19. Auftragsverarbeitung

Für eine Verarbeitung personenbezogener Daten im Auftrag der SKH nach Art. 4 Nr. 8, 28 DS-GVO gelten die nachfolgenden Regelungen:

19.1 Gegenstand und Dauer der Vereinbarung

19.1.1 Der Auftragnehmer verarbeitet personenbezogene Daten für die SKH im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage der vertraglichen Vereinbarungen.

19.1.2 Die vertraglich vereinbarte Leistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung der SKH und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (zum Beispiel Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

19.1.3 Die Auftragsverarbeitung beginnt zu dem im Vertrag festgelegten Termin und endet gemäß den vertraglichen Vereinbarungen. Soweit keine Beendigungstermine vereinbart sind, gilt der Vertrag auf unbestimmte Zeit abgeschlossen. Die Kündigungsfrist beträgt dann vier Wochen zum Monatsende.

19.1.4 Die SKH kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung der SKH nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte der SKH vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

19.2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Die Art und der Zweck der Verarbeitung, die Arten der personenbezogenen Daten entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO sowie die Kategorien betroffener Personen entsprechend der Definition von Art. 4 Nr. 1 DS-GVO werden in der Vereinbarung zur Auftragsverarbeitung festgelegt, die Anlage des Hauptvertrages ist.

19.3 Rechte und Pflichten sowie Weisungsbefugnisse der SKH

19.3.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Absatz 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist die SKH verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an die SKH gerichtet sind, unverzüglich an diesen weiterzuleiten.

19.3.2 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen der SKH und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

19.3.3 Die SKH erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

19.3.4 Die SKH ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

19.3.5 Die SKH informiert den Auftragnehmer, wenn sie Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

19.3.6 Die SKH ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

19.4 Weisungsberechtigte der SKH, Weisungsempfänger des Auftragnehmers

19.4.1 Die weisungsberechtigten Personen der SKH, die Weisungsempfänger beim Auftragnehmer und die für die Weisung zu nutzenden Kommunikationskanäle sind in der Vereinbarung zur Auftragsverarbeitung festgelegt.

19.4.2 Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger beziehungsweise die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

19.5 Pflichten des Auftragnehmers

19.5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen der SKH, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (zum Beispiel Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter der SKH diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Absatz 3 Satz 2 lit. a DS-GVO).

19.5.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen der SKH nicht erstellt.

19.5.3 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für die SKH verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

19.5.4 Die Datenträger, die von der SKH stammen beziehungsweise für die SKH genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für die SKH regelmäßige datenschutzrechtliche und IT-sicherheitstechnische Überprüfungen in seinem Bereich durchzuführen. Das Ergebnis der Kontrollen ist zu dokumentieren. Der Auftragnehmer übermittelt der SKH mindestens einmal jährlich einen aussagekräftigen Bericht über die Überprüfungen und deren Ergebnisse.

19.5.5 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch die SKH, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen der SKH hat der Auftragnehmer im notwendigen Umfang mitzuwirken und die SKH soweit möglich angemessen zu unterstützen (Art. 28 Absatz 3 Satz 2 lit. e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die SKH weiterzuleiten.

19.5.6 Der Auftragnehmer wird die SKH unverzüglich darauf aufmerksam machen, wenn eine von der SKH erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Absatz 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bei der SKH nach Überprüfung bestätigt oder geändert wird.

19.5.7 Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn die SKH dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

19.5.8 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch die SKH erteilen.

19.5.9 Der Auftragnehmer erklärt sich damit einverstanden, dass die SKH - grundsätzlich nach Terminvereinbarung - die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch von der SKH beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Absatz 3 Satz 2 lit. h DS-GVO).

19.5.10 Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

19.5.11 Die Verarbeitung von Daten in Privatwohnungen (Tele- beziehungsweise Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung der SKH gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

19.5.12 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die der SKH obliegen.

19.5.13 Der Auftragnehmer hat bei der Verarbeitung im Auftrag das Bankgeheimnis zu wahren. Das Bankgeheimnis erstreckt sich auf alle personenbezogenen Daten und anderen Informationen, die der SKH über ihre Kunden, Interessenten oder über Dritte aus der Geschäftsbeziehung zu diesen bekannt werden. Unter das Bankgeheimnis fällt auch die Angabe, ob die SKH überhaupt eine Geschäftsbeziehung zu einem Kunden unterhält.

19.5.14 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten der SKH die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages unbefristet fort.

