MUSTER ZUR VEREINBARUNG ZUR AUFTRAGSDATENVERARBEITUNG

Max Mustermann
Musterstraße 1
12345 Musterstadt

– Auftraggeber –

und

HCS Computertechnologie GmbH
Weberstr. 17
94513 Schönberg

– Auftragnehmer –

über eine Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 DSGVO.

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im o.g. Vertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

In der Regel handelt es sich hierbei um

- Fernwartungen im Rahmen des technischen Supports bzgl. Hard- und Software
- Patchmanagement
- Monitoring / Managed Services
- Cloud Backup

- Verwaltung von Mailaccounts und Domains

Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten Art und Zweck der Datenverarbeitung

Als IT-Dienstleister erbringt Auftragnehmer für den Aufraggeber im Rahmen von Wartungsarbeiten, Einrichtungen und Installationen Datenverarbeitungsleistungen.

Die Datenkategorien sind durch die Kundenaufträge und die in deren Rahmen von Kunden übermittelten Daten vorgegeben. Es handelt sich in der Regel um Bestandsdaten, Vertragsstammdaten von Kunden (insbesondere Namen, Anschriften Bankverbindungen), welche keinen Personenbezug aufweisen, sofern es sich beim Kunden nicht um einen Einzelunternehmer / Einzelkaufmann handelt. Personenbezug weisen indes insbesondere Kontaktdaten (z.B. Name, Telefonnummer und E-Mailadresse) von Ansprechpartnern auf. Ggf. werden auch weitergehende Identifikationsdaten (Steuernummern) oder persönliche Merkmale von Kundes-Kunden bekannt. Es handelt sich hierbei um Personenstammdaten (Name, Vorname, Anschrift, Geburtsdatum), Kontakt- und Kommunikationsdaten, die Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten sowie ggf. auch Versanddaten.

Durch einen Schwerpunkt in der Betreuung von Kunden aus dem Medizinsektor erhalten Mitarbeiter der HCS Computertechnologie GmbH auch regelmäßig Einsicht in sensible Patientenstammdaten mit sehr hohem Schutzbedarf. Weiter verarbeitet werden diese Daten vom Auftragnehmer nicht. In der Regel handelt es sich hierbei um Patientenstammdaten (Nachname, Vorname, weitere Namensdaten, Geburtsdatum (Alter) Geburtsort, ggf. Geburtsname, Geschlecht, Familienstand, Adresse (Straße, Hausnummer, Postleitzahl, Ort, Land) Kontaktinformationen (Telefon, E-Mail), Versichertenidentifikationsnummer), die den Patienten eindeutig identifizieren, ebenso medizinische Daten und Ergebnisdaten (Anamnese, Arztbrief, Diagnosen, Prozeduren, Befundberichte, Laborergebnisse, Röntgenbilder (CR, CT, MRT, PET, usw.) weitere bildgebende medizinische Verfahren, Allergien, Medikation, Vitalwerte, Messwerte, Verlaufsdokumentationen, Konsildaten).

Im Rahmen der Dienstleistungspakete aus dem Bereich Managed Services werden IT-Systeme der Auftraggeber automatisiert überwacht. Im Fehlerfall wird der Auftragnehmer alarmiert und die notwendigen Interventionen zur Fehlerbehebung werden gemeinsam mit dem Auftraggeber geplant. Hierzu wird auf den Servern / PCs des Auftraggebers eine Software installiert, die etwa im 5-Minuten-Takt technische Mess- und Zustandswerte, jedoch keinerlei Daten des Auftraggebers, in ein Cloudsystem überträgt.

Ist seitens des Auftraggebers ein Online-Backup Gegenstand des Vertrages, so erfolgt das Online-Backup in verschlüsselter Form auf Server in einem Deutsches Rechenzentrum.

Kategorien betroffener Personen

Von der Datenverarbeitung betroffen sind Kunden und Interessenten und Patienten des Auftraggebers, ggf. auch Daten von Beschäftigten und Lieferanten des Auftraggebers. Eine Speicherung dieser Daten auf den Systemen der HCS Computertechnologie GmbH erfolgt nicht.

1.1 Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinaus gehende Verpflichtungen ergeben.

2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses 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«).

2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3. Pflichten des Auftragnehmers

3.1 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) DSGVO 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 solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2 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 des Datenschutzrechts (insbesondere Art. 32 DSGVO) 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, und diese regelmäßig zu evaluieren und erforderlichenfalls anzupassen. Auf die Anlage zur vorliegenden Vereinbarung wird verwiesen. Der Auftragnehmer stellt dem Auftraggeber geeignete Nachweise darüber zur Verfügung. 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.

3.3 Der Auftragnehmer kann den Nachweis für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit durch Verweis auf entsprechende und gesetzlich anerkannte Zertifizierungen erbringen.

3.4 Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

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

3.6 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

3.7 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung 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.

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

3.9 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.

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

3.11 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund 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.

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

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

3.14 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 DSGVO liegen.

3.15 Sofern nicht gesondert festgehalten, kann der Auftragnehmer keine weitergehende Vergütung für die Erfüllung seiner Pflichten aus dieser Vereinbarung verlangen.

4. Pflichten des Auftraggebers

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

4.2 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO gilt § 3 Abs. 13 entsprechend.

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

5. Anfragen betroffener Personen

5.1 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 soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Nachweis kann u.a. in Gestalt der Durchführung eines Selbstaudits, unternehmensinterner Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung, ein Zertifikat zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001), durch genehmigte Verhaltensregeln nach Art. 40 DSGVO, Zertifikate nach Art. 42 DSGVO oder sonstige Nachweise, auf welche sich die Vertragsparteien einigen, geführt werden. Die Wahl der geeigneten Nachweismethode obliegt im Zweifel dem Auftraggeber.

6.2 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. Erforderlichenfalls hat der Auftraggeber einen externen unabhängigen Prüfer zu bestellen. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt, sofern nicht besondere Umstände eine längere Prüfung erforderlich machen.

6.3 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.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1 Der Auftragnehmer erbringt die nachfolgend aufgeführten Leistungen ausschließlich durch sorgfältig ausgewählte Unterauftragnehmer.

7.2 Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

7.3 Ein zustimmungspflichtiges 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.

7.4 Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf. Wird die Zustimmung nicht innerhalb angemessener Frist erklärt, gilt sie als abgegeben. Bloße 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, bedürfen keiner Zustimmung. Der Auftraggeber hat in diesen Fällen jedoch bei Vorliegen wichtiger datenschutzrechtlicher Gründe ein Widerspruchsrecht gegen die Auswahl bestimmter Subunternehmer. In diesem Fall hat der Auftragnehmer den Subunternehmer durch einen geeigneten anderen Subunternehmer zu ersetzen; Mehrkosten sind vom Auftraggeber zu tragen. Hierüber informiert der Auftragnehmer den Auftraggeber unverzüglich.

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

8. Schlussbestimmungen

8.1 Änderungen und Ergänzungen dieser Anlage 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.

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

8.3 Hinsichtlich Erfüllungsort, Rechtswahl und Gerichtsstand gelten die Regeln des Hauptvertrages.