Vereinbarung zur Auftragsdaten-verarbeitung

MHP Solution Group

01.01.2015

Inhaltsverzeichnis

MHP Solution Group
Justus-von-Liebig-Str. 3
D-31535 Neustadt

Tel.: +49 (0) 5032 - 965 60
Fax: +49 (0) 5032 - 965 611
www.mhp-solution-group.com

Vereinbarung

zwischen dem / der

.....

- nachstehend Auftraggeber genannt –

XXX
XXX
XXX
XXX
XXX
XXX

und dem / der

.....

- nachstehend Auftragnehmer genannt –

XXX
XXX
XXX
XXX
XXX
XXX

1. Gegenstand und Dauer des Auftrages

Der Gegenstand des Auftrages zum Datenumgang ergibt sich aus der durch Auftrag und Auftragsbestätigung zustande kommenden, schuldrechtlichen Geschäftsbeziehung zwischen Auftraggeber und Auftragnehmer vom……, auf die hiermit verwiesen wird (im Folgenden Leistungsvereinbarung).

Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhaltes

- Art, Umfang und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

Die Art der durch die Auftragsverarbeitung erfassten Kundendaten ist abhängig von dem erteilten Auftrag des Kunden und der Notwendigkeit für die Durchführung der Leistungsvereinbarung, wie beispielsweise Personen-/Vertrags- (Stamm-)Daten, Kommunikations- und Verbindungsdaten und Geschäftspartnerdaten, wie z.B. Kundenkontaktdaten, Vertragsabrechnungs- und Zahlungsdaten, Auskunftsangaben, Kundenhistorie, Transaktionsdaten.

Der Auftragnehmer verwendet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Verarbeitung oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, personenbezogene Daten des Auftraggebers in Systeme Dritter einzuspielen. Im Übrigen ist es dem Auftragnehmer nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

- Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrages Betroffenen umfasst Privat- und Firmenkunden sowie Lieferanten, Interessenten und Ansprechpartner.

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten, 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 des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Die als Anlage 1 beigefügte Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG (Datenschutz- und Datensicherheitskonzept) wird Teil dieser Vereinbarung. Insgesamt handelt es sich bei den zutreffenden Maßnahmen einerseits um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebotes; sowie andererseits um auftragsspezifische Maßnahmen, die sich aus der zu Grunde liegenden Leistungsvereinbarung ergeben.

Die festgelegten Maßnahmen müssen die personenbezogenen Daten vor der zufälligen oder unrechtmäßigen Zerstörung, vor dem zufälligen Verlust, der unberechtigten Änderung oder Weitergabe oder dem unberechtigten Zugang schützen. 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. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2, S. 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

4. Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weitergeben.

5. Kontrolle und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung folgende Pflichten nach § 11 Abs. 4 BDSG:

Der Auftragnehmer ist zur schriftlichen Bestellung (soweit gesetzlich vorgeschrieben) eines Datenschutzbeauftragten verpflichtet, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitgeteilt.

Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus dieser Vereinbarung ergebenen besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

Der Auftragnehmer ist verpflichtet, alle für diese Vereinbarung notwendigen technischen und organisatorischen Maßnahmen nach § 9 BDSG und Anlage umzusetzen und einzuhalten. Dabei hat er durch geeignete Kontrollen sicherzustellen, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden, die übertragene Datenverarbeitung aufgabenbezogen getrennt von anderer Datenverarbeitung erfolgt und die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Der Auftragnehmer ist überdies zur unverzüglichen Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG verpflichtet. Dies gilt auch, soweit eine zuständige

Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt. Er unterwirft sich eventuellen Kontrollmaßnahmen der Datenschutzaufsichtsbehörde und wird den Auftraggeber über eine eventuelle Kontrollmaßnahme unverzüglich informieren, wenn personenbezogene Daten des Auftraggebers betroffen sind.

Der Auftragnehmer ist überdies zur Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere die Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrages verpflichtet.

