Rahmenvertrag für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag

zwischen der

(„Krankenkasse“)

und

Deutscher Hausärzteverband Landesverband Baden-Württemberg e.V.
Kölner Straße 18, 70376 Stuttgart
vertreten durch den Vorstand Dr. med. Berthold Dietsche
(„Hausärzteverband“)

und dem

MEDI Baden-Württemberg e.V.
Industriestr. 2, 70565 Stuttgart
vertreten durch den Vorstand Dr. med. Werner Baumgärtner
(„MEDI e.V.“)

sowie der

HÄVG Hausärztliche Vertragsgemeinschaft eG

Von-der-Wettern-Straße 27, 51149 Köln

vertreten durch die Vorstände Joachim Schütz und Dr. Jochen Rose

(„HÄVG“)

und

MEDIVERBUND

MEDIVERBUND Dienstleistungs GmbH

Industriestr. 2, 70565 Stuttgart

vertreten durch den Geschäftsführer Werner Conrad

(„MEDIVERBUND“)

als Dienstleistungsgesellschaften für den Hausärzteverband und MEDI e.V.

PRÄAMBEL

Dieser Rahmenvertrag stellt die datenschutzkonforme Abwicklung der HzV sicher und enthält die dafür notwendigen Einzelregelungen zwischen den HzV-Partnern.

Nach dem HzV-Vertrag ist Voraussetzung der Auszahlung der HzV-Vergütung durch die Krankenkasse die ordnungsgemäße Abrechnung der Leistungen (§ 10 Abs. 1 des HzV-Vertrages). Für diese Abrechnung müssen bestimmte personenbezogene Daten von HzV-Versicherten an die Krankenkasse übermittelt werden. Die Krankenkasse benötigt diese Daten zur Prüfung der HzV-Abrechnung sowie im Rahmen des Prüfwesens gemäß § 73b Abs. 5 S. 5 in Verbindung mit § 106a Abs. 3 SGB V.

Würde der Hausarzt die Abrechnungsdaten selbst verarbeiten, bestünde aufgrund des damit verbundenen Zeitaufwandes wie der hierfür im erheblichen Umfang gebundenen Rechnerkapazitäten in der Praxis die Gefahr von Störungen des Betriebsablaufes. Um dies zu vermeiden und um mehr Zeit für die Versorgung der Patienten aufbringen zu können, beauftragen die teilnehmenden Hausärzte eine andere Stelle im Sinne des § 295 Abs. 1b SGB V mit der Erstellung der Abrechnung der ärztlich erbrachten Leistungen. Die Beauftragung ist erheblich kostengünstiger, als wenn der Hausarzt die Abrechnung selbst erstellen würde.

Der Hausärzteverband und MEDI e.V. sind als Vertragspartner der Krankenkasse (§ 73b Abs. 4 Satz 1 SGB V) unter anderem verantwortlich für die ordnungsgemäße Durchführung der Leistungsabrechnung und Honorarverteilung an die teilnehmenden Ärzte. Zur Wahrnehmung dieser Pflichten bedienen sich der Hausärzteverband und MEDI e.V. der HÄVG (**Dienstleistungsgesellschaft**) als Erfüllungsgehilfe. Im Falle eines Ausscheidens der Dienstleistungsgesellschaft aus dem HzV-Vertrag wird MEDIVERBUND gemäß § 2 Abs. 5 Satz 5 des HzV-Vertrages Erfüllungsgehilfe des Hausärzteverbandes und MEDI e.V. und tritt in deren vertraglichen Pflichten und Rechte als Dienstleistungsgesellschaft ein. Die Dienstleistungsgesellschaft bedient sich hierzu ihrerseits des Rechenzentrums.

