddatenschutzklauseln). Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen solchen Vertrag unter Einbeziehung der EU-Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern in seiner jeweils gültigen Form zu schließen. Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen weiteren Auftragsverarbeitern nachweisen. Soweit für bestimmte Übermittlungsvorgänge in Drittländer die Einwilligung gem. Art. 49 DS-GVO der betroffenen Person erforderlich ist, erklärt sich der Auftraggeber bereit, an der Erfüllung der Voraussetzungen des Art. 49 DS-GVO im erforderlichen Maße mitzuwirken.

§ 10 ANFRAGEN UND 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 23 sowie 32 bis 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 HAFTUNG

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Außenverhältnis alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(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.

§ 12 BEENDIGUNG DES HAUPTVERTRAGS

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle Unterlagen, Daten und Datenträger, die aus der Auftragsverarbeitung stammen, zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen oder vernichten. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Falls eine im ersten Satz beschriebene Verpflichtung zur Speicherung besteht, sind alle Unterlagen, Daten und Datenträger, die aus der Auftragsverarbeitung stammen und der Verpflichtung unterliegen, zurückzugeben, zu löschen oder zu vernichten, sobald diese Verpflichtung wegfällt. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

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

(3) Solange nicht alle personenbezogenen Daten, die im Auftrag des Auftraggebers verarbeitet wurden und nach Wegfall des Hauptvertrages noch im Besitz des Auftragnehmers waren, vom Auftragnehmer gelöscht bzw. vernichtet oder an den Auftraggeber zurückgegeben wurden, gilt dieser Ergänzungsvertrag als fortbestehend, auch über den Wegfall des Hauptvertrages – gleich aus welchem Rechtsgrund – hinaus. Ist die vorgenannte Bedingung entfallen, endet der Ergänzungsvertrag, ohne dass es einer gesonderten Erklärung einer der Parteien bedarf.

§ 13 SCHLUSSBESTIMMUNGEN

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

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Gevelsberg.

Folgende **ANLAGEN** sind vertragsgegenständlich:

ANLAGE 1	–	Art der Daten, Art und Zweck der Datenverarbeitung
ANLAGE 2	–	Kategorien betroffener Personen
ANLAGE 3	–	Technische und organisatorische Maßnahmen des Auftragnehmers
ANLAGE 4	–	Genehmigte Subunternehmer
ANLAGE 5	–	Weisungsberechtigte Personen

ANLAGE 1 – Art der Daten, Art und Zweck der Datenverarbeitung

Art der Daten	Art und Zweck der Datenverarbeitung
• Vorname • Nachname • Anschrift • Bestellnummer • Lieferscheinnummer • Artikelidente • Mail des Ansprechpartners • Streckengeschäft: Adresse, Mailadresse und Telefonnummer des Endkunden • Steuernummer bzw. Umsatzsteuer-Identifikationsnummer • Ausstellungsdatum der Rechnung • Rechnungsnummer • handelsübliche Bezeichnung der gelieferten Gegenstände oder Umgang und Art der sonstigen Leistungen • Zeitpunkt der Lieferung oder sonstigen Leistungserbringung • ggf. Zeitpunkt der Vereinnahmung des Entgelts oder eines Teils des Entgelts • nach Steuersätzen aufgeschlüsseltes Entgelt • anzuwendender Steuersatz • auf das Entgelt entfallender Steuerbetrag	Konvertierung von Geschäftsdokumenten (Bestellung, Lieferschein, Rechnung, etc.) aus oder in ein Inhouseformate in bzw. aus EDIFACT/EANCOM und individuellen Formaten im B2B-Bereich mit dem Ziel der Verarbeitung der Dokumente ohne Medienbruch. Empfang und Konvertierung der EDI-Nachrichten wie ORDERS, DESADV, INVOIC und das mit unseren Kunden vereinbarte Inhouseformat. Hosting einer allgemeinen WebSolution zum Empfang von ORDERS und der Erzeugung von DESADV und INVOIC über eine webbasierte Oberfläche. Visualisierung aller Nachrichten im Browser. Hosting individueller WebSolutions zur Digitalisierung der Lieferanten-prozesse.

ANLAGE 2 - Kategorien betroffener Personen

Kategorien betroffener Personen
Kunden des Auftraggebers

ANLAGE 3 - Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DS-GVO

Die Datenschutz-Grundverordnung (DS-GVO) fordert von Organisationen oder Unternehmen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, ein Schutzniveau, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen ist.

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt. Ziel ist die Gewährleistung insbesondere der **Vertraulichkeit, Integrität, Belastbarkeit und Verfügbarkeit** der im Auftrag verarbeiteten personenbezogenen Daten.

A. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Vertraulichkeit im Sinne des Art. 32 Abs. 1 lit. b in Verbindung mit Erwägungsgründen. 39 und 83 DS-GVO ist hinreichend gewährleistet, wenn Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können und die Daten außerdem gemäß Art. 5 Abs. 1 lit. f DS-GVO vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust geschützt sind.

