Anlage Datenschutz

Datenschutz- und Datensicherheitsbestimmungen (DuD-B)

1. Die vorliegende Anlage „Datenschutz- und Datensicherheitsbestimmungen“ (DuD-B) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem (Haupt-) Vertrag ergeben. Die Vereinbarung findet Anwendung auf alle Auftragsverarbeitungsleistungen oder Tätigkeiten im Sinne des Art. 28 DS-GVO, die mit dem (Haupt-)Vertrag in Zusammenhang stehen. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des (Haupt-)Vertrags.
2. Die DuD-B finden zudem Anwendung bei der Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen (Prüfung, Wartung und Pflege von Hard- oder Software), wenn dabei eine Verarbeitung personenbezogener Daten des AUFTRAGGEBERS nicht ausgeschlossen werden kann.

Die DuD-B bestehen aus:

Teil 1: Allgemeine Regelungen zur Verarbeitung personenbezogener Daten im Auftrag
Teil 2: a) Konkrete Angaben zur Auftragsverarbeitung sowie b) technische und organisatorische Maßnahmen (TOM)

Teil 1

Allgemeine Regelungen zur Verarbeitung personenbezogener Daten im Auftrag

§ 1 Allgemeine Bestimmungen

(1) Der AUFTRAGGEBER ist als Verantwortlicher im Sinne des Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) für die Einhaltung der Vorschriften über den Datenschutz verantwortlich. Der AUFTRAGNEHMER ist als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DS-GVO tätig. Darüber hinaus
verpflichtet sich der AUFTRAGNEHMER im Rahmen der Ausführung des Auftrags zur Einhaltung sämtlicher einschlägiger datenschutzrechtlicher Vorschriften.
(2) Sofern der AUFTRAGGEBER im Rahmen des jeweiligen Auftrags seinerseits selbst Dienstleister für andere Auftraggeber ist, stehen die Rechte aus dieser Anlage auch diesen anderen Auftraggebern zu.
(3) Der AUFTRAGNEHMER implementiert geeignete, wirksame und dokumentierte Maßnahmen, welche die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen, insbesondere im Hinblick auf das Erkennen und rechtzeitige Melden von Datenschutzverstößen.
(4) Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Einhaltung der DS-GVO zum Schutz personenbezogener Daten, insbesondere auch bei einer ggf. erforderlichen Datenschutz-Folgenabschätzung sowie vorherigen Konsultationen.
(5) Änderungen, Ergänzungen und Nebenabreden zu dieser Anlage bedürfen der Textform, sofern vertraglich nicht anders vereinbart ist.
(6) Für schuldhafte Verstöße des AUFTRAG-NEHMERS gegen datenschutzrechtliche Anforderungen gemäß dieser DuD-B und/oder gesetzlicher Regelungen finden etwaige zwischen den Vertragsparteien vereinbarte Haftungsbeschränkungen keine Anwendung.
(7) Im Fall eines Widerspruchs der Regelungen dieser DuD-B mit dem zugrundeliegenden (Haupt-)Vertrag gelten die Bestimmungen dieser DuD-B, sofern nicht explizit abweichend vereinbart.

§ 2 Ort der Datenverarbeitung

(1) Die Verarbeitung der Daten erfolgt grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Falls die Anwendung der DS-GVO in einem oder mehreren Staaten des EWR nicht verbindlich beschlossen wurde, gelten diese Staaten des EWR als Drittländer im Sinne der DS-GVO.
(2) Die Datenverarbeitung außerhalb der EU/EWR-Staaten (Drittländer) ist grundsätzlich unzulässig.
(3) Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des AUFTRAGGEBERS und kann darüber hinaus nur erfolgen, wenn zusätzlich die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
(4) Die Verarbeitung und Nutzung der personenbezogenen Daten des AUFTRAGGEBERS erfolgen grundsätzlich in den Betriebsstätten des AUFTRAGNEHMERS. Die auch nur zeitweise erforderliche Verarbeitung oder Nutzung der personenbezogenen Daten des AUFTRAGGEBERS außerhalb der Betriebsstätten des AUFTRAGNEHMERS (z.B. Telearbeit, Remotezugriff) ist nur gestattet, sofern betriebliche oder einzelvertragliche Vereinbarungen mit den Mitarbeitern des AUFTRAGNEHMERS getroffen sind.

§ 3 Zweckbindung und Weisungsrecht

(1) Der AUFTRAGNEHMER verarbeitet die personenbezogenen Daten ausschließlich zur Erbringung der vertraglich vereinbarten Zwecke.
(2) Der AUFTRAGNEHMER verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des AUFTRAGGEBERS, es sei denn, er ist nach
Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der AUFTRAGNEHMER dem AUFTRAGGEBER diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der AUFTRAGGEBER kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
(3) Der AUFTRAGNEHMER informiert den AUFTRAGGEBER unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen Vorschriften über den Datenschutz verstoßen.