Dies vorangestellt vereinbaren die Vertragspartner das Folgende:

§ 1
Gegenstand des Vertrags, Beitritt Hausarzt

(1) Dieser Rahmenvertrag für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag (**Rahmenvertrag**) ist als **Anlage 11** Bestandteil des HzV-Vertrages (Vertrag zur Durchführung einer hausarztzentrierten Versorgung gemäß § 73b SGB V vom XX.XX.XXXX zwischen der der Krankenkasse, dem Hausärzteverband, MEDI e.V., HÄVG und MEDIVERBUND.

(2) Gegenstand dieses Rahmenvertrages ist die Regelung der datenschutzrechtlichen Beauftragung des Hausärzteverbandes und MEDI e.V. und deren Unterauftragnehmern durch den Hausärzteverband und MEDI e.V. mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten für die Abrechnung der ärztlich erbrachten HzV-Leistungen des HAUSARZTES auf der Grundlage des HzV-Vertrages.

(3) Die Krankenkasse, der Hausärzteverband, MEDI e.V. und die Dienstleistungsgesellschaft sind sich einig, dass der HAUSARZT diesem Rahmenvertrag beitreten kann, indem er die als **Anhang A** beigefügte Beitrittserklärung (**Datenschutzerklärung**) unterzeichnet und per Fax an die auf der Datenschutzerklärung aufgeführte Faxnummer der Dienstleistungsgesellschaft übermittelt.

(4) Mit Wirksamwerden des Beitritts des Hausarztes durch Rücksendung der unterzeichneten Datenschutzerklärung zu diesem Rahmenvertrag kommt zwischen dem HAUSARZT und dem Hausärzteverband und MEDI e.V. eine Beauftragung gem.

§ 295 Abs. 1b S. 1 und 4 SGB V zustande. Der HAUSARZT wird nachfolgend auch als **Auftraggeber** bezeichnet. Der Hausärzteverband und MEDI e.V. werden nachfolgend auch als **Auftragnehmer** bezeichnet.

§ 2
Pflichten der Vertragsparteien

(1) Der Hausärzteverband und MEDI e.V. verpflichten sich, Ärzten, die an dem HzV-Vertrag teilnehmen wollen, diesen Rahmenvertrag und die diesem Rahmenvertrag als **Anhang A** beigefügte Datenschutzerklärung vor Erklärung der Teilnahme an dem HzV-Vertrag zusammen mit der Teilnahmeerklärung dem HAUSARZT zugänglich zu machen.

(2) Der Hausärzteverband und MEDI e.V. verpflichten sich gegenüber dem HAUSARZT, die für die Abrechnung erforderlichen personenbezogenen Daten nach Maßgabe der Regelungen dieses Rahmenvertrages zu erheben, zu verarbeiten und zu nutzen.

(3) Die Auftragnehmer stellen dem HAUSARZT für alle Fragen in Zusammenhang mit diesem Rahmenvertrag einen einheitlichen Ansprechpartner zur Verfügung. Die vollständigen Kontaktinformationen sind auf den Internetseiten des Hausärzteverbandes (www.hausarzt-bw.de) und MEDI e.V. (www.medi-verbund.de) hinterlegt.

§ 3
Anforderungen an die Datenverarbeitung

(1) Die Auftragnehmer erheben, verarbeiten und nutzen personenbezogene Daten im Auftrag des Auftraggebers.

(2) Der Auftrag umfasst die Aufbereitung der personenbezogenen Daten des Hausarztes und der personenbezogenen Daten der von ihm im Rahmen der HzV behandelten Versicherten der Krankenkasse sowie die Weiterleitung der für die Zwecke der Abrechnung der HzV-Vergütung (§§ 10 bis 14 des HzV-Vertrages) erforderlichen personenbezogenen Daten zum Zweck der Abrechnung an die Krankenkasse.

(3) Für die Ausführung der Tätigkeit nach Abs. 2 leitet der Auftraggeber laufend je Abrechnungsquartal die erforderlichen Daten mittels des in **Anhang B** festgelegten EDV-Verfahrens an den Auftragnehmer über die Vertragssoftware weiter. Das Verfahren entspricht grundsätzlich den Richtlinien des GKV-Spitzenverbands zur Umsetzung des Datenaustauschs nach § 295 Abs. 1b SGB V (**Richtlinien**) und dem zwischen dem Hausärzteverband, dem MEDI e.V. bzw. Dienstleistungsunternehmen und der Krankenkasse festgelegten Verfahren. Die übermittelten Daten ergeben sich aus **Anhang B**. Die jeweils aktuelle Fassung von **Anhang B** ist im Internet unter www.hausarzt-bw.de und www.medi-verbund.de abrufbar.

(4) Die Auftragnehmer erstellen aus den Daten nach Abs. 3 elektronisch einen Abrechnungsdatensatz (**HzV-Abrechnung**, vgl. Anlage 3). Sie leiten die Daten ausschließlich zu dem Zweck der Abrechnung und Abrechnungsprüfung an die Krankenkasse weiter.

§ 4
Pflichten der Auftragnehmer

(1) Die Auftragnehmer erheben, verarbeiten und nutzen personenbezogene Daten ausschließlich für die Abrechnung von HzV-Leistungen mit der Krankenkasse und nach schriftlichen Weisungen des Auftraggebers.

(2) Die Auftragnehmer gewährleisten, dass die in der Anlage zu § 78a SGB X bzw. § 9 BDSG genannten technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit getroffen und eingehalten werden. Zu den Regelungstatbeständen des § 78a SGB X werden die im **Anhang C** aufgeführten technischen und organisatorischen Maßnahmen verbindlich festgelegt. Abweichungen von diesen Maßnahmen sind nur zur Verbesserung des Datenschutzes und der Datensicherheit zulässig. Aktualisierungen werden auf den Webseiten des Hausärzteverbands und MEDI e.V. bekannt gemacht, der HAUSARZT wird in diesem Fall benachrichtigt.

(3) Die Auftragnehmer verpflichten sich, dem Auftraggeber und der nach § 295 Abs. 1b Satz 4 SGB V und § 38 Abs. 6 BDSG zuständigen Aufsichtsbehörde jederzeit während der Betriebs- und Geschäftszeiten Auskünfte zu erteilen und Zugang zu den Geschäftsräumen zu gewähren, in denen die Datenerhebung, -verarbeitung und -nutzung im Auftrag erfolgt, sofern dies im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist. Der Auftraggeber und die zuständige Aufsichtsbehörde sind berechtigt, mit den in § 80 Abs. 2 Satz 4 SGB X und § 38 Abs. 3 und Abs. 5 BDSG genannten Mitteln die Einhaltung der Vorschriften über den Datenschutz sowie die ergänzenden Weisungen nach § 80 Abs. 2 Satz 3 SGB X zu kontrollieren, soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist.

(4) Die Auftragnehmer benennen einen Beauftragten für den Datenschutz und teilen dem Auftraggeber dessen Kontaktadresse schriftlich mit. Sie informieren ihn unverzüglich über Änderungen, die die Person oder die Kontaktdaten des Beauftragten für Datenschutz betreffen. Wenn (sofern rechtlich zulässig) kein Datenschutzbeauftragter bestellt ist, haben die Auftragnehmer dies zu begründen und die Meldepflichten nach §§ 4d, 4e BDSG zu erfüllen und dies dem Auftraggeber auf Verlangen nachzuweisen.

(5) Die Auftragnehmer sind verpflichtet, für die auftragsgemäße Datenerhebung, -verarbeitung und –nutzung ausschließlich Personen einzusetzen, die auf das Sozialgeheimnis des § 35 Abs. 1 SGB I entsprechend und das Datengeheimnis nach § 5 BDSG verpflichtet sind. Die Auftragnehmer stellen sicher, dass das von ihnen eingesetzte Personal im Sinne der gesetzlichen Datenschutzvorschriften und insbesondere gemäß § 295 Abs. 1b SGB V, §§ 78a, 80 SGB X, § 35 Abs. 1 SGB I und der Regelungen des BDSG ausreichend informiert und angewiesen ist.

(6) Die Auftragnehmer dürfen die für die Erhebung, Verarbeitung und Nutzung überlassenen personenbezogenen Daten nur für die Dauer der Laufzeit des Rahmenvertrages speichern, es sei denn der Auftraggeber bestimmt schriftlich eine anderweitige Aufbewahrungszeit oder zwingende gesetzliche Vorschriften sehen eine andere Aufbewahrungsfrist vor. Die Auftragnehmer bewahren die personenbezogenen Daten innerhalb dieser Frist unter Verschluss bzw. unter Einsatz entsprechender technischer Mittel vor unbefugtem Zugriff gesichert auf. Sie geben sie ausschließlich an die Krankenkasse weiter, nicht an anderweitige Dritte.

(7) Sämtliche Unterlagen und Daten sowie Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit den in diesem Vertrag genannten Leistungen in den Besitz der Auftragnehmer gelangt sind, haben diese entsprechend den jeweiligen Vereinbarungen bzw. nach Beendigung des HzV-Vertrages auf Verlangen dem Auftraggeber auszuhändigen, soweit dies technisch möglich ist und keine gesetzlichen Pflichten entgegen stehen. Die Auftragnehmer haben im Zusammenhang mit der auftragsgemäßen Erfüllung der Dienstleistung Daten bzw. Datenbestände (physische Datenträger, elektronische Dateien und Datenbanken in ihren DV-Systemen), die sich in ihrem Besitz befinden, 12 Monate nach Auftragserledigung nichtreproduzierbar zu löschen bzw. physisch zu vernichten, wenn diese für die vertraglichen vereinbarten Dienstleistungen nicht mehr erforderlich sind oder der Auftraggeber eine entsprechende Weisung erteilt. Dies gilt auch für erzeugte Test- und Zwischenergebnisse.

Die Löschung bzw. Vernichtung haben die Auftragnehmer in geeigneter Weise zu protokollieren – ggf. maschinell – und auf Verlangen dem Auftraggeber vorzuzeigen.

(8) Der Arbeitsablauf wird von den Auftragnehmern lückenlos und revisionssicher dokumentiert. Die Dokumentation ist für einen Zeitraum von 12 Monaten nach Beendigung dieses Rahmenvertrages aufzubewahren. Sie ist dem Auftraggeber bzw. den Aufsichtsbehörden auf Verlangen vorzulegen.

(9) Die Auftragnehmer verpflichten sich, keine Kopien oder Duplikate der Datenbestände bzw. Datenbanken ohne Wissen des Auftraggebers oder für andere Zwecke zu erstellen.

(10) Die Auftragnehmer unterrichten den Auftraggeber unverzüglich über den Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Datenerhebung, -verarbeitung und -nutzung und bei Störungen des Verarbeitungsablaufs.

(11) Die Auftragnehmer sind nur berechtigt, die Daten im Geltungsbereich des Sozialgesetzbuches oder des Mitgliedstaates der EU oder anderen Vertragsstaaten des Abkommens über den EWR zu erheben, zu verarbeiten oder zu nutzen, für den im Rahmen des Abschlusses des Vertrags die Genehmigung erteilt wurde.

(12) Die Auftragnehmer haben den bzw. die für die Erhebung, Verarbeitung und Nutzung der Daten des Auftraggebers im Rahmen des Auftragsverhältnisses vorgesehene(n) Standort/Standorte bzw. ihre Geschäftsräume dem Auftraggeber vor Vertragsschluss schriftlich zu benennen (**Anhang E**). Eine Veränderung der Standorte, in denen Daten des Auftraggebers verarbeitet und/oder genutzt werden, bedarf der schriftlichen Zustimmung des Auftraggebers. Die Zustimmung darf nur aus wichtigem Grund versagt werden. Die Auftragnehmer stellen sicher, dass ein Zugriff auf Daten des Auftraggebers von Standorten außerhalb der in **Anhang E** angegebenen Geschäftsräume der Auftragnehmer ausgeschlossen ist.