19.5.15 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Absatz 3 Satz 2 lit. b und Art. 29 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

19.5.16 Der beim Auftragnehmer benannte Beauftragte(r) für den Datenschutz ist in der Vereinbarung zur Auftragsverarbeitung festgelegt. Ein Wechsel des Datenschutzbeauftragten ist der SKH unverzüglich mitzuteilen.

19.5.17 Der Auftragnehmer verpflichtet sich, die SKH über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Absatz 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Absatz 7 DS-GVO unverzüglich zu informieren.

19.6 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt der SKH unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten SKH nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, der SKH erforderlichenfalls bei ihren Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Absatz 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für die SKH darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

19.7 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Absatz 3 Satz 2 lit. d DS-GVO)

19.7.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten der SKH ist dem Auftragnehmer nur mit Genehmigung der SKH gestattet, Art. 28 Absatz 2 DS-GVO, welche auf einem der vertraglich vereinbarten Kommunikationswege mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer der SKH Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind der SKH auf Anfrage zur Verfügung zu stellen.

19.7.2 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (zum Beispiel Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

19.7.3 Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen der SKH und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss die SKH berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihr beauftragte Dritte durchführen zu lassen.

19.7.4 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Absatz 4 und Absatz 9 DS-GVO).

19.7.5 Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Absatz 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

19.7.6 Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) zu überprüfen.

19.7.7 Das Ergebnis der Überprüfungen ist zu dokumentieren und der SKH auf Verlangen zugänglich zu machen.

19.7.8 Soweit zum Zeitpunkt des Vertragsschlusses bereits Subunternehmer bekannt sind, werden diese in einem gesonderten Dokument mit Namen, Anschrift und Auftragsinhalt benannt. Mit deren Beauftragung erklärt sich die SKH einverstanden.

19.7.9 Der Auftragnehmer informiert die SKH immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch die SKH die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Absatz 2 Satz 2 DS-GVO).

19.8 Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Absatz 3 Satz 2 lit. c DS-GVO)

19.8.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Absatz 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

19.8.2 Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

19.8.3 Das Datenschutzkonzept des Auftragnehmers stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko dar. Dabei werden die Schutzziele nach Stand der Technik detailliert und die eingesetzten IT- Systeme und Verarbeitungsprozesse berücksichtigt. Soweit das Datenschutzkonzept nicht als Anlage in der Vereinbarung zur Auftragsverarbeitung beigefügt ist, ist ein Datenschutzkonzept auf Anforderung der SKH innerhalb einer Frist von 14 Tagen vom Auftragnehmer vorzulegen.

19.8.4 Das im Datenschutzkonzept beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt. Soweit ein solches Verfahren vertraglich nicht weiter festgelegt ist, kann die SKH entsprechende Anforderungen auch nach Vertragsschluss definieren. Dabei sind die gesetzlichen Anforderungen und die der SKH bekannten betrieblichen Belange des Auftragnehmers zu berücksichtigen.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Absatz 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist der SKH mitzuteilen.

19.8.5 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und der SKH abzustimmen.

19.8.6 Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen der SKH nicht genügen, benachrichtigt er die SKH unverzüglich.

19.8.7 Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards und den Stand der Technik nicht unterschreiten.

19.8.8 Wesentliche Änderungen muss der Auftragnehmer mit der SKH in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

19.8.9 Die Modalitäten des Transports der Daten mittels Datenträger (einschließlich Übergabe und Abholung) oder gegebenenfalls einer Datenfernübertragung werden vom Auftragnehmer vor Beginn beziehungsweise am Ende der Auftragsabwicklung abgestimmt und protokolliert.

19.9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Absatz 3 Satz 2 lit. g DS-GVO

19.9.1 Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, der SKH auszuhändigen oder datenschutzgerecht zu löschen beziehungsweise zu vernichten/vernichten zu lassen.

19.9.2 Die Löschung beziehungsweise Vernichtung ist der mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

19.10 Haftung, Aufbewahrung

19.10.1 Auf Art. 82 DS-GVO wird verwiesen. Im Übrigen gelten die Haftungsregelungen gemäß den AZB.

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

19.10.3 Im Falle einer Inanspruchnahme der SKH durch eine betroffene Person hinsichtlich etwaiger Ansprüche aus Art. 82 DSGVO, verpflichtet sich der Auftragnehmer die SKH bei der Abwehr des Anspruches weitgehend zu unterstützen.