Allgemeine Geschäftsbedingung zur Auftragsverarbeitung

der

stratEDI GmbH, Lusebrink 9, 58285 Gevelsberg

-Auftragnehmer-

Präambel

Diese Bedingung beschreibt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Verträgen der Parteien ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit einem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im jeweiligen Vertrag und ggf. in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen jedes Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

Die datenschutzrechtlichen Pflichten des Auftragnehmers sind durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

Die Art der zu verarbeitenden Daten und die Kategorien der betroffenen Personen ergeben sich aus der Leistungsbeschreibung (Name, Adresse, E-Mailadresse, Telefonnummer).

§ 2 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

Weisungsberechtigte Personen des Auftraggebers werden von diesem benannt. Ein Wechsel ist rechtzeitig vorher schriftlich anzuzeigen.

Weisungsempfänger beim Auftragnehmer sind:

- Dr. Thorsten Georg, Geschäftsführung, 02332 66600-0
- Andreas Weng, EDI-Projektmanager, 02332 66600-0
- Markus Martini, EDI-Projektmanager, 02332 66600-0

2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Die Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass ein angemessenes oder vertraglich vereinbartes Schutzniveau nicht unterschritten wird.

Eine Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers findet sich im Anschluss an diese Bedingungen.

3. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Dieser Aufwand wird dem Auftragnehmer vom Auftraggeber zu den jeweils geltenden Stundensätzen des Auftragnehmers vergütet.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien aufgrund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart

9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

11. Die vorstehend geschilderten Aufwände sind vom Auftraggeber an den Auftragnehmer zu dessen jeweils gültigen Preisen gemäß Preisliste zu vergüten.

§ 3 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 4 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung so weit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 5 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion mit dem Auftraggeber wird dem Auftragnehmer sein Aufwand zu seinen jeweiligen gültigen Stundensätzen vergütet.

3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine

Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 6 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Auftragnehmer bedient sich zur Erfüllung seiner vertraglichen Verpflichtungen […]

2. Ein solches Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber mit einer Frist von drei Wochen. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben.

3. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 7 Informationspflichten, Schriftformklausel, Rechtswahl

1. 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

2. Änderungen und Ergänzungen dieser Bedingungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Bedingungen unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

3. Es gilt deutsches Recht.

Anhang über technische und organisatorische Maßnahmen nach Art. 32 DSGVO (vgl. auch § 2 Abs. 2):

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. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- 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

5. 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

6. Verfügbarkeitskontrolle

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

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

Software:
- Eigenentwicklung

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Die Datensicherung findet nach einem definierten QM-System nach ISO 9001 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

7. Trennungskontrolle

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

- Die Trennungskontrolle basiert auf der Adressierung nach Kundenvorgabe