

Anlage 3

Bestimmungen zum Datenschutz nach Art. 28 DSGVO

Auftragnehmer: **Firma XXXXX**

§ 1 Gegenstand der Datenschutzbestimmungen

(1) Gegenstand der Vereinbarung ist der datenschutzgerechte Umgang mit Sozialdaten/personenbezogenen Daten des Auftraggebers für die

Einführung eines browserbasierten elektronischen Fachwissen-/Literaturportals.

Sie konkretisiert die Verpflichtungen des Auftraggebers und Auftragnehmers zum Datenschutz, die sich aus daraus ergeben.

(2) Beinhaltet der Auftrag die Durchführung einer Fernwartung, erfolgt diese gemäß dem im MD Bayern freigegebenen Fernwartungsverfahren.

(3) Die nachfolgenden Bestimmungen regeln den Schutz der Daten bei der Datenverarbeitung im Auftrag entsprechend Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung / DSGVO), § 80 Sozialgesetzbuch (SGB) X / Art. 2 Bayerisches Datenschutzgesetz (BayDSG) / § 25 Bundesdatenschutzgesetz (BDSG);

(4) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder Verarbeitung (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

§ 2 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren. Hierzu kann er bei ihm Auskünfte einholen, nach Vereinbarung während der üblichen Geschäftszeiten die Grundstücke und Geschäftsräume betreten und Besichtigungen und Prüfungen vornehmen und geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einsehen, soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch durch Vorlage geeigneter Dokumente (zum Beispiel Berichte oder Auszüge unabhängiger Instanzen, wie Wirtschaftsprüfer, Revision, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit, erfolgen. Die Anerkennung trifft der Auftraggeber. Der Auftraggeber orientiert sich an den Richtlinien und Empfehlungen des BSI.

(3) Der Auftraggeber ist verpflichtet und berechtigt, ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung sowie zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen (Art. 28 Abs. 3 Satz 2 lit. f) DSGVO); sie sind schriftlich zu fassen. Er hat seine Weisungen auf Wunsch des Auftragnehmers zu präzisieren. Die weisungs-, empfangs- und kontrollberechtigten Personen sind dem Auftragnehmer schriftlich zu benennen. Sie haben sich bei der Ausübung ihrer Befugnisse zu legitimieren.

(4) An der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e) und f) DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

MD Bayern, Datenschutzbeauftragte, Haidenauplatz 1, 81667 München, E-Mail: datenschutz@md-bayern.de

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich über festgestellte Fehler oder Unregelmäßigkeiten bei der Auftragserfüllung.

(6) Der Auftragnehmer darf personenbezogene Daten aus dem Auftragsverhältnis nur dann berichtigen, löschen oder deren Verarbeitung einschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(7) Die Informationspflichten bei Verletzung des Schutzes von Sozialdaten/personenbezogenen Daten obliegen dem Auftraggeber (§ 83 a SGB X, Art. 33 und 34 DSGVO). Wird dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt, hat er diese dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber unverzüglich folgende Informationen mitzuteilen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der Betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,
- eine Beschreibung bereits ergriffener oder möglicher Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten

(8) Der Auftraggeber bestimmt, wie bei Vertragsende die beim Auftragnehmer vorhandenen Daten, Datenträger etc. einschließlich Sicherungen an den Auftraggeber zurückzugeben sind.

(9) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Daten Sicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln und in keinem Fall Dritten zur Kenntnis zu bringen.

(10) Beim Auftraggeber ist zur Datenschutzbeauftragten bestellt:

Frau Suzana Raso, Haidenauplatz 1, 81667 München, E-Mail: datenschutz@md-bayern.de

§ 3 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die Daten des Auftraggebers ausschließlich im Rahmen dieser Vereinbarung unter Beachtung der datenschutzrechtlichen Bestimmungen und den ergänzenden schriftlichen Weisungen des Auftraggebers. Er ist nicht befugt, die Daten für andere Zwecke zu verarbeiten, zu nutzen oder Dritten zugänglich zu machen. Dies gilt auch für etwaige Datenbestände, die für Testzwecke vorgehalten werden oder der Datensicherung dienen. Eine Vermischung der Datenbestände – auch mit denen anderer Kunden – darf nicht erfolgen. Er bewahrt die Daten nicht länger auf, als es für die Erfüllung des Auftragsverhältnisses erforderlich ist, oder als dies vom Auftraggeber ausdrücklich bestimmt ist. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung.

