Vereinbarung zur Auftragsverarbeitung

nach der EU-Datenschutz-Grundverordnung (DSGVO)
Elektronische-Variante, Stand Mai 2018
zwischen

siehe Angaben zum Kunden in der elektronischen Annahmebestätigung
(Verantwortlicher/Auftraggeber)

und

Seyfried Informatik KG

(Auftragsverarbeiter/Auftragnehmer)

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers (Auftragsverarbeitung) durch den Auftragnehmer, die in den vertraglichen Vereinbarungen im Einzelnen festgelegt sind. Umfasst sind alle Tätigkeiten, die der Auftragnehmer gemäß den Leistungsbeschreibungen und vertraglichen Vereinbarungen mit dem Auftraggeber erbringt.

Der Auftrag ist unbefristet erteilt, sofern nichts anderes vereinbart ist. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon ebenso unberührt wie die in den jeweiligen vertraglichen Vereinbarungen geregelten Kündigungsfristen.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO. Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistungen erforderlichen Tätigkeiten sowie alle weiteren Vertragszwecke.

(2) Art der Daten

Art der personenbezogenen Daten sind alle Arten personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet. Hiervon umfasst sind auch besondere Kategorien personenbezogener Daten. Arten sind insbesondere Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten und Auskunftsangaben (von Dritten, z.B. Auskunfteien oder aus öffentlichen Verzeichnissen).

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen insbesondere Kunden, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Handelsvertreter, Ansprechpartner etc.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen 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/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in der Anlage].

(3) 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.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt (→ Anwenderportal, Dokumente zur Lohnabrechnung, Verfahrensverzeichnis).

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages wird gewährleistet.

6. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Der Auftraggeber erteilt dem Auftragnehmer die Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO in Anspruch zu nehmen, soweit dies für die Geschäftsabwicklung notwendig ist. Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es ihm,

seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Verarbeiter zu übertragen. Das gilt insbesondere für die Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Auftrages.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er 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.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Das Ergebnis ist von dem Auftraggeber und -nehmer zu dokumentieren.

8. Mitteilung bei Verstößen des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber -spätestens mit Beendigung der Leistungsvereinbarung- hat der Auftragnehmer sämtliche in seinen Besitz gelangten 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.

(3) 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

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO für Auftragsverarbeiter

1. Vertraulichkeit

Zutritts-/Zugangskontrolle

Der Zutritt zu den Betriebsräumen wird kontinuierlich kontrolliert. Nur die Mitarbeiter des Auftragsnehmers haben Zugang zu den Betriebsräumen. Unbefugte Systembenutzung wird durch sichere Kennwörter, automatische Sperrmechanismen und Verschlüsselung von Datenträgern ausgeschlossen.

Zugriffskontrolle

Eine Reihe von Hardware- und Software-Identifikationsmaßnahmen und die Verschlüsselung der Daten bei der Datenübertragung schließen den unbefugten Zugriff auf die gespeicherten Datenbestände und deren unberechtigte Kenntnisnahme aus. Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen. Unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems sind ausgeschlossen.

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt bearbeitet. D.h., schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung erforderlich ist.

2. Integrität

Weitergabekontrolle

Unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei der elektronischer Übertragung oder dem Transport sind nicht möglich, da das Sicherungssystem beim elektronischen Datenaustausch aus vielschichtigen und komplexen Prüfungen besteht. Ein unbefugtes Entfernen von Datenträgern aus dem Sicherheitsbereich wird durch Sicherungsvorkehrungen ausgeschlossen. Entsorgungsgut mit schutzwürdigem Inhalt wird nach einer hohen Sicherheitsstufe ordnungsgemäß vernichtet.

Eingabekontrolle

Ein Protokollverfahren verhindert eine unbemerkte Dateneingabe, -veränderung und -entfernung.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Zahlreiche Datensicherungsmaßnahmen gewährleisten, dass personenbezogene und andere schutzwürdige Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Besonderes Augenmerk wird auf die Brandschutz-, Verlustsicherungs- und Katastrophenschutzmaßnehmen gelegt (Notfallpläne). Rasche Wiederherstellbarkeit ist in jedem Falle gewährleistet (Art. 32 Abs. 1 lit. c DSGVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüft, bewertet und evaluiert. Dazu dient das Datenschutzmanagement, datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) und die Auftragskontrolle (keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen).