

**VEREINBARUNG ZUM DATENSCHUTZ**  
**(Auftragsverarbeitung gemäß Art. 28 DSGVO)**  
zwischen

**Städtisches Klinikum Braunschweig gGmbH, Freisestraße 9/10, 38118 Braunschweig**

- nachstehend **Auftraggeber** genannt –

und

....., ....., .....

- nachstehend **Auftragnehmer** genannt -

**1. Gegenstand und Dauer des Auftrags**

(1) Der Gegenstand dieser weisungsgebundenen Verarbeitung von personenbezogenen Daten ist in der Anlage 1 Punkt 1 benannt.

(2) Die Dauer dieser Vereinbarung entspricht der Laufzeit der Leistungsvereinbarung gem. Anlage 1 Punkt 1.

**2. Umfang, Art und Zweck der Verarbeitung**

(1) Der Auftragnehmer verarbeitet weisungsgebunden personenbezogene Daten für den Auftraggeber. Umfang, Art und Zweck der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Anlage 1 Punkt 2.

(2) Daten dürfen durch den Auftragnehmer nur und ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. Art. 28 Abs. 3 lit. a DSGVO) verwendet werden.

(3) Die Daten dürfen nur zweckgebunden verarbeitet werden. Ausgeschlossen ist es, die Daten für andere Zwecke, insbesondere eigene Zwecke zu verwenden oder außerhalb des vereinbarten Zweckes an Dritte weiterzugeben.

(4) Die Verarbeitung umfasst nicht die Erteilung von Auskünften an Dritte oder den Betroffenen. Dies bedarf im Einzelfall einer gesonderten Beauftragung.

(5) Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Sofern erforderlich, wird der Nachweis in Anlage 4 dieser Vereinbarung beigelegt.

(6) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und nach Einigung der Parteien in Schriftform zu dokumentieren.

**3. Art der Daten, Betroffene**

Die Art der personenbezogenen Daten sowie die Kategorien bzw. der Kreis der betroffenen Personen sind konkret beschrieben in der Anlage 1 unter Punkt 3 und 4.

**4. Verpflichtung zur Verschwiegenheit bei der Verarbeitung von Patientendaten, Hinweis auf Strafbarkeit**

(1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von 203 StGB) fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

(2) Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB.

Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(3) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

**5. Technische und organisatorische Schutzmaßnahmen**

(1) Der Auftragnehmer stellt sicher, dass bei der vereinbarten Verarbeitung geeignete technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO ergriffen und so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen geltenden Datenschutzrechts erfolgt und den Schutz der Rechte betroffener Personen gewährleistet.

(2) Für die auftragsgemäße Verarbeitung wird ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden Maßnahmen zur Sicherstellung der Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Abhängigkeit von Art, Umfang, Umständen und Zweck der Verarbeitungen getroffen, so dass mittels geeigneter technischer und organisatorischer Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung welche Maßnahmen getroffen werden und die Umsetzung der Maßnahmen offen.

(3) Die Durchführung der Verarbeitung außerhalb der Geschäfts- und Betriebsräume durch den Dienstleister oder seiner Beschäftigten (z.B. mittels Home-Office, Telearbeit) ist grundsätzlich zulässig, soweit der Auftragnehmer angemessene organisatorische und technische Maßnahmen i.S.d. Art. 32 DSGVO ergreift um die besonderen Risiken, welche sich aus dieser Form der Verarbeitung ergibt, zu begegnen.

(4) Die seitens des Auftragnehmers erforderlichen Maßnahmen i.S.d. Abs. 1 - 3 sind in der Anlage 2 beschrieben und geltend als vereinbart. Er weist die getroffenen Maßnahmen in geeigneter Weise zur Prüfung durch den Auftraggeber nach.

(5) Die Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es können alternative Maßnahmen umgesetzt werden, wenn das Schutzniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber bekannt zu geben.