(2) Der Auftragnehmer trägt die Gewähr dafür, dass die in Art. 32 DSGVO, genannten technischen und organisatorischen Maßnahmen gemäß **Anhang 1** getroffen worden sind und eingehalten werden. Maßnahmen sind nicht erforderlich, wenn ihr Aufwand in keinem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Sofern ergänzende schriftliche Weisungen des Auftraggebers ergangen sind, trägt der Auftragnehmer auch die Gewähr für deren Einhaltung. Die Verarbeitung der Daten in Privatwohnungen ist nicht zulässig.

(3) Als Nachweis für die Einhaltung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO kann der Auftragnehmer, soweit der Auftraggeber seine Kontrollrechte diesbezüglich nicht anders wahrnimmt oder andere Nachweise fordert, auch aktuelle, aussagekräftige Testate, Berichte oder Berichtsauszüge unabhängiger

Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), Nachweise der Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder eine geeignete Zertifizierung gemäß Art. 42 DSGVO vorlegen.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragnehmer ist es gestattet, entsprechende Maßnahmen anzupassen, wobei das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden darf. Wesentliche Änderungen sind grundsätzlich mit dem Auftraggeber abzustimmen. Sie sind schriftlich zu fixieren und werden Vertragsbestandteil. Der Auftragnehmer stellt dem Auftraggeber auf Anforderung die Informationen gemäß Art. 30 Abs. 2 DSGVO in Bezug auf den Auftraggeber als Verantwortlichen einschließlich der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO zur Verfügung.

(5) Der Auftragnehmer räumt dem Auftraggeber und dessen zuständigen Prüf- und Aufsichtsbehörden nach Vorankündigung und angemessener Frist von 3 Tagen das Recht ein, Auskünfte bei ihm einzuholen, nach Vereinbarung während der üblichen Geschäftszeiten seine Grundstücke und Geschäftsräume zu betreten und Prüfungen/Audits vorzunehmen und geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen, soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist. Für den dafür entstandenen Aufwand beim Auftragnehmer fallen keine sonstigen Kosten/Nebenkosten an, Aufwandsentschädigung wird seitens des Auftraggebers in keiner Hinsicht erstattet. Dies gilt auch dann, wenn die Überprüfung in Form eines Dokumentenaudits stattfinden sollte. Der Auftraggeber ist in diesem Fall verpflichtet die angeforderten Unterlagen dem Auftraggeber innerhalb von 7 Werktagen zur Verfügung zu stellen.

(6) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, oder anderen Unregelmäßigkeiten bei der Verarbeitung oder Nutzung der Daten des Auftraggebers. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen Vorschriften des Datenschutzes verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(7) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum statt. Die Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen gemäß Art. 44 ff. DSGVO erfüllt sind. Der Auftragnehmer teilt die für die Verarbeitung der Sozialdaten/personenbezogenen Daten des Auftraggebers vorgesehenen Standorte und Geschäftsräume vor Vertragsabschluss mit **(Anhang 2)**.

(8) Der Auftragnehmer erfüllt eigenverantwortlich seine Dokumentations- und Meldepflichten (Art. 32 DSGVO, Art. 30 Abs. 2 DSGVO, § 80 Abs. 1 Satz 2 SGB X, § 79 Abs. 3 SGB X) und weist dies dem Auftraggeber auf Anforderung nach. Er unterstützt den Auftraggeber bei dessen Verpflichtungen insoweit (z.B. § 286 SGB V, Art. 32 Abs. 2 BayDSG, Art. 33 Abs. 2 DSGVO).

(9) Vor dem Einsatz neuer Technologien (Art. 35 DSGVO) hat der Auftragnehmer die Zustimmung des Auftraggebers einzuholen. Der Einsatz neuer Technologien ohne Zustimmung des Auftraggebers ist unzulässig. Der Auftragnehmer ist verpflichtet, den Auftraggeber über den beabsichtigten Einsatz neuer Technologien im Sinne des Art. 35 DSGVO unverzüglich zu informieren.