§ 5
Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenerhebung, -verarbeitung und –nutzung sowie für die Wahrung der Rechte der Betroffenen bleibt allein der Auftraggeber verantwortlich. Das alleinige Verfügungsrecht über die Daten verbleibt bei dem Auftraggeber.

(2) Die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung richtet sich nach dem SGB V, insbesondere § 295 Abs. 1b SGB V in Verbindung mit den §§ 78a, 80 SGB X sowie nach den Richtlinien in der jeweils gültigen Fassung.

(3) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich.

(4) Der Auftraggeber ist verpflichtet und berechtigt, erforderlichenfalls Weisungen nach § 80 Abs. 2 Satz 3 SGB X (bzw. § 11 BDSG) betreffend die Ergänzung der bei den Auftragnehmern vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu erteilen. Die Weisungen sind schriftlich zu erteilen.

(5) Der Auftraggeber informiert die Auftragnehmer unverzüglich über festgestellte Fehler oder Unregelmäßigkeiten der Auftragsleistung.

§ 6
Information der Aufsichtsbehörden

(1) Der Auftraggeber beauftragt hiermit die Auftragnehmer, der für den Auftraggeber zuständigen Aufsichtsbehörde für den Datenschutz rechtzeitig die nach § 80 Abs. 5 SGB X erforderlichen Informationen zukommen zu lassen.

§ 7
Verpflichtung auf das Sozialgeheimnis

(1) Die Auftragnehmer verpflichten sich, bei der auftragsgemäßen Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten des Auftraggebers das Sozialgeheimnis gemäß § 35 Abs. 1 SGB I entsprechend und das Datengeheimnis gemäß § 5 BDSG zu wahren.

(2) Das Sozialgeheimnis und das Datengeheimnis gelten auch nach Beendigung des Auftrags und nach Beendigung der Beschäftigungsverhältnisse des Personals der Auftragnehmer fort.

§ 8
Unterauftragnehmer

(1) Unterauftragnehmer, die für die Auftragnehmer unmittelbar Daten des Auftraggebers erheben, verarbeiten oder nutzen, dürfen von den Auftragnehmern nur mit vorheriger, schriftlicher Einwilligung des Auftraggebers eingeschaltet werden. Die Vertragsparteien und der Auftraggeber erklären hiermit ihr Einverständnis, dass a) die Dienstleistungsgesellschaft als Unterauftragnehmerin des Hausärzteverbandes und MEDI e.V. tätig wird, b) der MEDIVERBUND als Unterauftragnehmer des Hausärzteverbandes und MEDI e.V. tätig wird, wenn er im Falle eines Ausscheidens der Dienstleistungsgesellschaft aus dem HzV-Vertrag gemäß § 2 Abs. 5 Satz 5 des HzV-Vertrags Erfüllungsgehilfe des Hausärzteverbandes und von MEDI e.V. wird und in deren vertraglichen Pflichten und Rechte als Dienstleistungsgesellschaft eintritt, c) das Rechenzentrum als Unterauftragnehmer der Dienstleistungsgesellschaft tätig wird und d) in **Anhang D** dieses Rahmenvertrages aufgeführten Stellen zulässige Unterauftragnehmer sind.

(2) Alle Unterbeauftragungen sind so auszugestalten, dass sie den Regelungen dieses Rahmenvertrages betreffend die Rechte und Pflichten von Auftraggeber und Auftragnehmern entsprechen. Der Auftraggeber muss zudem die Möglichkeit haben, die in diesem Rahmenvertrag niedergelegten Rechte auch unmittelbar gegenüber Unterauftragnehmern geltend zu machen. Dies gilt auch für den einzuhaltenden Mindeststandard hinsichtlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit. Die Auftragnehmer haben die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Verträge mit Unterauftragnehmern zur Datenverarbeitung sind dem Auftraggeber auf Verlangen vorzulegen. Verhalten seiner Unterauftragnehmer ist den Auftragnehmern wie eigenes Verhalten zuzurechnen.

