

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DS-GVO

zwischen

dem TMF – Technologie- und Methodenplattform, für die vernetzte medizinische Forschung e.V., vertreten den Vorstand, dieser vertreten durch den Geschäftsführer Sebastian C. Semler, Charlottenstraße 42, 10117 Berlin

als Verantwortlicher - nachfolgend "Auftraggeber" genannt –

und

...

als Auftragsverarbeiter/in - nachfolgend "Auftragnehmer/in" genannt –

- Auftraggeber und Auftragnehmer nachfolgend jeder auch "Partei" und gemeinsam "Parteien" -

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Softwareerstellung auf Basis des Vertrags ... vom xx.xx.xxxx (im Folgenden: "Hauptvertrag").

Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("DS-GVO"). Zur Erfüllung der Anforderungen der DS-GVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Gegenstand/Umfang der Beauftragung

(1) Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "Auftraggeberdaten") erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DS-GVO verarbeitet.

(2) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich in der in Anlage 1 spezifizierten Art sowie in dem dort spezifizierten Umfang und Zweck. Der Kreis der von der Datenverarbeitung betroffenen Personen ist in Anlage 2 zu diesem Vertrag dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

(3) Dem Auftragnehmer ist eine abweichende oder über die Festlegungen in den Anlagen 1 und 2 hinausgehende Verarbeitung von Auftraggeberdaten untersagt. Dies gilt auch für die Verwendung anonymisierter Daten.

(4) Die Verarbeitung der Auftraggeberdaten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DS-GVO erfüllt sind.

(5) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

§ 2 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers iSv Art. 28 DS-GVO (Auftragsverarbeitung), dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "Weisungsrecht"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer schriftlich zu bestätigen. Die weisungs- und empfangsberechtigten Personen ergeben sich aus Anlage 3. Bei einem Wechsel oder einer längerfristigen Verhinderung der in Anlage 3 benannten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Der Auftragnehmer wird dem Auftraggeber einen Wechsel der Person des Weisungsberechtigten frühzeitig anzeigen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

§ 3 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte

weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden "Mitarbeiter" genannt), in Schriftform zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DS-GVO, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in Anlage 4 bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen.

§ 4 Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen gemäß § 4 Abs. 1 Satz 1 enthalten jeweils zumindest die in Art. 33 Absatz 3 DS-GVO genannten Angaben.

(2) Der Auftragnehmer wird den Auftraggeber im Falle des § 4 Abs. 1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu

stellen, die zur Durchführung einer Kontrolle gemäß § 7 Abs. 1 dieses Vertrages erforderlich sind. Ferner wird der Auftragnehmer dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung stellen.

§ 5 Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DS-GVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO zu unterstützen.

(3) Der Auftragnehmer bestätigt, dass er –soweit eine gesetzliche Verpflichtung hierzu besteht- einen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten sind:

...

Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

(4) Sollten die Auftraggeberdaten 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegt.

§ 6 Subunternehmerverhältnisse

Die Rechte des Auftragnehmers zum Einsatz von Subunternehmern für die Erfüllung seiner Verpflichtungen richtet sich nach der EVB-IT Rahmenvereinbarung, die zwischen den Parteien geschlossen wurde.

§ 7 Kontrollrechte

(1) Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 3 Abs. 3 dieser Vereinbarung, zu überzeugen. Hierfür kann er zB Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des

Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DS-GVO. Er wird dem Auftraggeber unverzüglich, spätestens aber innerhalb von 7 Werktagen, die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftragnehmer nicht selbst über die entsprechenden Informationen verfügt.

(2) Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DS-GVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich zu berichtigen, löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

§ 9 Laufzeit und Kündigung

(1) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

(2) Der Auftraggeber ist jederzeit zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragnehmer für eine Dauer von 10 Jahren aufzubewahren und auf Verlangen an den Auftraggeber herauszugeben.