(10) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen und den Empfehlungen des BSI über das Vertragsende des Hauptvertrages hinaus aufzubewahren. Er kann sie bei Vertragsende des Hauptvertrages zu seiner Entlastung dem Auftraggeber übergeben.

(11) Beim Auftragnehmer ist als Beauftragter für den Datenschutz schriftlich bestellt:

Ein Wechsel des Beauftragten wird dem Auftraggeber umgehend schriftlich mitgeteilt.

§ 4 Subunternehmer/Wartungsfirmen

(1) Aufträge an Subunternehmer dürfen nur nach vorheriger schriftlicher Einwilligung des Auftraggebers vergeben werden. Die zum Zeitpunkt des Vertragsabschlusses tätigen Subunternehmer sind dem Auftraggeber bekannt zu geben (**Anhang 3**), die vertraglichen Bedingungen auf Anforderung zugänglich zu machen. Sofern der Auftraggeber nicht widerspricht, gelten diese mit Abschluss des Vertrages als genehmigt im Sinne des Satzes 1. Für die Erteilung weiterer Unteraufträge durch unter Auftragsverhältnisse gilt entsprechendes. Alle Auftragsvergaben haben unter Beachtung der Art. 28 DSGVO, § 80 SGB X, Art. 2 BayDSG zu erfolgen.

(2) Der Auftragnehmer bleibt für die Erfüllung der auf Subunternehmer weiter verlagerten Aufgaben in dem gleichen Umfang verantwortlich, als würden diese durch den Auftragnehmer selbst erbracht. Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Subunternehmer sind daher so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses und ggf. ergänzenden Weisungen zwischen Auftraggeber und Auftragnehmer entsprechen. Sie sind rechtzeitig vor Abschluss des Vertrages vorzulegen.

(3) Der Auftragnehmer hat Subunternehmer bezüglich der Einhaltung der vertraglichen Pflichten regelmäßig zu prüfen und dies dem Auftraggeber auf Verlangen nachzuweisen. Verhalten des Subunternehmers ist dem Auftragnehmer wie eigenes Verhalten zuzurechnen. Der Auftragnehmer stellt durch entsprechende vertragliche Vereinbarungen sicher, dass der Auftraggeber beim Subunternehmer die gleichen Kontrollrechte besitzt wie beim Auftragnehmer selbst.

(4) Wird beim Auftragnehmer die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen in Auftrag vorgenommen und kann dabei der Zugriff auf Daten des Auftraggebers oder deren Kenntnisnahme durch diese Stellen nicht ausgeschlossen werden, sind dem Auftraggeber rechtzeitig die Verträge über Wartungsarbeiten einschließlich der damit beauftragten Firmen zur Prüfung zu überlassen.

(5) Der Auftragnehmer ist verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (§ 3) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechend vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Subunternehmer/Wartungsfirma die vereinbarten Kontrollmaßnahmen und etwaige vor Ort Kontrollen zu dulden hat.

(6) Der Auftragnehmer darf Daten an Subunternehmer erst weiterleiten, wenn dieser nachgewiesen hat, dass seine Mitarbeiter entsprechend § 9 dieses Vertrages verpflichtet wurden.

§ 5 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen Verletzung datenschutzrechtlicher Bestimmungen, insbesondere einer nach dem Sozialgesetzbuch, dem BayDSG oder der DSGVO unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen mitverantwortlich. Machen Dritte dem Auftraggeber gegenüber Schadensersatzforderungen geltend, und hat diese der Auftragnehmer zu vertreten, so stellt der Auftragnehmer den Auftraggeber von allen Ansprüchen frei.

(2) Der Auftragnehmer bestätigt, sich gegen die Inanspruchnahme wegen Verletzung von Datenschutzvorschriften in branchenüblicher Höhe versichert zu haben. Der Nachweis einer Versicherungspolice wird dem Auftraggeber gegenüber auf Anforderung unverzüglich, spätestens, innerhalb von fünf Arbeitstagen vorgelegt.

