



UHREN • SCHMUCK • TRAURINGE • ANFERTIGUNGEN • REPARATUREN

Hammer Landstraße 234 • 20537 Hamburg
Tel.: (040) 21 80 88 • Fax.: (040) 210 40 776
www.PeterKratz.com • info@PeterKratz.com

Vertrag zur Auftragsdatenverarbeitung zwischen

Werner Ohse
Peter Kratz
Hammer Landstr. 234
20537 Hamburg
-

nachstehend Auftragnehmer genannt -
und

-
nachstehend Auftraggeber genannt -

1. Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer führt gleichartig und wiederkehrend die im Anhang 1 beschriebenen Dienstleistungen für den Auftraggeber durch.

(2) Da der Auftragnehmer in Erfüllung seiner Aufgaben, Daten im Auftrag, nach Weisung und im Interesse des Auftraggebers verarbeitet bzw. ein Zugriff auf personenbezogene Daten bei der Auftrags Erfüllung nicht ausgeschlossen werden kann, erfolgt die Dienstleistung als

Auftragsdatenverarbeitung gemäß § 11
Bundesdatenschutzgesetz (BDSG).

(3) Dieser Vertrag beginnt mit Unterzeichnung beider Parteien und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten im Auftrag verarbeitet. Er endet jedoch nicht vor Erfüllung der Lösch- und Rückgabepflichten nach Ziff. 10.

2. Umfang, Art und Zweck der Datenverarbeitung, Datenarten und Betroffenenkreis

Umfang, Art und Zweck der Datenverarbeitung, die Art der Daten sowie der Kreis der Betroffenen werden in Anhang 1 beschrieben.

3. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich, für die zu verarbeitenden Daten angemessene und dem Stand der Technik entsprechende technische und organisatorische Sicherheitsmaßnahmen nach § 9 BDSG zu treffen und zu dokumentieren (siehe Anhang 2).

(2) Der Auftragnehmer hat an der Erstellung des Verfahrensverzeichnis des Auftraggebers mitzuwirken, soweit es die Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen betrifft. Er hat dem Auftraggeber die erforderlichen Angaben und Dokumente auf Anfrage offen zu legen.

4. Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer darf die Daten, die er im Auftrag des Auftraggebers verarbeitet, nur berichtigen, löschen und sperren, wenn der Auftraggeber dies anweist.

5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und

diese gem. § 5 BDSG auf das Datengeheimnis verpflichtet sind. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer schriftlich einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(4) Der Auftragnehmer darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erheben, verarbeiten oder nutzen. Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei allen gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen. Auskünfte an Betroffene oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit ein Betroffener seine Rechte nach dem BDSG unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6. Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragnehmer darf Unterauftragnehmer beauftragen, wenn sichergestellt ist, dass die vertraglichen Vereinbarungen mit dem Unterauftragnehmer, den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Der Auftragnehmer

prüft die Einhaltung der Vertragspflichten durch den Unterauftragnehmer regelmäßig.

(2) 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 oder Reinigungskräfte. 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 Kontrollmaßnahmen zu ergreifen.

7. Kontrollrechte des Auftraggebers

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihm beauftragte Person, berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften, die Einsichtnahme in die Datenverarbeitungsprogramme oder durch Zugang zu den Arbeitsräumen des Auftragnehmers.

8. Mitzuteilende Verstöße des Auftragnehmers

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggebers. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

9. Weisungen des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte Betroffener, allein verantwortlich.

(2) Der Auftraggeber hat das Recht, dem Auftragnehmer Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Grundsätzlich können Weisungen mündlich erteilt werden. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragnehmer dies verlangt.

(3) Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

10. Beendigung des Auftrags

(1) Nach Abschluss der Auftragsdatenverarbeitung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Datenträger und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, an den Auftraggeber zurückzugeben.

Nicht mehr benötigte Daten sind unverzüglich zu löschen, sofern der Löschung keine gesetzlichen Speicherfristen entgegenstehen.

(2) Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen gesetzliche Bestimmungen des BDSG begeht und dem Auftraggeber aufgrund dessen die Fortsetzung der Auftragsdatenverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

11. Schlussbestimmungen

(1) Die Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei vertraulich zu behandeln. Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Geheimnisträger ein berechtigtes Interesse hat.

Datensicherheitsmaßnahmen sind alle technischen und organisatorischen Sicherheitsmaßnahmen, die eine Partei nach § 9 BDSG getroffen hat. Diese Geheimhaltungspflicht besteht nach Beendigung dieses Vertrags fort.