(3) Die Regelungen dieses § 8 gelten auch für Unterauftragnehmer, die Prüfungen oder die Wartung von automatisierten Verfahren oder von Datenverarbeitungsanlagen der Auftragnehmer vornehmen. Derartige Aufträge sind dem Auftraggeber vor Vertragsschluss mitzuteilen. Zurzeit sind die im **Anhang D** aufgeführten Wartungsfirmen für die Auftragnehmer tätig.

(4) Beauftragen die Auftragnehmer für den Datentransport einen Transportunternehmer, so hat er sicherzustellen und dem Auftraggeber auf Verlangen nachzuweisen, dass der Transportunternehmer den Datenschutzbestimmungen Genüge tut. Werden Unterlagen beim Auftraggeber abgeholt, so statten die Auftragnehmer den Transportunternehmer mit einem schriftlichen Berechtigungsausweis für die Entgegennahme der Unterlagen aus.

(5) Die vorstehenden Regelungen gelten auch im Hinblick auf die Beauftragung eines Unterauftragnehmers durch einen Unterauftragnehmer.

§ 9
Haftung

(1) Für die Haftung gelten die Regelungen im HzV-Vertrages.

§ 10
Inkrafttreten, Laufzeit, Kündigung

(1) Dieser Rahmenvertrag tritt mit seiner Unterzeichnung durch die Vertragsparteien in Kraft. Für den Hausarzt wird dieser Rahmenvertrag mit Beitritt wirksam.

(2) Die Laufzeit und Kündigungsmöglichkeiten dieses Vertrages richten sich nach den Regelungen des HzV-Vertrags.

§ 11
Sonstige Regelungen

(1) Ergänzend gelten die Regelungen zu Vertragsänderungen nach § 17 sowie die Schlussbestimmungen gemäß § 22 des HzV-Vertrages.

§ 12
Anhänge/Vordrucke

(1) Die folgenden Anhänge sind Bestandteil dieses Rahmenvertrages:

Anhang A	Datenschutzerklärung
Anhang B	EDV-Verfahren und übermittelte Daten
Anhang C	Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit
Anhang D	Übersicht über die Unterauftragnehmer/Wartungsfirmen
Anhang E	Standorte der Geschäftsräume des Auftragnehmers

(2) Die Anhänge können einvernehmlich zwischen den Vertragspartnern dieses Rahmenvertrages geändert werden. Diese Änderungen gelten ab dem Zeitpunkt auch für die anderen Vertragspartner dieses Rahmenvertrages; diese erklären sich durch ihren Beitritt mit diesem Verfahren einverstanden.

Stuttgart, den

_____

Krankenkasse

_____

Deutscher Hausärzteverband Landesverband Baden-Württemberg e.V.

Dr. med. Berthold Dietsche

MEDI Baden-Württemberg e. V.

Dr. med. Werner Baumgärtner

HÄVG eG

Joachim Schütz und Dr. Jochen Rose

MEDIVERBUND Dienstleistungs GmbH

Werner Conrad

Anhang A

Per Fax an die Hausärztliche Vertragsgemeinschaft eG für den Hausärzteverband Baden-Württemberg e.V.: 01805- 55 88 33 437

(EUR 0,14/Minute aus dem deutschen, Mobilfunk max. EUR 0,42/Minute)

Datenschutzerklärung HAUSARZT

Beitrittserklärung nach § 1 des „Rahmenvertrages für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag“ zwischen der BKK-Vertragsarbeitsgemeinschaft der Krankenkasse, dem Deutschen Hausärzteverband Landesverband Baden-Württemberg e.V., dem MEDI Baden-Württemberg e. V., der Hausärztlichen Vertragsgemeinschaft eG und dem MEDIVERBUND Dienstleistungs GmbH vom XX.XX.2010.

