Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO

Präambel

Diese Vereinbarung regelt die Rechte und Pflichten zwischen der

- Smart-SP GmbH, Fröbelstraße 1a – 49811 Lingen (im Folgenden „Auftragnehmer“ genannt) &
- Ihnen (im Folgenden „Auftraggeber“ genannt)

im Zuge einer Auftragsverarbeitung gem. Art. 28 Datenschutzgrundverordnung (DS-GVO).

Da es sich hierbei um eine standardisierte Vereinbarung handelt, sind sämtliche Dokumente, Aufzeichnungen, Angebote, Auftragsbestätigungen, Notizen und Kommunikationsunterlagen als Bestandteil dieser Vereinbarung zu sehen, wenn diese für die genaue Definition und Bestimmung sämtlicher Rechte, Pflichten, Zwecke und Mittel relevant sein können. Im Folgenden werden diese Dokumente gemeinschaftlich als „weitere Dokumente“ bezeichnet.

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 schließen die Parteien die nachfolgende Vereinbarung.

Falls zwischen den Parteien eine gesonderte Vereinbarung gem. Art. 28 DS-GVO vereinbart wurde, genießt die spezielle Vereinbarung einen Anwendungsvorrang.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein 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 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 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Personaleinsatzplanung & Routenoptimierung. Der Vertragsgegenstand kann, falls notwendig, auch aus den weiteren Dokumenten entnommen. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers.

(2) Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer können sich ebenfalls aus den weiteren Dokumenten und anderen Verträgen (und der dazugehörigen Leistungsbeschreibungen) ergeben, falls diese nicht bereits in diesem Vertrag genannt sind. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

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

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten die mit anderen Verträgen in Zusammenhang stehen und bei der 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.

(5) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit anderer Verträge, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben. Falls weder andere Verträge existieren, noch eine Laufzeit in diesem Vertrag definiert ist, ist dieser Vertrag auf unbestimmte Zeit geschlossen.

§ 3 Art der verarbeiteten Daten, Kreis der Betroffenen

Die Kategorien personenbezogener Daten und die Kategorien der Betroffenen können sich ebenfalls aus den weiteren Dokumenten ergeben.

§ 4 Konkretisierung der Art der verarbeiteten Daten, Kreis der Betroffenen, Zweck & Umfang

(1) Die §§ 3 und 4 dieser Vereinbarung haben den Sinn und Zweck die Art der Verarbeitung personenbezogener Daten, den Kreis der Betroffenen, den Zweck und den Umfang der Datenverarbeitung zu konkretisieren, falls diese nicht bereits aus dieser Vereinbarung hervorgehen, um einen bestmöglichen Schutz der personenbezogenen Daten und der Rechte der Betroffenen zu gewährleisten.

(2) Zweck & Umfang der Verarbeitung:

a. Der Auftragnehmer erhält von dem Auftraggeber einen Zugang für deren Online-Plattform der ista Deutschland GmbH.

    i. Zusätzliche Informationen zum Gesamtverständnis: Der Auftraggeber agiert als Dienstleister der ista Deutschland GmbH und erbringt verschiedene Dienstleitungen für die Kunden der ista Deutschland GmbH.

b. Der Auftragnehmer soll hier personenbezogene Daten erheben &
c. diese für den Auftraggeber so aufbereiten, dass der Auftraggeber einen optimalen Personaleinsatz und eine optimale Fahrroute planen kann.

d. Bei den personenbezogenen Daten, die durch den Auftragnehmer erhoben werden sollen, handelt es sich um Kunden der ista Deutschland GmbH.

e. Falls der Aufraggeber die „Premium“ Variante/Paket/Option wählt, werden zusätzlich die Kunden des Auftraggebers über den Besuchstermin informiert.

(3) Art der Verarbeitung:

a. Der Auftragnehmer soll für den Auftraggeber personenbezogene Daten aus der Online-Plattform der ista Deutschland GmbH erheben &

b. Der Auftragnehmer soll diese Daten so verarbeiten, dass eine optimale Personal- und Routenplanung für den Auftraggeber gewährleistet werden kann.

c. Falls der Aufraggeber die „Premium“ Variante/Paket/Option wählt, werden (im Zuge der Informationen der Kunden des Auftraggebers über den Besuchstermin) Adressdaten und Namen der Betroffenen zum Versand des Informationsschreibens verarbeitet.