(6) Der Auftragnehmer hat in regelmäßigen und dem Risiko der Verarbeitung angemessen Abständen eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

#### 6. Besondere Pflichten des Auftragnehmers

(1) Hat der Auftragnehmer einen Datenschutzbeauftragten benannt, der seine Tätigkeit gemäß Art. 37, 38 DSGVO (weisungsfrei und unabhängig) ausübt, kann der Auftraggeber diesen direkten Kontakt aufnehmen; die Kontaktdaten sind in der Anlage 1 in Punkt 7 benannt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich angezeigt. Soweit der Auftragnehmer nicht der gesetzlichen Benennungspflicht unterliegt, ist in diesem Fall in der Anlage 1 in Punkt 7 ein Ansprechpartner für den Datenschutz beim Auftragnehmer benannt. Das vorgenannte gilt entsprechend.

(2) Sofern der Auftragnehmer seinen Sitz außerhalb der Europäischen Union hat, benennt er in Anlage 1 in Punkt 8 einen Vertreter nach Art. 27 Abs. 1 DSGVO innerhalb der Europäischen Union.

(3) Alle beim Auftragnehmer mit der Abwicklung des Auftrages beschäftigten Personen haben sich zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht. Sie sind vom Auftragnehmer mit den für sie relevanten Bestimmungen zum Datenschutz – insbesondere im Hinblick auf den vorliegenden Auftragsgegenstand – vertraut gemacht worden.

(4) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften bekannt sind.

(5) Der Auftragnehmer hat dem Auftraggeber vor der Verarbeitung mitzuteilen, wenn er durch eine rechtliche Vorschrift zu einer anderen Verarbeitung verpflichtet ist.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt. Die Informationspflichten gelten nicht, sofern dies dem Auftragnehmer durch eine gerichtliche oder behördliche Anweisung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber liegt.

(7) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungs- oder Strafverfahren, dem

Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer im Rahmen des ihm Zumutbaren zu unterstützen.

(8) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei dessen Pflichten zur Gewährleistung der Sicherheit der Verarbeitung, Datenschutz-Folgenabschätzung und vorheriger Konsultation der Aufsichtsbehörden, sofern gesetzlich vorgeschrieben.

(9) Der Auftragnehmer überprüft regelmäßig die Erfüllung der hier getroffenen Regeln, insbesondere die Einhaltung und ggf. notwendige Anpassung von Schutzmaßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der betroffenen Personen gewährleistet ist.

(10) Der Auftragnehmer stellt dem Auftraggeber auf Anforderung alle Informationen zum Nachweis der Einhaltung seiner aus diesem Vertrag und den gesetzlichen Anforderungen resultierenden Pflichten zur Verfügung.

(11) Auf Anforderung stellt der Auftragnehmer dem Auftraggeber die Angaben für das Verarbeitungsverzeichnis gemäß Art. 30 DSGVO zur Verfügung.

#### 7. Fernzugriff

(1) Benötigt der Auftragnehmer zur Erbringung seiner Verarbeitung eine Fernzugriffsmöglichkeit, so wird diese durch den Auftraggeber bereitgestellt.

(2) Art und Weise des Fernzugriffs wird zwischen den Vertragspartnern abgestimmt.

(3) Der Auftragnehmer stellt sicher, dass die benötigten Zugangsdaten nur Beschäftigten zugänglich sind, welche zur Nutzung des Fernzugriffs-Zugangs befugt sind. Darüber hinaus hat er sicher zu stellen, dass jederzeit nachvollziehbar ist, von wem der Fernzugriff-Zugang genutzt worden ist. Die diesbezügliche Dokumentation ist manipulationssicher min. ein Jahr aufzubewahren.

#### 8. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Unterauftragnehmer zur Verarbeitung der Daten zu den in dieser Vereinbarung festgelegten Zwecken sind nur mit schriftlicher Genehmigung des Auftraggebers gestattet.

(3) Der Auftraggeber stimmt der Beauftragung der in Anlage 3 aufgeführten Unterauftragnehmer unter der Voraussetzung der

Erfüllung der nachfolgenden Regelungen dieser Vereinbarung zu.

