

## **Vereinbarung**

### **über die Einhaltung des branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Kranken- und Pflegekassen gem. § 392 Abs. 6 SGB V und § 103a Abs. 6 SGB XI**

zwischen der

#### **Siemens Betriebskrankenkasse/SBK-Pflegekasse**

Ganghoferstr. 29 | 80339 München

vertreten durch die Vorständin Dr. Getrud Demmler,  
diese wiederum vertreten durch XX

nachstehend auch Auftraggeber (AG) genannt

und dem/der

[Name des Dienstleisters, Anschrift, Vertretung]

nachstehend auch Auftragnehmer (AN) genannt

## **§ 1 – Gegenstand der Vereinbarung, Laufzeit, Kündigung**

### **(1) Gegenstand der Vereinbarung**

Diese Vereinbarung regelt die Einhaltung des branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Kranken- und Pflegekassen in Bezug auf den zwischen den Parteien am xx.xx.xxxx geschlossenen Vertrag Nr. xx (im Folgenden: „Hauptvertrag“).

### **(2) Laufzeit der Vereinbarung**

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages.

### **(3) Kündigung**

Der Auftraggeber kann den Hauptvertrag unabhängig von dem bereits in diesem geregelten Kündigungsrechten auch dann jederzeit und ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer schuldhaft gegen die in dem hiesigen Vertrag geregelten Pflichten verstößt. Die ist insbesondere der Fall bei:

- a) einem Verstoß gegen die in § 2 geregelten vertragswesentlichen Pflichten
- b) einem Verstoß gegen die in § 3 geregelten Pflichten bzgl. Unterauftragsverhältnissen
- c) einer Verweigerung der dem Auftraggeber oder der Aufsichtsbehörde nach § 4 des Vertrages zustehenden Kontrollrechte oder
- d) bei Nichtausführung einer erforderlichen Weisung des Auftraggebers zur Gewährleistung der Informationssicherheit gemäß § 5 dieses Vertrages binnen der in der Weisung genannten Frist
- e) einer wesentlichen Änderung oder eines Wegfalls der Grundlage des Vertragsschlusses aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen.

Voraussetzung für die Kündigung nach den lit. a) bis d) ist, dass der Auftragnehmer die Pflichtverletzung zu vertreten hat.

### **§ 2 – Konkretisierung der vertragswesentlichen Pflichten**

Zur Einhaltung des branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit bei den Kranken- und Pflegekassen vereinbaren die Parteien folgendes:

- (1)** Der Auftragnehmer verpflichtet sich zur Einhaltung des jeweils aktuell gültigen branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Kranken- und Pflegekassen gem. § 392 Abs. 3 SGB V und § 103a Abs. 3 SGB XI (derzeit: B3S-GKV/PKV, V.1.4, Stand: 20.01.2025) bezüglich der durch den Auftraggeber in Anspruch genommenen IT-Dienstleistungen im Sinne von § 392 Abs. 6 SGB V und § 103a Abs. 6 SGB XI.
- (2)** Der Auftragnehmer verpflichtet sich weiter, die Einhaltung nach Abs. 1 regelmäßig in geeigneter Form nachzuweisen. Dazu zählt auch eine Überprüfung durch den Auftraggeber gemäß §4.
- (3)** Der Auftragnehmer muss vor Vertragsschluss schriftlich oder in Textform dokumentieren, wie er die im Vorfeld der Auftragsvergabe dargelegten organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit seiner IT-Systeme im Rahmen des

Leistungsgegenstands umsetzt. Diese Vorkehrungen müssen den Anforderungen des B3S-GKV/PV insbesondere Abschnitt 4.12 Lieferanten, Dienstleister und Dritte entsprechen und dem Auftraggeber zur Prüfung übergeben werden. Bei Akzeptanz durch den Auftraggeber werden sie Bestandteil des Auftrags. Falls die Prüfung Anpassungsbedarf ergibt, muss dieser umgesetzt werden.

- (4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf den im Hauptvertrag beschriebenen Leistungsgegenstand beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- (5) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- 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 nach besten Kräften zu unterstützen.

### **§ 3 – Unterauftragsverhältnisse**

- (1) Nimmt der Auftragnehmer die Unterstützung eines weiteren Dritten (im Folgenden: „Unterauftragnehmer“) in Anspruch, um Dienstleistungen im Namen des Auftraggebers zu erbringen, so muss der Dienstleister dem Dritten dieselben Pflichten auferlegen, die in der hiesigen Vereinbarung festgelegt wurden.
- (2) Für die Überwachung und Durchsetzung der zwischen dem Auftragnehmer und dem Unterauftragnehmer vereinbarten Pflichten ist der Auftragnehmer verantwortlich. Der Auftraggeber kann den Nachweis einer entsprechenden Vereinbarung vom Auftragnehmer verlangen.
- (3) Der Auftragnehmer hat den Unterauftragnehmer bezüglich der Einhaltung der vertraglichen Pflichten regelmäßig, mindestens aber alle drei Jahre, zu prüfen. Das Ergebnis ist zu dokumentieren, mindestens sechs Jahre aufzubewahren und auf Verlangen dem Auftraggeber vorzulegen.

### **§ 4 – Kontrollrechte des Auftraggebers und seiner Aufsichtsbehörde**

- (1) Der Auftraggeber oder von ihm beauftragte Dienstleister sind, ebenso wie die Aufsichtsbehörden des Auftraggebers berechtigt, Überprüfungen beim Auftragnehmer durchzuführen, um die Einhaltung der Anforderungen der vorliegenden Vereinbarung zu kontrollieren. Diese Überprüfungen können auch operatives Monitoring vereinbarter Sicherheitsparameter und Stichprobenkontrollen im Geschäftsbetrieb

des Auftragnehmers umfassen. Hierzu gewährt der Auftragnehmer dem Auftraggeber Zugang. Die Überprüfung kann zusätzlich aufgrund regelmäßiger KRITIS-Audits des Auftraggebers erfolgen, die mindestens alle drei Jahre durchgeführt werden. Ebenfalls ist der Auftraggeber berechtigt, anlassbedingt (z.B. aufgrund eines Incidents) Kontrollen durchzuführen.

- (2) Das Kontrollrecht des Auftraggebers beinhaltet insbesondere die Berechtigung zum Betreten von Grundstücken und Geschäftsräumen des Auftragnehmers sowie zur Einsichtnahme in Unterlagen (inkl. Dokumentationen), sofern dies zur Wahrnehmung des Kontrollrechts erforderlich ist.
- (3) Aufwände und Kosten, die beim Auftragnehmer im Zuge der Prüfungen entstehen, sind vom Auftragnehmer zu tragen.

## § 5 – Weisungsbefugnis des Auftraggebers

- (1) Der Auftraggeber hat das Recht, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu erteilen, um die Einhaltung des branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Krankenkassen in der jeweils gültigen Fassung sicherzustellen.
- (2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. in Textform).

## § 6 – Ansprechpersonen

Ansprechpersonen ergeben sich aus **Anhang 3**.

## § 7 – Inkrafttreten

Diese Vereinbarung tritt mit dem Datum der Unterzeichnung in Kraft.

-----  
Ort, Datum

-----:  
Ort, Datum

-----  
Stempel & Unterschrift des Auftragnehmers

-----:  
Stempel & Unterschrift des Auftraggebers