(2) Sofern eine Partei weiteren Geheimnisschutzregeln unterliegt und sie dies der anderen Partei zu Vertragsbeginn schriftlich mitteilt, ist auch diese Partei verpflichtet, die Geheimnisschutzregeln zu beachten.

(3) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.

(4) Für Vertragsänderungen und Nebenabreden ist die Schriftform erforderlich.

(5) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Ort, Datum

Ort, Datum

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Anhang 1: Auflistung der beauftragten Dienstleistungen
(Umfang, Art, Zweck der Erhebung,
Verarbeitung, Nutzung von Daten, Art der Daten, Kreis der
Betroffenen)

Dienstleistung

: Administration des Webauftrittes

Umfang, Art, Zweck der Erhebung, Verarbeitung, Nutzung von
Daten:

Weiterentwicklung, Fehlersuche und -behebung, in
Einzelfällen Kontaktaufnahme mit
Endverbrauchern zur technischen Hilfe, falls sowohl vom
Endverbraucher als auch vom
Auftraggeber erwünscht.

Kreis der Betroffenen:

- Kunden bzw. Ansprechpartner von Kunden des Auftraggebers
- sonstige Personen, die den Internetauftritt des Auftraggebers
nutzen

Datenarten:

- Name, Vorname, E-Mail-Adresse, Adresse, Telefonnummer,
Geburtsdatum, bisherige

Bestellungen

Anhang 2: Technisch-organisatorische Sicherheitsmaßnahmen
gemäß § 9 BDSG

Im Folgenden werden die technischen und organisatorischen
Maßnahmen geregelt, die bei der
durch den Auftragnehmer erbrachten Dienstleistung gemäß
Anlage zu § 9 Satz 1 BDSG
umzusetzen sind.

Werden personenbezogene Daten automatisiert verarbeitet
oder genutzt, ist die innerbehördliche
oder

innerbetriebliche Organisation so zu gestalten, dass sie den
besonderen Anforderungen des

Datenschutzes gerecht wird. Dabei sind insbesondere
Maßnahmen zu treffen, die je nach der Art der
zu schützenden personenbezogenen Daten oder
Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit
denen personenbezogene Daten
verarbeitet oder genutzt werden, zu verwehren
(Zutrittskontrolle):

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe
- Türsicherung

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle):

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- persönlicher und individueller User-Log-In bei Anmeldung am System bzw.

Unternehmensnetzwerk

- Kennwortverfahren
- Hardwareverschlüsselung
- zusätzlicher System-Log-In für bestimmte Anwendungen
- automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität

• elektronische Dokumentation sämtlicher Passwörter in verschiedenen Sicherheitsstufen und

Verschlüsselung dieser Dokumentation zum Schutz vor unbefugtem Zugriff, Freigabe der

verschiedenen Sicherheitsstufen nach typischer Arbeit des jeweiligen Mitarbeiters.

3. zu 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 (Zugriffskontrolle):

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- Passwort-Identifikation
- Hardwareverschlüsselung
- Trennung der Passwortdokumentation in verschiedene Sicherheitsstufen und Einteilung der Mitarbeiter in dieselben.

4. zu 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 (Weitergabekontrolle)

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- FT/PS Verbindung falls vom Auftraggeber zur Verfügung gestellt

- Protokollierung

- kein WLAN bzw. bei Bedarf Gast-WLAN ohne Zugriffsberechtigung auf das Netzwerk

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von

wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder

entfernt worden sind (Eingabekontrolle):

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- limitierte Vergabe von Zugriffsrechten

- systemseitige Protokollierung

- Mehraugenprinzip

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur

entsprechend den Weisungen des Auftraggebers verarbeitet werden können

(Auftragskontrolle):

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- schriftlicher Vertrag zur Auftragsdatenverarbeitung gemäß § 11 BDSG mit

Auftragnehmern und Unterauftragnehmern

- Verpflichtung der Mitarbeiter auf das Datengeheimnis

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust

geschützt sind (Verfügbarkeitskontrolle):

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- Back-Up-Verfahren

- laufende (24/7) systemseitige Suche nach Schadprogrammen

- Spiegeln von Festplatten

- unterbrechungsfreie Stromversorgung

- geeignete abgeschlossene Archivierungsräumlichkeiten

- Trennung der gespeicherten personenbezogenen Daten von den Mitarbeiter PCs.

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet

werden können:

Beim Auftragnehmer hierzu getroffene Maßnahmen:

- getrennte Datenbanken
- Zugriffsberechtigungen
- Trennung durch Zugriffsregelungen