(4) Der Auftragnehmer hat den/die Unterauftragnehmer entsprechend dieser Vereinbarung zu verpflichten, d.h. der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie mindestens den Anforderungen dieser Vereinbarung zur Sicherstellung eines ausreichenden Datenschutzniveaus und den gesetzlichen Vorschriften entsprechen. Insbesondere das Recht des Auftraggebers auf Auskunft über die Umsetzung von datenschutzrelevanten Verpflichtungen muss auch gegenüber Unterauftragnehmern gewährleistet werden.

(5) Die Weitergabe personenbezogener Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher und weist diese gegenüber dem Auftraggeber nach.

(7) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

#### 9. Pflichten des Auftraggebers

(1) Der Auftraggeber ist bezüglich der zu verarbeitenden Daten für die Einhaltung der datenschutzrechtlichen Regelungen Hauptverantwortlicher i.S.d. des Art 4 Nr. 7 DSGVO.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus Art. 33 Abs. 1 und Art. 34 DSGVO resultierenden Meldepflichten.

#### 10. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich vor Beginn der Verarbeitung und sodann regelmäßig von der Angemessenheit der beim Auftragnehmer getroffenen Maßnahmen zum Schutz der Daten überzeugen. Hierzu darf der Auftraggeber selbst oder durch ihn benannte Prüfer Überprüfungen im Geschäftsbetrieb des Auftragnehmers vornehmen. Die Überprüfungen sind mit einer angemessenen Frist, min. aber 3 Wochen vorher, mit dem Auftragnehmer abzustimmen. Die Überprüfungen sind so zu gestalten, dass die Betriebsabläufe des Auftragnehmers nur in dem für die Überprüfung notwendigen Maße beeinträchtigt werden.

(2) Wird seitens des Auftraggebers zur Durchführung der Kontrollen ein Prüfer benannt, so ist seitens des Auftraggebers darauf zu achten, dass dieser nicht im konkreten Konkurrenzverhältnis mit dem Auftragnehmer steht. Ein Anspruch diesbezüglich besteht seitens des Auftragnehmers nicht.

(3) Der Auftragnehmer kann eine Kostenerstattung für die Unterstützungsleistungen zur Durchführung der Überprüfung nur verlangen, wenn durch diese die Betriebsabläufe nachhaltig beeinträchtigt wurden. Dies ist durch den Auftragnehmer nachzuweisen.

(4) Nachweise über die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen können auch durch

Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragnehmer verpflichtet sich, die erforderlichen Unterlagen und Nachweis innerhalb einer angemessenen Frist – regelhaft innerhalb 1 Monats - zur Verfügung zu stellen. Ist eine Bereitstellung seitens des Auftragnehmers innerhalb dieser Frist nicht möglich, so teilt der Auftragnehmer dies unter Benennung der Gründe und eines voraussichtlichen Bereitstellungszeitraumes mit.

(5) Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

(6) Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind und den Auftraggeber dabei zu unterstützen.

#### 11. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat betreffend der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer ein Weisungsrecht gegenüber dem Auftragnehmer. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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) Zur Anweisung und zur Entgegennahme befugte Personen sind in Anlage 1 in Punkt 5 abschließend benannt.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind den jeweiligen Vertragspartnern unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. Vertreter mitzuteilen.

(4) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(5) Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei (3) volle Kalenderjahre aufzubewahren.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

#### 12. Löschung/Vernichtung von Daten und Datenträgerrückgabe

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung

alle ihm überlassenen Unterlagen in Papierform, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Die Herausgabe- bzw. Vernichtungsverpflichtung betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung und Vernichtung ist durch den Auftragnehmer so zu gestalten, dass eine Wiederherstellung ausgeschlossen oder zumindest in Anbetracht der verarbeiteten Daten und damit einhergehenden Risiken für die Rechte der Betroffene unangemessenen Aufwand zur Wiederherstellung steht.

(2) Werden im Rahmen der Verarbeitung Daten i.S.d. von Art. 9 DSGVO verarbeitet, so ist die Vernichtung gem. den Vorgaben der DIN 66399 Schutzklasse 3 Sicherheitsstufe 4 oder höher durchzuführen.

(3) Das Protokoll der Löschung ist vorzulegen.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung dienen oder für die eine gesetzliche Verpflichtung zur Speicherung besteht, hat der Auftragnehmer entsprechend der jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

### 13. Mitteilung und Umgang bei Schutzverletzungen

(1) Der Auftragnehmer ist verpflichtet, Verletzungen des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) in seinem Herrschafts- und Organisationsbereich, soweit sie die Verarbeitung des Auftraggebers betreffen, gemäß Art. 33 Abs. 2 DSGVO, auch ohne Ansehen der Verursachung, unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei konkretem Verdacht auf andere Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder Strafvorschriften betreffend personenbezogener Daten des Auftraggebers im Herrschafts- und Organisationsbereich des Auftragnehmers. Die Meldung hat an den Datenschutzbeauftragten des Auftraggebers zu erfolgen (Anlage 1 in Punkt 6).

(2) Darüber hinaus hat der Auftragnehmer den Auftraggeber bei dessen Meldepflicht gegenüber der Aufsichtsbehörde und dessen Benachrichtigungspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

(3) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie vorläufige Maßnahmen zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

(4) Der Auftragnehmer stellt durch angemessene technische und organisatorische Maßnahmen sicher, dass Verletzungen des Schutzes personenbezogener Daten in seinem Herrschafts- und Organisationsbereich i.S.d. Art. 4 Nr. 12 DSGVO festgestellt werden können.

### 14. Betroffenenrechte

(1) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei dessen gesetzlichen Pflichten zur Umsetzung der Rechte betroffener Personen.

(2) Der Auftragnehmer löscht auf Anforderung des Auftraggebers von der Verarbeitung umfasste personenbezogene Daten. Darüber hinaus hat der Auftragnehmer die zu verarbeitenden Daten nur nach dokumentierter Weisung des Auftraggebers zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken (sperrern).

(3) Wendet sich ein Betroffener unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten, leitet der Auftragnehmer das Anliegen unverzüglich an den Auftraggeber weiter und stimmt sich zum weiteren Vorgehen ab.

### 15. Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

(2) Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Auftraggeber in dieser Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.

(3) 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 einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DS-GVO

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

### 16. Verschwiegenheitspflicht

Die Parteien verpflichten sich, alle im Rahmen des Auftragsverhältnisses erlangten Kenntnisse über Sicherheitsmaßnahmen der jeweils anderen Partei vertraulich als Betriebs- und Geschäftsgeheimnisse zu behandeln. Diese Pflicht gilt auch nach Beendigung des Auftragsverhältnisses.

### 17. Schriftformerfordernis, Aufbewahrung, Salvatorische Klausel

(1) Änderungen oder Ergänzungen zu dieser Vereinbarung bedürfen der Schriftform. Auf dieses Schriftformerfordernis kann nur schriftlich verzichtet werden.

(2) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Unterauftragnehmern) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei (3) volle Kalenderjahre aufzubewahren.

(3) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so wird dadurch die Gültigkeit dieser Vereinbarung im Übrigen nicht berührt. Die Vertragsparteien werden in einem solchen Fall die unwirksame Bestimmung durch eine gesetzeskonforme Regelung ersetzen.

|       |       |
|-------|-------|
| Datum | Datum |
|       |       |

Kurzbez.: SKBS-DS-FB-0005  
Rev.Nr.: 003  
Gültig ab: 01.06.2023  
Seite: 5 von 10

Formblatt  
G - Vereinbarung zur  
Auftragsverarbeitung im SKBS



|                                      |                                     |
|--------------------------------------|-------------------------------------|
| Stempel / Unterschrift Auftragnehmer | Stempel / Unterschrift Auftraggeber |
|--------------------------------------|-------------------------------------|

