Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO

Zwischen der Firma

KLEINformat, Marius Klein, Gutenbergstraße 4, 56865 Panzweiler, Deutschland

– Nachfolgend „Auftragnehmer“ genannt –

und

Firma/Organisation:

.....

Name:
Wichtig: vollständiger Name, keine Abkürzungen

.....

Straße, Hausnummer:

.....

Postleitzahl, Ort:

.....

Land:

.....

– Nachfolgend „Auftraggeber“ genannt –

Präambel

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsverarbeitung ergeben. Er findet Anwendung auf alle Tätigkeiten, bei denen durch den Auftragnehmer Beauftragte personenbezogene Daten (nachstehend „Daten“) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung (16)

(1) Gegenstand dieses Vertrags ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Als Hosting Dienstleister und Administrator von Server-Systemen kann auf Seiten des Auftragnehmers ein Zugriff auf personenbezogene Daten allerdings nicht ausgeschlossen werden.

(2) Die Verarbeitung beginnt mit Abschluss dieses Vertrags und erfolgt auf unbestimmte Zeit bis zur Kündigung durch eine Partei.

§ 2 Anwendungsbereich und Verantwortlichkeit

(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 Datenverarbeitung allein verantwortlich („Verantwortlicher“ i.S.v. Art. 4 Nr.7 DS-GVO).

(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“).

§ 3 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 von Art. 28 Abs. 3 lit. a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Die Durchführung von rechtswidrigen Weisungen darf der Auftragnehmer ablehnen.

(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 Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität,

Verfügbarkeit, Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

(3) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

(4) Technische und organisatorische Maßnahmen nach Art. 32 DSGVO
Der Auftragnehmer hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.
   a) Zugangskontrolle: Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung, automatische Sperre von Desktops nach wenigen Minuten Inaktivität
   b) Zugriffskontrolle: Nutzung kryptografischer Verfahren (z.B. Verschlüsselung), Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip, Protokollierung von Zugriffsversuchen, Minimale Anzahl an Administratoren, Durchführung von Dokumentenvernichtung
   c) Trennungskontrolle: Trennung von Entwicklungs-, Test- und Produktivumgebung, Personenbezogene Daten dürfen nicht für Testzwecke verwendet werden
   d) Weitergabekontrolle: Bereitstellung von Daten über verschlüsselte Verbindungen (z.B. SFTP, SSL, TLS), Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do-Prinzips, Wo möglich wird E-Mailverschlüsselung eingesetzt, Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag
   e) Eingabekontrolle: Rollenbasiertes Berechtigungskonzept (Lese-, Schreib-, und Löschrechte)
   f) Auftragskontrolle: Daten die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet, Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert
   g) Datenschutzfreundliche Voreinstellungen: Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden, es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind

(5) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
Der Auftragnehmer unterstützt soweit erforderlich den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten.

(6) Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern, Partnern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner stellt der Auftragnehmer sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben, oder einer angemessenen gesetzlichen Schweigepflicht unterliegen. Die Vertraulichkeits- / Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.

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

(8) Für alle im Rahmen dieses Vertrags anfallenden Datenschutzfragen ist der Ansprechpartner:
Marius Klein

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

(10) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Lösung 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.

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

§ 4 Pflichten des Auftraggebers

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

§ 5 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 soweit vereinbart. Der Auftragnehmer haftet bei Erfüllung seiner Pflichten nicht dafür, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig, oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese ohne Störung des Betriebsablaufs nach Anmeldung und 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. Für die Unterstützung bei der Durchführung einer

Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(2) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 1 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 Drittstaatentransfer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

(1) Mit der Hinzuziehung von Unternehmen für Hosting, Telekommunikationsdienstleistungen und Benutzerservice durch den Auftragnehmer ist der Auftraggeber einverstanden.

(2) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Die volle Verantwortung für die vom Auftragnehmer eingeschalteten Subunternehmer bleibt beim Auftragnehmer.

§ 9 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 DS-GVO liegen.

(2) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrags zum Datenschutz im Übrigen nicht.

(3) Es gilt deutsches Recht.

(4) Dieser Vertrag ersetzt alle vorangegangenen Vereinbarungen dieser Art.

§ 10 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Datum:

.....

Unterschrift Auftraggeber

Unterschrift Auftragnehmer
(Geschäftsführer: Marius Klein)