

**Bestimmungen zum Datenschutz und zur Datensicherheit
zur Wartung automatisierter Verfahren
oder Datenverarbeitungsanlagen
(§ 80 Abs. 5 SGB X i. V. m. Art. 28 EU-DSGVO)**

– Datenschutzbestimmungen –

§ 1

Gegenstand der Datenschutzbestimmungen

Diese Datenschutzbestimmungen sind Bestandteil der vereinbarten Leistungen entsprechend

<Spot Consulting>

- im Folgenden Hauptvertrag genannt.

§ 2

Grundsätze

- (1) Geschäftsgrundlage des Rechtsverhältnisses zwischen Auftragnehmer und Auftraggeber ist, dass der Datenschutz beim Auftragnehmer nach der Art der zu verarbeitenden Daten den Anforderungen genügt, die für den Auftraggeber gelten.
- (2) Der Auftraggeber, die für ihn zuständigen Aufsichtsbehörden oder von ihm beauftragte externe Prüfeinrichtungen sind berechtigt, sich vor Beginn der Auftragsverarbeitung und anschließend regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, vgl. § 8 (Kontrollrechte des Auftraggebers).

§ 3

Allgemeine Pflichten des Auftragnehmers

- (1) Der Auftragnehmer führt die (*Fern*)Wartung ausschließlich im Rahmen der im Vertragsgegenstand getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Er verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrages bekannt geworden sind, nur für Zwecke der (*Fern*)Wartung. Wartungsaktivitäten dürfen nur mit Einverständnis des Auftraggebers und im Einzelfall erfolgen.
- (2) Dem Auftragnehmer ist die Verarbeitung von Daten (*Fern*)Wartung nur nach den datenschutzrechtlichen Vorschriften unter Beachtung der technischen und organisatorischen Maßnahmen gem. § 4 dieser Bestimmungen gestattet. Er verpflichtet sich, keine Kopien oder Duplikate der Datenbestände bzw. Datenbanken ohne Wissen des Auftraggebers zu erstellen oder die Daten für andere Zwecke zu nutzen.

- (3) Der vom Auftragsverarbeiter bestellte Datenschutzbeauftragte (vgl. Art. 37 Abs. 4 EU-DSGVO i. V. m. § 81 Abs. 4 SGB X) wird zum Zweck der direkten Kontaktaufnahme in **Anhang A** mit Anschrift und telefonischer und elektronischer Erreichbarkeit mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt.
- (4) Die Erbringung der vertraglich vereinbarten Leistung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Bei der Verarbeitung zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679 stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, die Schweiz und Länder mit einem Angemessenheitsbeschluss der EU-Kommission den Mitgliedstaaten der Europäischen Union gleich.
- (5) Der Auftragnehmer ist verpflichtet, den Auftraggeber zu informieren, wenn Aufsichtsbehörden nach Art. 51 EU-DSGVO i. V. m. § 40 BDSG tätig werden oder eine zuständige Behörde beim Auftragnehmer oder seinen Unterauftragnehmern ermittelt. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens gemäß § 41 ff. BDSG in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

§ 4

Technische und organisatorische Maßnahmen

- (1) Der Auftraggeber verarbeitet in der Regel nur Daten, die einem hohen bis sehr hohem Schutzbedarf nach den Klassifikationen der IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unterliegen. Der Auftraggeber bleibt für die Beurteilung der Zulässigkeit der (Fern)Wartung sowie für die Wahrung der Rechte der Betroffenen verantwortlich.
- (2) Der Auftragnehmer trägt daher die Gewähr dafür, dass die hierzu erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit getroffen sind und eingehalten werden.
- (3) Für die Sicherheit erhebliche Entscheidungen zur Durchführung der beauftragten Leistung sind mit dem Auftraggeber abzustimmen.
- (4) Es werden folgende technische und organisatorische Maßnahmen festgelegt:

z. B. Maßnahmen zur innerbetrieblichen Organisation:

- *Vergabe eingeschränkter und zeitlich beschränkter Zugriffsrechte (keine Administratorrechte)*
- *Protokollierung der Aktivitäten*

(Nur bei Fernwartung:)

Der Fernwartungszugang ist besonders abzusichern und zu überwachen.

Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen, Ausnahmen sind gesondert schriftlich zu begründen.

Der Auftragnehmer teilt dem Auftraggeber vor Beginn der Fernwartung mit, welche Mitarbeiter er dafür einsetzen wird und wie diese sich identifizieren werden. Dabei sind hinreichend sichere Identifizierungsverfahren zu verwenden.

Die Fernwartungsverbindung darf nur von der zu wartenden Stelle zeitlich befristet aktiviert werden. Die Aktivitäten des Wartungspersonals müssen grundsätzlich auf einem Bildschirm beim Auftraggeber nachvollzogen werden können.

Der Beginn der Fernwartung ist telefonisch- anlassbezogen auch kurzfristig - anzukündigen, um dem Auftraggeber die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen.

Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der (Fern)Wartung zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Im System des Auftraggebers werden alle Zugriffe, die für Wartungsarbeiten erfolgen, protokolliert. Die Protokollierung muss revisionssicher erfolgen. Die Protokollierung darf vom Auftragnehmer nicht abgeschaltet werden.

Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, insbesondere, wenn unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann erfolgen, wenn eine Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

- (5) Der Auftragnehmer hat die ergriffenen technischen und organisatorischen Maßnahmen zu dokumentieren und dem Auftraggeber auf Verlangen zur Prüfung zu übergeben. Der Nachweis technischer und organisatorischer Maßnahmen kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI Grundschutz)
- (6) Soweit die Prüfung des Auftraggebers Feststellungen ergibt, dass die Anforderungen der technischen und organisatorischen Maßnahmen einer sicheren Datenverarbeitung für diesen Vertrag nicht entspricht und sich daher ein Anpassungsbedarf ergibt, so ist diese Anforderung zur Verbesserung des Datenschutzes und der Datensicherheit umzusetzen.
- (7) 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. Die Kontrollen, die Ergebnisse und ggf. umgesetzte Maßnahmen sind zu protokollieren und für mindestens 6 Jahre aufzubewahren.

§ 5

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der vertraglichen Regelungen die Bestimmungen gemäß Art. 28 bis 33 EU-DSGVO sicherzustellen.

Insofern sind insbesondere folgende Anforderungen zu gewährleisten:

- Ein Wechsel des Datenschutzbeauftragten/der verantwortlichen Person wird dem Auftraggeber unverzüglich mitgeteilt.
- Der Auftragnehmer ist verpflichtet, zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2b, 29, 32 Abs. 4 EU-DSGVO für die Erfüllung der vertraglich vereinbarten Leistungen nur Personen einzusetzen, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden sowie regelmäßig informiert und angewiesen werden (Datengeheimnis).

§ 6

Unterauftragnehmer

Sollen für die Wartungsarbeiten Unterauftragnehmer eingeschaltet werden, bedarf dies der gesonderten schriftlichen Zustimmung des Auftraggebers. Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer entsprechen.

§ 7

Abschluss des Vertrages und Löschung von Daten

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangte Verarbeitungsergebnisse und Daten sowie erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Sofern der Auftragnehmer über Datenträger des Auftraggebers verfügt, sind diese auftragsgemäß entsprechend der DIN 66399 zu löschen. Dies gilt auch für Test- und Ausschussmaterial sowie erzeugte Zwischenergebnisse. Über die Löschung ist ein Protokoll zu fertigen und auf Verlangen dem Auftraggeber vorzulegen.

§ 8

Kontrollrechte des Auftraggebers

- (1) Der Auftragnehmer gewährt dem Auftraggeber bzw. den für den Auftraggeber zuständigen Aufsichtsbehörden oder von ihm beauftragte externe Prüfeinrichtungen in den Betriebsräumen des Auftragnehmers zu jeder geschäftsmäßigen Zeit nach vorheriger schriftlicher Ankündigung (ggf. per Telefax/E-Mail) ein Prüferecht. Das Prüferecht umfasst die Besichtigung von Grundstücken und Geschäftsräumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen als auch die Einsichtnahme in die beim Auftragnehmer gespeicherten Sozialdaten des Auftraggebers, soweit dies im Rahmen des Auftrags zur Überwachung von Datenschutz und Datensicherheit erforderlich ist. Dies gilt insbesondere für den Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen.
- (2) Der Auftragnehmer sichert zu, dass er die notwendige personelle und sachliche Unterstützung bei den Prüfungen zur Verfügung stellt.