Überdies ist der Auftragnehmer zur Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber verpflichtet. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (bspw. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, etc.) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) vorlegen.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

Der Auftraggeber kann im Einzelfall zur Vertragsdurchführung Dritte einsetzen, soweit der Auftragnehmer vorher schriftlich zugestimmt hat. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.

Der Auftragnehmer hat die vertraglichen Vereinbarungen mit Unterauftragnehmern so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftragnehmer und Auftraggeber entsprechen. Zwischen den Unternehmen der MHP Solution Group, der TIA Innovations GmbH und der MHP Software GmbH ist eine gegenseitige Vereinbarung zur Auftragsdatenverarbeitung geschlossen.

Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme, vertragliche Vereinbarungen zu treffen sowie Kontrollmaß-nahmen zu ergreifen.

7. Kontrollrecht des Auftraggebers

Der Auftragnehmer räumt dem Auftraggeber und dessen Bevollmächtigten bezüglich der getroffenen Datenschutz- und Datensicherungsvorkehrungen ein jederzeitiges Besichtigungs- und Kontrollrecht, grundsätzlich nach vorheriger Ankündigung, ein. Der Auftragnehmer ist verpflichtet, im Falle von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen.

Der Auftraggeber 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. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftrag-nehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Unabhängig davon wird der Auftragnehmer den Nachweis der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG durch ein regelmäßiges, alle 3 Jahre zu erneuerndes Testat z. B. von einer anerkannten Wirtschaftsprüfungsgesellschaft, Revision oder von seinem betrieblichen Datenschutzbeauftragten oder ein anderes den gesetzlichen Anforderungen genügendes Dokument (z.B. aktualisierte Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen) erbringen.

8. Mitteilung bei Verstößen des Auftragnehmers

Bei begründetem Verdacht der Verletzung von in dieser Vereinbarung festgelegten Datenschutz- und Datensicherheitsbestimmungen durch den Auftragnehmer selbst, Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte, ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich zu benachrichtigen. Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die in der Vereinbarung getroffenen Festlegungen vorgefallen sind. Das Gleiche gilt auch bei Verstößen gegen die allgemeinen Vorschriften zum Schutz personenbezogener Daten.
Den Parteien ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Solche Vorfälle sind dem Auftraggeber unverzüglich mitzuteilen. Der Auftragnehmer hat in Absprache mit dem Auftraggeber, angemessene Maßnahmen zur Sicherung der Daten sowie zur möglichen Minderung nachteiliger Folgen zu ergreifen.

9. Weisungsbefugnis des Auftraggebers

Der Auftraggeber ist für die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz sowie die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer verantwortlich.

Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per Email bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate 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. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen das BDSG oder eine andere Vorschrift über den Datenschutz verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber geändert oder bestätigt wird.

10. Löschung von Daten

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung/Kündigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

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.

Anlage 1 zur Vereinbarung nach § 11 BDSG (gemäß Ziffer 3.)

Datum, Unterschrift

MHP Solution Group
Justus-von-Liebig-Str. 3
D-31535 Neustadt

Tel.: +49 (0) 5032 - 965 60
Fax: +49 (0) 5032 - 965 611
www.mhp-solution-group.com

Anlage 1 zur Vereinbarung nach § 11 BDSG (gemäß Ziffer 3)

Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG (Datenschutz- und Datensicherheitskonzept) und Anlage

Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG zu. Dies bedeutet insbesondere

- **Zutrittskontrolle**: Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, räumlich zu verwehren.

- **Zugangskontrolle:** Zu verhindern, dass in Datenverarbeitungssysteme von Unbefugten eingedrungen werden kann oder diese genutzt werden können.

- **Zugriffskontrolle:** 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. Verhindert werden soll jede unerlaubte Tätigkeit in Datenverarbeitungssystemen außerhalb der eingeräumten Berechtigung.

- **Weitergabekontrolle:** 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.

- **Eingabekontrolle:** Zu gewährleisen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Hierbei ist die Nachvollziehbarkeit /Dokumentation der Datenverwaltung und –pflege zu gewährleisten.

- **Auftragskontrolle:** Zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- **Verfügbarkeitskontrolle:** Zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- **Trennungskontrolle:** Zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.