

Auftragsverarbeitungsvertrag

zwischen

-Auftraggeber-

und

EXONN UG (haftungsbeschränkt)

**Bahnhofstr. 1b
79539 Lörrach**

-Auftragnehmer-

über Auftragsdatenverarbeitung i.S.d. §11 Abs. 2 Bundesdatenschutzgesetz (BDSG)

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung 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 mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung.

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

§ 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 Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»verantwortliche Stelle« im Sinne des § 3 Abs. 7 BDSG).
- (2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

§ 3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten von Betroffenen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.
- (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 Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) genügen. Diese Maßnahmen werden wie folgt festgelegt:

a) Zutrittskontrolle

Mit der Zutrittskontrolle wird Unbefugten die räumliche Annäherung verwehrt.

- Einbruchmeldeanlage
- Vergitterung von Fenstern
- Abholung und Begleitung von Besuchern

b) Zugangskontrolle

Mit der Zugangskontrolle wird verhindert, dass Unbefugte Zugang zu IT-Systemen erhalten.

- Sperren von Bildschirmen
- Technische Prüfung der Passwortqualität
- Bildschirme für Dritte nicht einsehbar aufstellen/ausrichten

c) Zugriffskontrolle

Unter Zugriffskontrolle versteht man, dass nur berechtigte Benutzer Daten in IT-Systemen erheben, verarbeiten und nutzen dürfen.

- Prüfung der vergebenen Berechtigungen
- Verschlüsselungsverfahren nach dem Stand der Technik

d) Weitergabekontrolle

Mittels der Weitergabekontrolle wird verhindert, dass personenbezogene Daten bei der Übermittlung von Unbefugten eingesehen oder verarbeitet werden können.

- Protokollierung der Datenübermittlung
- Verschlüsselungsverfahren nach dem Stand der Technik

e) Eingabekontrolle

Bei der Eingabekontrolle erfolgt die Überprüfung, wer, wann, welche Daten und auf welchen Systemen eingegeben und verarbeitet hat.

- Eine Kontrolle der Eingabemöglichkeiten selbst wird analog zu Zugangs- und Zugriffskontrollen sichergestellt (s.o.).

f) Auftragskontrolle

Bei der Auftragskontrolle wird sichergestellt, dass der externe Dienstleister die personenbezogenen Daten alleinig nach Weisung des Auftraggebers verarbeitet.

- Schriftliche Verträge zwischen dem Auftraggeber und dem Auftragnehmer (Vertrag zur Auftragsdatenverarbeitung gemäß § 11 BDSG) unter anderem zur Fixierung der Weisungen und Berichtspflichten
- Sorgfältige Auswahl des Auftragnehmers nach dem Niveau seiner technischen und organisatorischen Maßnahmen

g) Verfügbarkeitskontrolle

Unter der Verfügbarkeitskontrolle versteht man den Schutz vor Datenverlust und Zerstörung, sowie sämtliche Maßnahmen zu Wiederherstellung.

- Sicher Aufbewahrung von Datensicherungen
- E-Mail-Archivierung
- Unabhängige Stromversorgung

h) Trennungskontrolle

Bei Trennungsgebot wird eine getrennte Verarbeitung sichergestellt, damit keine Zweckentfremdung der personenbezogenen Daten möglich ist.

- Strikte Trennung von Entwicklungs- und Produktivsystem
- Einrichtung logischer Datenbanken

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

- (3) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Informationen zur Verfügung, sofern er sie sich nicht selbst beschaffen kann.
- (4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis entsprechend § 5 BDSG). Das Datengeheimnis besteht auch nach Beendigung des Auftrages fort.
- (5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten nach § 42a BDSG.
- (6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- (7) Der Auftragnehmer gewährleistet, seinen Pflichten nach §§ 4f, 4g BDSG nachzukommen (§ 11 Abs. 2 Nr. 5 i.V.m. § 11 Abs. 4 BDSG), wie z.B. seiner Pflicht, einen Datenschutzbeauftragten zu bestellen, soweit vom Gesetz vorgeschrieben.
- (8) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.
- (9) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.
- (10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

§ 4 Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (2) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.

§ 5 Anfragen Betroffener

- (1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.

- (2) Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

§ 6 Kontrollpflichten

- (1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis.
- Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen,
 - sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen
 - oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.
- (2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

§ 7 Subunternehmer

- (1) Eine Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer erfolgt nicht.
- (2) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit den aufgeführten Leistungen unterbeauftragt.
- (3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Eine etwaige Prüfung durch den Auftraggeber beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragnehmer.*
- Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
- (4) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 8 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 Stelle« im Sinne des Bundesdatenschutzgesetzes liegen.
- (2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung 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.

(3) 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.

(4) Es gilt deutsches Recht.

Ort, Datum

Unterschrift Auftraggeber

Ort, Datum

Unterschrift Auftragnehmer