(3) Der Auftragnehmer ist dem Auftraggeber zum Ersatz sämtlicher Schäden verpflichtet, die dem Auftraggeber infolge einer Verletzung dieses Vertrages entstehen, wenn und soweit der Auftragnehmer die Pflichtverletzung zu vertreten hat.

(4) Das Schadensersatzverfahren richtet sich nach den gesetzlichen Bestimmungen, insbesondere § 83 BDSG, Art. 82 DSGVO, § 81 b SGB X.

§ 6 Laufzeit

Diese Datenschutzbestimmungen gelten solange der unter § 1 genanntes **Vertragsgegenstand** Gültigkeit hat. Die Verpflichtung zur Einhaltung des Datenschutzes sowie zur Wahrung der im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- und Betriebsgeheimnissen besteht über das Vertragsende fort.

§ 7 Vergütung

Eine Vergütung zur Erfüllung dieser Datenschutzbestimmungen wird nicht bezahlt. Sie ist mit der Vergütung zu den unter § 1 genannten **Vertragsgegenstand** abgegolten.

§ 8 Sonstiges

(1) Sollte Eigentum des Auftraggebers, insbesondere die Daten des Auftraggebers, beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer wird die in diesem Zusammenhang Beteiligten darüber informieren, dass die Hoheit der Daten und Datenbestände beim Auftraggeber liegt. Alle Daten des Auftraggebers sind in diesem Zusammenhang rechtzeitig vor Eintritt dieser Maßnahmen von den betroffenen DV-Komponenten zu entfernen. Ein Zurückbehaltungsrecht im Sinne von § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

§ 9 Verpflichtungserklärung/Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, die gesetzlichen Bestimmungen zum Sozialgeheimnis (§ 35 SGB I) einzuhalten:

§ 35 SGB I - Sozialgeheimnis

(1) Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 2 SGB X) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis).

...

(4) Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.

...

(2) Der Auftragnehmer bestätigt, dass ihm die für die Vertragserfüllung einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er sichert zu, für die auftragsgemäße Datenverarbeitung nur Personen einzusetzen, die insbesondere im Umgang mit personenbezogenen Daten geschult und mit dem erforderlichen Datenschutz vertraut sind, sowie auf das Datengeheimnis gemäß Art. 28 Abs. 3 Satz 2 lit. b) DSGVO und auf das Sozialgeheimnis nach § 35 SGB I verpflichtet sind (**Anhang 4**). Die Verpflichtungserklärungen sind dem Auftraggeber auf Anforderung vorzulegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(3) Kommt der Auftragnehmer der Einhaltung seiner Datenschutzverpflichtungen schuldhaft nicht nach oder verstößt sein eingesetztes Personal schuldhaft gegen den Inhalt der Verpflichtungserklärung, ist der Auftragnehmer dem Auftraggeber, ungeachtet der gesetzlichen Strafvorschriften, schadensersatzpflichtig.

§ 10 Schlussbestimmungen

(1) Dieser Vertrag tritt vorbehaltlich des Nichtbestehens von Einwänden des Bayerischen Datenschutzbeauftragten sowie der für die Rechtsaufsicht zuständigen Rechtsaufsichtsbehörde, die einer Übernahme der Dienstleistung entgegenstehen, in Kraft.

(2) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam sein, so bleibt der Vertrag im Übrigen gültig. Die Parteien sind verpflichtet, unwirksame Bestimmungen so zu ändern oder zu ersetzen, dass der

mit einer unwirksamen Bestimmung beabsichtigte wirtschaftliche Zweck möglichst erreicht wird. Das vorstehende gilt im Fall von Lücken entsprechend.

(3) Bestehende Datenschutzvereinbarungen verlieren mit Wirksamkeit dieses Vertrages ihre Gültigkeit. Verpflichtungserklärungen von Mitarbeitern sind hiervon ausgenommen.

(4) Ausschließlicher Gerichtsstand ist der Sitz des Auftraggebers.

Anhang 1 - Übersicht über die technisch-organisatorischen Maßnahmen des Auftragnehmers

Anhang 2 - Standorte des Auftragnehmers

Anhang 3 - Subunternehmerverzeichnis

Anhang 4 - Verpflichtungserklärung für Mitarbeitende externer Firmen