- (3) Die genannten Rechte des Auftraggebers können auch durch Mitarbeiter von damit beauftragten Fremdfirmen wahrgenommen werden. Sofern Mitarbeiter von Fremdfirmen mit den genannten Kontrollmaßnahmen beauftragt werden, sind diese vom Auftraggeber ausdrücklich auf die Geheimhaltung aller in diesem Zusammenhang erlangten Kenntnisse, Daten sowie Betriebs- und Geschäftsgeheimnisse zu verpflichten.

§ 9

Mitteilungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten. Der Auftragnehmer unterrichtet den Auftraggeber gemäß Art. 33 Abs. 2 und 3 EU-DSGVO unverzüglich über den Verdacht auf Datenschutzverletzungen – auch seiner Mitarbeiter - oder andere Unregelmäßigkeiten bei der Datenerhebung, -verarbeitung und -nutzung und bei Störungen des Verarbeitungsablaufs. In diesem Falle hat der Auftragnehmer seine Arbeiten sofort zu unterbrechen, erforderliche Maßnahmen zur Sicherung der Daten zu treffen und weitere Anweisungen durch den Auftraggeber abzuwarten.

§ 10

Haftung

Der Auftragnehmer haftet gegenüber dem Auftraggeber nach Maßgabe der gesetzlichen Bestimmungen für Schäden, die infolge seines oder seiner Unterauftragnehmer (§ 6) schuldhaften Verhaltens gegen Datenschutzbestimmungen und/oder durch die schuldhafte Verletzung dieses Vertrages entstehen. Das Nähere ist im Hauptvertrag geregelt.

§ 11

Nebenabreden

Änderungen und Nebenabreden zu diesen Datenschutzbestimmungen bedürfen der Schriftform und sind von beiden Vertragsparteien zu unterschreiben.

§ 12

Laufzeit des Vertrages und Kündigung

- (1) Beginn und Ende des Auftragsverhältnisses sind im Hauptvertrag geregelt.
- (2) Unabhängig von Abs. 1 unterliegen der Auftragnehmer und dessen eingesetzte Mitarbeiter auch nach dem im Hauptvertrag genannten Vertragsende hinaus hinsichtlich der im Rahmen des Auftragsverhältnisses übermittelten Daten und bekannt gewordenen Vertraulichkeiten der Geheimhaltungspflicht. Ebenso gelten die Regelungen zur Haftung nach § 10 über die Laufzeit des Vertrages hinaus.
- (3) Die Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen durch den Auftragnehmer ist ein wichtiger Grund für den Auftraggeber, das im Hauptvertrag vorbehaltene Recht zur außerordentlichen Kündigung auszuüben.

§ 13

Salvatorische Klausel

- (1) Sollten einzelne Bestimmungen dieser Datenschutzbestimmungen einschließlich

dieser Regelung ganz oder teilweise unwirksam sein oder werden oder sollten die Datenschutzbestimmungen eine Regelungslücke enthalten, bleibt die Wirksamkeit der übrigen Bestimmungen oder Teile solcher Bestimmungen unberührt. Anstelle der unwirksamen oder fehlerhaften Bestimmungen treten die jeweiligen gesetzlichen Regelungen. Unwirksam gewordene Vereinbarungen werden die Vertragspartner durch wirksame Regelungen ersetzen, die dem ursprünglich verfolgten Zweck möglichst nahekommen. Diese sind bei nächster Gelegenheit als Ergänzung in diese Datenschutzbestimmungen aufzunehmen.

- (2) Sollten sich gesetzliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.

Anhang

Anhang A Übersicht Ansprechpartner