1. Zutrittskontrolle:

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Im Verizon-Rechenzentrum sind unter anderem besonders die folgenden Maßnahmen hervorzuheben:

- Für das Betreten der Anlage ist eine vorherige Anmeldung mit einer vorherigen Auftragserstellung notwendig
- Nur ein definierter Personenkreis hat Zugang
- Zur Authentifizierung werden mehrere Faktoren hinzugezogen

Für die Zutrittskontrolle zu den Büros sind besonders hervorzuheben:

- Das Gebäude ist durch eine Alarmanlage gesichert
- Es existiert ein Schließsystem mit definierten Verantwortlichkeiten und einer Nachverfolgung für die Schlüsselaus- und -rückgabe. Bei einem Schlüsselverlust wird ein Austausch des Schließsystems vorgenommen; eine Nachbestellung von Schlüsseln findet nur nach gesonderter Authentifizierung und Autorisierung statt
- Firmenfremde (einschließlich Handwerker) werden am zentralen Empfang des Unternehmens abgeholt und innerhalb des Unternehmens begleitet

- Besuchern ist es durch die verschlossenen Bereiche des Unternehmens und durch die verschlossenen Etagen nicht möglich sich Zutritt in die Räume zu verschaffen
- Für die Backup-Aufbewahrung sind Verantwortlichkeiten definiert und der Zugriff stark eingeschränkt; der Aufbewahrungsraum des Safes für die Backups ist gesondert gesichert

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Die Zugangskontrolle für die Server unterliegt den Maßgaben von Verizon
- Beim Auftragnehmer gibt es ein mehrstufiges Berechtigungssystem für die Administration der Server
- Für alle Passwörter existieren Passwortrichtlinien

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Es ist sichergestellt, dass nur Personen aus dem Bereich der EDI-Verarbeitung auf die Serverinfrastruktur zugreifen können
- Die verschiedenen Berechtigungsbereiche sind durch die Vergabe von unterschiedlichen Passwörtern getrennt

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Die Trennungskontrolle basiert auf der Adressierung nach Kundenvorgabe

B. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Integrität im Sinne des Art. 32 Abs. 1 lit. b in Verbindung mit Art. 5 Abs. 1 lit. f DS-GVO ist gewährleistet, wenn Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten also vollständig, unverändert und unversehrt sind.

1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

- Ein- und ausgehende Verbindungen werden protokolliert
- Die Übertragung bei den automatisierten Verfahren erfolgt verschlüsselt
- In Ausnahmefällen wird nur auf besonderen Kundenwunsch die Verarbeitung per E-Mail ermöglicht; aufseiten des Auftragnehmers findet keine gesonderte Übermittlung von E-Mails zwischen Anwendung und Server statt
- Lokale Backups werden im feuerfesten Safe gelagert, Verantwortlichkeiten für den Zugriff darauf sind definiert und der Zugriff stark eingeschränkt; der Raum des Safes ist gesondert gesichert
- Transport des Backups ohne Umwege von und zum Safe

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

- Im Rahmen der automatisierten Verarbeitung findet eine Protokollierung der ein- und ausgehenden Daten statt
- Für die Administration werden die Logging-Funktionalitäten der Betriebssysteme genutzt
- Aufgrund der nahezu Echtzeitverarbeitung sind die Manipulationsmöglichkeiten sehr begrenzt

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeit im Sinne des Art. 32 Abs. 1 lit. b DS-GVO ist gewährleistet, wenn die Daten ihrem Zwecke nach jederzeit nutzbar sind. Zusätzlich muss gemäß Art. 32 Abs. 1 lit. c DS-GVO die Fähigkeit bestehen die Verfügbarkeit und den Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können.

Belastbarkeit ist gemäß Art. 32 Abs. 1 lit. b DS-GVO auf Dauer sicherzustellen und betrifft Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzt der Auftragnehmer folgende Einrichtungen:

1. Hardware:

- Hochverfügbare Serverinfrastruktur bei Verizon mit Raid
- Hochverfügbare Server Inhouse mit Raid

2. Software:

- Eigenentwicklung

D. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c)

- Die Datensicherung findet auf räumlich getrennten NAS-System statt
- Lokale Backups werden im feuerfesten Safe gelagert, Verantwortlichkeiten für den Zugriff darauf sind definiert und der Zugriff stark eingeschränkt; der Raum des Safes ist gesondert gesichert
- Allgemein sind die Systeme hochverfügbar und redundant aufgebaut

E. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1, Abs. 2 DS-GVO)

(z.B. Datenschutz Managementsystem (DSMS), Auditplanung und Durchführung von internen und externen Audits, Durchführung von Sensibilisierungsmaßnahmen, Maßnahmenplanung, Reporting bzw. Berichterstattung, Risikomanagement und -Analyse, Prozess zur Behandlung von Datenschutzvorfällen, Datenschutzfreundliche Voreinstellungen)

- Auditplanung und Durchführung von internen und externen Audits
- Durchführung von Sensibilisierungsmaßnahmen
- Maßnahmenplanung
- Reporting bzw. Berichterstattung
- Risikomanagement und -Analyse
- Prozess zur Behandlung von Datenschutzvorfällen
- Datenschutzfreundliche Voreinstellungen

ANLAGE 4 – Genehmigte Subunternehmer

Der Auftragnehmer hat folgende Subunternehmer mit weiteren Dienstleistungen beauftragt, in dessen Zusammenhang personenbezogene Daten verarbeitet werden:

Firma	Anschrift	Auftragsinhalt
Verizon Deutschland GmbH	Rechenzentrumsleistungen	Sebrathweg 20, 44149 Dortmund
Telekom Deutschland GmbH	BusinessMail X.400 EDI-Kommunikation	Landgrabenweg 151, 53227 Bonn

ANLAGE 5 – Weisungsberechtigte Personen

Weisungsempfänger beim Auftragnehmer

Name	Kontaktdaten	Position	Weisungsbereich / Befugnisse
Hr. Dr. Thorsten Georg	*info@stratedi.de*	Geschäftsführer	weisungsbefugt
Herr Marvin Karl	*Info@stratedi.de*	Geschäftsführer	weisungsbefugt
Herr Andreas Weng	*edi-support@stratedi.de*	EDI-Projektmanager	eingeschränkt weisungsbefugt im Bereich EDI-Development