§ 4 Unverzügliche Meldungen und Informationspflichten bei Datenschutzereignissen

(1) Der AUFTRAGNEHMER teilt dem AUFTRAGGEBER unverzüglich Unregelmäßigkeiten, Störungen und Verstöße des

AUFTRAGNEHMERS und/oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen sowie den Verdacht auf Datenschutzverletzungen im Zusammenhang mit den vom AUFTRAGGEBER verarbeiteten Daten mit. Der AUFTRAGNEHMER sichert zu, den AUFTRAGGEBER bei möglichen Informationspflichten nach Art. 33, 34 DS-GVO zu unterstützen.

(2) Die Meldung des Datenschutzereignisses an den AUFTRAGGEBER muss unverzüglich, nachdem dem AUFTRAGNEHMER das Datenschutzereignis bekannt wurde, an den Ansprechpartner für den (Haupt-)Vertrag und den Datenschutzbeauftragten/Ansprechpartner für den Datenschutz des AUFTRAGGEBERS erfolgen.

(3) Jedes Datenschutzereignis ist vom AUFTRAGNEHMER zu dokumentieren. Die Meldung eines Datenschutzereignisses an den AUFTRAGGEBER enthält mindestens folgende Informationen:

1. eine Beschreibung der Art des Datenschutzereignisses, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
3. eine Beschreibung der wahrscheinlichen Folgen des Datenschutzereignisses und
4. eine Beschreibung der von dem AUFTRAGNEHMER ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung des Datenschutzereignisses und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

§ 5 Unterauftragsverarbeiter

(1) Der AUFTRAGNEHMER darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des AUFTRAGGEBERS gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Zustimmung des AUFTRAGGEBERS an einen Unterauftragsverarbeiter untervergeben. Der AUFTRAGNEHMER reicht den Antrag auf die gesonderte Zustimmung vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der AUFTRAGGEBER benötigt, um über die Zustimmung zu entscheiden. Die Liste der vom AUFTRAGGEBER genehmigten Unterauftragsverarbeiter findet sich hier in Teil II.

(2) Beauftragt der AUFTRAGNEHMER einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des AUFTRAGGEBERS), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den AUFTRAGNEHMER gemäß diesen Klauseln gelten. Der AUFTRAGNEHMER stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der AUFTRAGNEHMER entsprechend diesen Klauseln und gemäß der DS-GVO unterliegt.

§ 6 Auskunft, Berichtigung, Einschränkung, Löschung und Rückgabe von Daten

(1) Der AUFTRAGNEHMER darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach entsprechender, dokumentierter Weisung des AUFTRAGGEBERS beauskunften, berichtigen, regelmäßig oder anlassbezogen löschen oder deren Verarbeitung einschränken.

(2) Der AUFTRAGGEBER kann vorbehaltlich gesetzlicher Aufbewahrungspflichten oder sonstiger entgegenstehender Rechtsvorschriften auch während der Laufzeit und nach Beendigung des (Haupt-)Vertrages jederzeit die Berichtigung, Löschung, Sperrung (iSd Einschränkung der Verarbeitung gemäß Art. 4 Nr. 3 DS-GVO) und Herausgabe von personenbezogenen Daten verlangen. Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER diesbezüglich und wird ausschließlich im Rahmen der erteilten Weisungen tätig.

(3) Nach Abschluss der vertraglichen Arbeiten hat der AUFTRAGNEHMER sämtliche in seinen Besitz gelangten Unterlagen, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzkonform zu löschen oder dem AUFTRAGGEBER auszuhändigen. Dokumente, Daten und Kopien, die nicht ausgehändigt werden können, sind nach Abschluss der vereinbarten Leistungen zu löschen. Die Löschung ist unaufgefordert schriftlich oder in Textform zu bestätigen. Gesetzliche Aufbewahrungspflichten, denen der AUFTRAGNEHMER unterliegt, bleiben hiervon unberührt. Vertragsbezogene Daten, die zur Sicherung von Beweisinteressen des AUFTRAGNEHMERS erforderlich sind, dürfen in gesperrter Form bis zum Ablauf der hierfür geltenden Verjährungsfrist aufbewahrt werden. Bis zur Löschung oder Rückgabe der Daten gewährleistet der AUFTRAGNEHMER weiterhin die Einhaltung dieser Klauseln.

§ 7 Sicherheit der Verarbeitung

(1) Der AUFTRAGNEHMER ergreift mindestens die in Teil II aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu den Daten führt.

(2) Der AUFTRAGNEHMER legt dem AUFTRAGGEBER eine Einhaltungsbestätigung (z. B. Zertifikate oder Nachweise/Belege einer Revision, eines Datenschutzbeauftragten oder einer Wirtschaftsprüfungsgesellschaft über die Einhaltung angemessener Maßnahmen) vor Beginn der Datenverarbeitung und danach, sofern im Einzelfall nichts anderes vereinbart wird, unaufgefordert jährlich vor bzw. stellt diese entsprechend bereit.