(2) Der Auftragnehmer wird dem Auftraggeber die Löschung schriftlich bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren; § 7 Abs. 2 dieses Vertrags gilt hierfür entsprechend.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

§ 11 Vereinbarungen bezüglich der IT-Sicherheitsstandards

(1) Der Dienstleister verpflichtet sich, die folgenden Sicherheitsstandards einzuhalten und entsprechende Nachweise zu erbringen:

- ISO/IEC 27001 oder vergleichbare Sicherheitszertifizierungen

(2) Sollte der Auftragnehmer die Sicherheit der IT-Infrastruktur des Auftraggebers oder die Sicherheit und Integrität von Dateien in besagter Infrastruktur oder der für die Erfüllung der Leistungen aus dem Hauptvertrag bestimmte IONOS Cloud gefährdet, behält sich der Auftraggeber vor die Zugriffsrechte des Auftragnehmers zu widerrufen.

(3) Der Auftragsverarbeiter stellt sicher, dass alle Daten, die zwischen den Parteien oder innerhalb der Systeme übertragen werden, mittels TLS (Transport Layer Security) verschlüsselt sind. Der

Auftragsverarbeiter verpflichtet sich, bei Zugriffen auf das System, insbesondere bei remote Zugängen, nach Möglichkeit ein sicheres Virtual Private Network (VPN) zu nutzen.

(4) Der Auftragsverarbeiter führt umfassende Protokolle über alle Zugriffe und Änderungen an den Systemen und Daten. Diese Protokolle müssen regelmäßig überprüft und auf Anomalien oder verdächtige Aktivitäten hin analysiert werden. Alarmierungssysteme Der Auftragsverarbeiter implementiert ein Alarmierungssystem für verdächtige Aktivitäten. Verdächtige Vorfälle müssen unverzüglich gemeldet und untersucht werden.

(5) Für Schäden, die dem Auftraggeber durch die Missachtung der Nutzungsbedingungen der IONOS Cloud seitens des Auftragnehmers entsteht, haftet der Auftragnehmer.

§ 12 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DS-GVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. § 11 Abs. 2 Satz 1 gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftraggebers, Berlin.

Unterschriften der Parteien

Für den Auftragnehmer

...

_____, den _____
[Ort] [Datum] ...

Für den Auftraggeber

TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., vertreten durch den Geschäftsführer Sebastian C. Semler, Charlottenstraße 42, 10117 Berlin

Berlin _____, den _____
[Ort] [Datum] Sebastian C. Semler (Geschäftsführer)

Anlagen

Anlage 1 – Konkretisierung von Art, Umfang und Zweck der Datenverarbeitung

Anlage 2 – Beschreibung der Datenarten und der Kategorien betroffener Personen

Anlage 3 – Weisungs- und empfangsberechtigte Personen

Anlage 4 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 1 – Konkretisierung von Art, Umfang und Zweck der Datenverarbeitung

1. Der Auftragnehmer entwickelt die FDPG Software auf Basis einer aktuellen Version in den in der Leistungsbeschreibung beschriebenen Ebenen weiter und hat somit dort einen Admin-Zugang und Zugang zu personenbezogenen Daten der FDPG-Nutzer. Der Auftraggeber nutzt seine Berechtigungen ausschließlich, um den Mitarbeitern der TMF oder deren Partnern auf Weisung der TMF Zugang zur FDPG-Nutzerverwaltung zu ermöglichen. Der Auftragnehmer ist nicht mit der Verwaltung der Nutzer an sich beauftragt.

Anlage 2 – Beschreibung der Datenarten und der Kategorien betroffener Personen

1. Personenbezogene Daten der FDPG-Nutzer: hierbei handelt es sich um Titel und Namen, Institutionen, sowie die geschäftlichen Kontaktdaten der Nutzer.
2. In den Anträgen wird Bezug zu FDPG-Nutzern hergestellt. Anträge sind mit Antragsstellern (Datenart 1) und beteiligten Wissenschaftlern (ebenfalls Datenart 1) verknüpft. Darüber hinaus enthalten die Anträge schützenswerte Projektideen der Forschenden. Institutionen sind außerdem mit Mitarbeitern (Transferstellennutzer und UAC-Mitglieder) verknüpft (Datenart 1).

Anlage 3 – Weisungs- und empfangsberechtigte Personen

In der TMF Geschäftsstelle:

...

Des Auftragnehmers:

...

Anlage 4 – Technische und organisatorische Maßnahmen