## Anlage 1 zur Vereinbarung zum Datenschutz

|                                                                     |                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Gegenstand des Auftrages</b>                                  | Datenschutzvereinbarung zu folgender Leistungsvereinbarung:<br>Vertrag                                                                                                                                                                                                                                                      | Der Auftrag ist zur einmaligen Ausführung erteilt<br><input type="checkbox"/> ja<br><input type="checkbox"/> nein                                                                                                                                                                                          |
|                                                                     | Beschreibung der Aufgaben, die vom Auftragnehmer auszuführen sind:                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                            |
| <b>2. Umfang, Art und Zweck der Datenerhebung und -verarbeitung</b> | Der Umfang der Verarbeitung ist wie folgt festgelegt (Für welche Zwecke darf der Auftragnehmer Daten erheben, für welche Zwecke speichern, was ist mit den Daten erlaubt und was nicht):                                                                                                                                    |                                                                                                                                                                                                                                                                                                            |
| <b>3. Art der Daten</b>                                             | Welche Datenarten und -kategorien verarbeitet der Auftragnehmer (z.B. Stammdaten, Adressdaten, Vertragsdaten, IT-Nutzungsdaten etc.):                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                            |
|                                                                     | Werden besondere Arten personenbezogener Daten dem Auftragnehmer zur Verfügung gestellt oder von diesem erhoben:<br><input type="checkbox"/> nein<br><input type="checkbox"/> ja, Angaben über:                                                                                                                             | <input type="checkbox"/> rassische /ethnische Herkunft<br><input type="checkbox"/> politische Meinungen<br><input type="checkbox"/> religiöse /philos. Überzeugungen<br><input type="checkbox"/> Gewerkschaftszugehörigkeit<br><input type="checkbox"/> Gesundheit<br><input type="checkbox"/> Sexualleben |
| <b>4. Kreis der betroffenen Personen</b>                            | Welcher Personenkreis ist von der Verarbeitung betroffen:<br><input type="checkbox"/> Patienten<br><input type="checkbox"/> Beschäftigte<br><input type="checkbox"/> Kontakte<br><input type="checkbox"/> Interessenten<br><input type="checkbox"/> Kunden<br><input type="checkbox"/> sonstige (Bitte genauer beschreiben) |                                                                                                                                                                                                                                                                                                            |
| <b>5. Weisungsbefugnis</b>                                          | 6.1. Weisungsbefugte Stellen/Personen des Auftraggebers:<br>[...]                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                            |
|                                                                     | 6.2. Zur Entgegennahme von Weisungen befugte Stellen/Personen des Auftragnehmers:<br><br>Name, Vorname:<br>Organisationseinheit:<br>Telefon:<br>Email:<br><br>Vertretung:                                                                                                                                                   |                                                                                                                                                                                                                                                                                                            |
| <b>6. Kontakt Datenschutzbeauftragte</b>                            | 8.1. Kontaktdaten des Datenschutzbeauftragten des Auftraggebers<br>Name: Ass.Jur. Matthias Reinecke<br>Telefon: +49 531 595-1796<br>Email: <a href="mailto:datenschutzbeauftragter@sksb.de">datenschutzbeauftragter@sksb.de</a>                                                                                             | 8.2. Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers<br>Name:<br>Telefon:<br>Email:<br><br>Alternativ: Ansprechpartner für Datenschutz:                                                                                                                                                        |
|                                                                     | <b>7. Vertreter des Auftragnehmers nach Art. 27 Abs. 1 DSGVO</b><br>Name, Vorname:<br>Organisationseinheit:<br>Ladungsfähige Anschrift:<br>Telefon / Telephone<br>Email:                                                                                                                                                    |                                                                                                                                                                                                                                                                                                            |

|        |        |
|--------|--------|
| Datum: | Datum: |
|--------|--------|

Kurzbez.: SKBS-DS-FB-0005  
Rev.Nr.: 003  
Gültig ab: 01.06.2023  
Seite: 7 von 10