(4) Art der Betroffenen:

a. Bei den Betroffenen handelt es sich um Kunden der ista Deutschland GmbH.

(5) Art der personenbezogenen Daten:

a. Name, Vorname

b. Anschrift

c. Telefonnummer

§ 5 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen dieses Vertrages 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 oder in Textform 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. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die vertraglich 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. Der Auftragnehmer ist berechtigt die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 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 und § 64 BDSG. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Für den Fall, dass der Auftragnehmer Personen beschäftigt gilt: 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. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 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 Schriftform oder 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, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(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 schriftlich zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich schriftlich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO liegen.

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

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

(7) 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) Falls notwendig gilt: Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig einmal pro Jahr 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 durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder 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 stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

§ 9 Einsatz von Subunternehmern

(1) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

(3) Aktuelle Subunternehmer sind:

a) Hetzner Online GmbH: Hier wird die Software/ IT-System des Auftragnehmers gehostet.
b) Google LLC.: Über den Dienst „Googel Maps“ werden die Fahrtrouten errechnet.

§ 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. 12-22 sowie 32 und 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 Innenverhältnis zum Auftragnehmer 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.

(3) Der Auftraggeber ist für die Rechtmäßigkeit sämtlicher rechtlicher und vertraglicher Beziehungen zu der ista Deutschland GmbH verantwortlich.

§ 12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann diesen Vertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen - also weder vorsätzlichen noch grob fahrlässigen - Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 13 Vertragsbeendigung

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung dieses Vertrages oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger 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. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer.

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

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende dieses Vertrages hinaus die ihm im Zusammenhang mit diesem Vertag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende anderer Verträge hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Zustandekommen dieser Vereinbarung

Falls keine schriftlichen Einwände, Anmerkungen etc. vorliegen, gilt Folgendes:

Dieser Vertrag bedarf nicht der Unterzeichnung der Parteien für deren Wirksamkeit. Der Vertrag kommt zustande, sobald sich die Parteien über die Mittel und Zwecke einig sind, ein Auftrag erteilt wurde bzw. angenommen wurde. Der Vertrag kann auch durch ein konkludentes Handeln der Parteien Zustandekommen.

§ 15 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 der Ort der Hauptniederlassung des Auftragnehmers.

Stand: April 2021

Übersicht über die allgemeinen technischen und organisatorischen Maßnahmen

smart-sp GmbH – Stand: April 2021	
Zutrittskontrolle	Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. u.a.: • organisierte Schlüsselvergabe nach Berechtigungen • Überwachungseinrichtungen
Zugangskontrolle	Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. u.a.: • Kennwortverfahren • automatische Sperrung • Firewall • Anti-Viren Software • Differenzierung von Benutzern
Zugriffskontrolle	Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. u.a.: • Benutzerkennung • Firewall • Anti-Viren Software • regelmäßige Updates der Systeme • Protokollierung von Zugriffen
Trennungskontrolle	Gewährleisten, dass eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, möglich ist. u.a.: • Zweckbindung • separierte Datenbanken • Separierung von Tables in Datenbanken • Funktionstrennung
Pseudonymisierung	Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet

	werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. u.a.: • Identifizierung von Datensätzen mit IDs anstatt Klarnamen und anderen persönlichen Daten
Weitergabekontrolle	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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. u.a.: • Verschlüsselung / Tunnelverbindung • Regelungen zum datenschutzkonformen Vernichten von Datenträgern
Eingabekontrolle	Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. u.a.: • Protokollierungs- und Protokollauswertungssysteme • Sicherung von Protokolldaten gegen Verlust oder Veränderung
Verfügbarkeitskontrolle	Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. u.a.: • Backup-Strategie • Unterbrechungsfreie Stromversorgung
Auftragskontrolle	Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden. u.a.: • Verwendung von geprüften Vertragsbedingungen • sorgfältige Auswahl der Auftragnehmer • Prüfung der Vorgänge durch einen externen Experten
Widerstandsfähigkeit- und Ausfallsicherheitskontrolle	Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen. u.a.: • Daten befinden sich bei einem professionellen und Erfahrenen deutschen Dienstleister, der entsprechende Maßnahmen getroffen hat.
Kontrollverfahren/ organisatorische Maßnahmen	Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren. u.a.: • Einsatz einen externen Experten als fester Ansprechpartner • feststehender Plan zur weiteren Entwicklung des Datenschutzes und der Datensicherheit • geplante Nachkontrollen