(3) Der AUFTRAGNEHMER gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der AUFTRAGNEHMER gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen

gesetzlichen Verschwiegenheitspflicht unterliegen und damit vertraut gemacht wurden.

§ 8 Dokumentation und Einhaltung der Klauseln

(1) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
(2) Der AUFTRAGNEHMER bearbeitet Anfragen des AUFTRAGGEBERS bezüglich der Verarbeitung von Daten gemäß diesen Klauseln unverzüglich und in angemessener Weise.
(3) Der AUFTRAGNEHMER stellt dem AUFTRAGGEBER alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DS-GVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des AUFTRAGGEBERS gestattet der AUFTRAGNEHMER ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der AUFTRAGGEBER einschlägige Zertifizierungen des AUFTRAGNEHMERS berücksichtigen.
(4) Der AUFTRAGGEBER kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des AUFTRAGNEHMERS umfassen und werden mit angemessener Vorankündigung durchgeführt.

Teil 2

Konkrete Angaben zur Auftragsverarbeitung und technische und organisatorische Maßnahmen (TOM)

a) Konkrete Angaben zur Auftragsverarbeitung

Bezeichnung des (Haupt-)Vertrags	
Kontaktdaten des betrieblichen Datenschutzbeauftragten des AUFTRAGGEBERS	
Kontaktdaten des Datenschutzbeauftragten/ Ansprechpartner für den Datenschutz des AUFTRAGNEHMERS	
Fachlicher Ansprechpartner des AUFTRAGGEBERS	
Gegenstand des Auftrags	
Art der personenbezogenen Daten	
Art und Zweck der Verarbeitung	
Kategorien der von der Datenverarbeitung betroffenen Personen.	

Unterauftragsverarbeiter

Firmenbezeichnung des Unter-auftragsverarbeiters	**Firmen-adresse**	**Beauftragte Tätigkeit**	**Drittland** (falls einschlägig)	**Rechtsgrundlage für den Drittlandstransfer** (falls einschlägig)

b) Technische und organisatorische Maßnahmen (TOM)

Folgende technische und organisatorische Maßnahmen werden zwischen dem AUFTRAGGEBER und dem AUFTRAGNEHMER verbindlich festgelegt:

Maßnahme	**Umsetzung der Maßnahme**
Vertraulichkeit (Art. 32 Abs. 1 lit. a und b DS-GVO)	
Zutrittskontrolle Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	
Zugangskontrolle Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. *Nicht auszufüllen, sofern eine Auftragsverarbeitung ausschließlich auf Systemen des AUFTRAGGEBERS ausgeführt wird*	
Zugriffskontrolle Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten während und nach der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. *Nicht auszufüllen, sofern eine Auftragsverarbeitung ausschließlich auf Systemen des AUFTRAGGEBERS ausgeführt wird*	
Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. *Nicht auszufüllen, sofern eine Auftragsverarbeitung ausschließlich auf Systemen des AUFTRAGGEBERS ausgeführt wird*	
Pseudonymisierung Es ist zu gewährleisten, dass Namen und andere Identifikationsmerkmale von natürlichen Personen durch ein Kennzeichen ersetzt werden, um die Identifikation des Betroffenen auszuschließen oder wesentlich zu erschweren.	

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)	
Weitergabekontrolle Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	
Eingabekontrolle Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. *Nicht auszufüllen, sofern eine Auftragsverarbeitung ausschließlich auf Systemen des AUFTRAGGEBERS ausgeführt wird*	
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	
Verfügbarkeitskontrolle und Belastbarkeit Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. *Nicht auszufüllen, sofern eine Auftragsverarbeitung ausschließlich auf Systemen des AUFTRAGGEBERS ausgeführt wird*	
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)	
Auftragskontrolle Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des AUFTRAGGEBERS verarbeitet werden können.	
Datenschutz-Management Es ist zu gewährleisten, dass die Gesamtheit aller dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen, mit welchen der datenschutzkonforme Umgang mit personenbezogenen Daten im Unternehmen sichergestellt wird, systematisch gesteuert und kontrolliert wird.	
Technikgestaltung/Datenschutzfreundliche Voreinstellungen Es ist zu gewährleisten, dass bei Einführung neuer Datenverarbeitungsanlagen und Software zum frühestmöglichen Zeitpunkt die Verarbeitungsvorgänge so gestaltet werden, dass die Privatsphäre und die Datenschutzgrundsätze von Beginn an garantiert werden können. *Nicht auszufüllen, sofern eine Auftragsverarbeitung ausschließlich auf Systemen des AUFTRAGGEBERS ausgeführt wird*	