Formblatt  
G - Vereinbarung zur  
Auftragsverarbeitung im SKBS



.....  
Unterschrift Auftragnehmer

.....  
Unterschrift Auftraggeber

## Anlage 2 zur Vereinbarung zum Datenschutz

### TECHNISCH ORGANISATORISCHE SCHUTZMAßNAHMEN

Die Beschreibung der technischen und organisatorischen Maßnahmen gibt Aufschluss darüber, wie der Auftragnehmer die Schutzziele an die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit seiner Systeme bei der Auftragsverarbeitung sowie die Wirksamkeit der Maßnahmen sicherstellt.

|                                                                                                                                                        |                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)<br>Zutrittskontrolle<br>Zugangskontrolle<br>Zugriffskontrolle<br>Trennungskontrolle<br>Pseudonymisierung | Verfügbarkeit und Belastbarkeit<br>Verfügbarkeitskontrolle<br>Wiederherstellbarkeit                                                                                                        |
| Integrität (Art. 32 Abs. 1 lit. b DSGVO)<br>Weitergabekontrolle<br>Eingabekontrolle                                                                    | Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung<br>Datenschutzmanagement<br>Incident-Response-Management<br>Datenschutzfreundliche Voreinstellungen<br>Auftragskontrolle |

Die Verarbeitung erfolgt auch außerhalb der Geschäfts- und Betriebsräume des Auftragnehmers im Rahmen von Home-Office, Telearbeit, mobiles Arbeiten etc.

☐ Ja ☐ Nein

(Ausführungen hier oder als separate Anlage sind Bestandteil der Vereinbarung)

|                            |  |                           |  |
|----------------------------|--|---------------------------|--|
| Datum:                     |  | Datum:                    |  |
| .....                      |  | .....                     |  |
| Unterschrift Auftragnehmer |  | Unterschrift Auftraggeber |  |

### Anlage 3 zur Vereinbarung zum Datenschutz

#### GENEHMIGTE UNTERAUFTRAGNEHMER

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

| Firma Unterauftragnehmer | Anschrift | Name Ansprechpartner | Leistung |
|--------------------------|-----------|----------------------|----------|
|                          |           |                      |          |
|                          |           |                      |          |

Der Wechsel eines hier benannten Unterauftragnehmers ist zulässig, soweit der Auftragnehmer einen Wechsel dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen den Wechsel erhebt und eine vertragliche Vereinbarung nach Maßgabe dieser Vereinbarung zum Datenschutz und Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

|                            |  |                           |  |
|----------------------------|--|---------------------------|--|
| Datum:                     |  | Datum:                    |  |
| .....                      |  | .....                     |  |
| Unterschrift Auftragnehmer |  | Unterschrift Auftraggeber |  |

#### Anlage 4 zur Vereinbarung zum Datenschutz

##### NACHWEIS DES ANGEMESSENEN SCHUTZNIVEAUS BEI ÜBERMITTLUNG VON PERSONENBEZOGENEN DATEN IN EIN DRITTLAND

- ☐ Die Auftragsverarbeitung wird nicht in einem Drittland erbracht.
- ☐ Die Auftragsverarbeitung wird in einem Drittland erbracht. Das angemessene Schutzniveau in
- ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO)
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DSGVO)
- ☐ wird hergestellt durch Standardvertragsklauseln (Art. 46 Abs. 2 lit. c, d DSGVO)
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. Art. 40 DSGVO)
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DSGVO)
- ☐ wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs. 2 lit. a, Abs. 3 lit. a,b DSGVO):

Die Nachweise sind dem Auftraggeber auf Anforderung vorzulegen.

|                            |  |                           |  |
|----------------------------|--|---------------------------|--|
| Datum:                     |  | Datum:                    |  |
| .....                      |  | .....                     |  |
| Unterschrift Auftragnehmer |  | Unterschrift Auftraggeber |  |