Hiermit trete ich	…… (Vorname)	…….. (Name)
Hiermit trete ich	…… (LANR)	…….. (BSNR)
Praxis	…….. (Straße)	……. (Hausnr.)
	…….. (PLZ)	

dem vorgenannten Rahmenvertrag (Anlage 8 zum HzV-Vertrag) bei.

Der Text des Rahmenvertrages liegt mir vor. Ich hatte ausreichend Zeit, den Inhalt des Rahmenvertrages einschließlich seiner Anlagen zur Kenntnis zu nehmen und bin nach reiflicher Überlegung mit dem Inhalt einverstanden. Der Text des Rahmenvertrages und seiner Anlagen ist im Internet unter www.hausarzt-bw.de und www.medi-verbund.de abrufbar.

_____

Ort, Datum

_____

Unterschrift

Anhang B* **Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit gemäß § 14 Abs. 2**

* Bei den unterstrichenen, in Rot gesetzten „Anmerkungen“ / „Beispielen“ handelt es sich um Erläuterungen, die nicht Inhalt des Anhangs B, sondern als Hilfen für die Vertragspartner gedacht sind.

Zu den Regelungstatbeständen des § 295 Abs. 1b Satz 6 SGB V in Verbindung mit § 78a SGB X werden folgende technische und organisatorische Maßnahmen festgelegt:

1. Zutrittkontrolle

Maßnahmen, damit Unbefugten der Zutritt zu Datenverarbeitungsanlagen verwehrt ist, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

……

……

……...

Anmerkung: Die zum Zutritt befugten Personen (Mitarbeiter, Fremdbehörden, Fremdfirmen, Wartungsdienste, Anwendungsbetreuung) einschließlich des Umfangs der Befugnisse sollten festgelegt werden; zudem: Sicherung der Räume, Rollos, Schlüssel, Besucherregelung; Anwesenheitsaufzeichnung; Brand- und Bewegungsmelder; Bewachung, u. U. Spezialverglasung; Überwachung mittels Kamera etc.

2. Zugangskontrolle

Maßnahmen, damit die unbefugte Benutzung der Datenverarbeitungssysteme verhindert wird:

……

……

……...

Anmerkung: Es muss sichergestellt werden, dass nur befugte Personen Zugang zu den Datenverarbeitungssystemen haben. Datenverarbeitungssystem ist nach DIN 44300 Nr. 99 eine Funktionseinheit zur Verarbeitung von Daten. Dies betrifft die Hardware ebenso wie Datenverarbeitungsprogramme (Software) und Daten, durch deren Wechselwirkung der Verarbeitungsprozess möglich ist. Beispiele für entsprechende Maßnahmen sind: Festlegung und Kontrolle der Befugnisse (Zuordnung bestimmter Personalcomputer zu bestimmten Funktionen, etwa dem Zugriff auf eine bestimmte Datenbank); Identifikation sowie Berechtigungsprüfung der Benutzer; enge Begrenzung der befugten Benutzer, Einrichten einer formalen Benutzerverwaltung; Signaturverfahren zur Identifizierung eines Benutzers; Vergabe von Passwörtern; Zugriffsbeschränkungen; Einsatz eines virtuellen privaten Netzwerkes (VPN); spezielle Sicherheitssysteme, Einrichtung von sicheren Übertragungstechniken, etc.

3. Zugriffskontrolle

Maßnahmen, damit gewährleistet ist, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

……

……

……...

Anmerkung: Die Zugriffskontrolle soll sicherstellen, dass zur Benutzung eines Datenverarbeitungssystems Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Beispiele für Maßnahmen sind: Festlegung und Kontrolle der Zugriffsbefugnisse, differenziert nach Daten, Programmen und Zugriffsart (Trennung auch bei den Datenträgern vornehmen); Datenträgerkontrolle einschließlich Protokollieren der Befugten, Periodizität der Bestandskontrollen, Datenträgervernichtungsprotokollierung, Einschränkungen von Softwaremöglichkeiten zum Kopieren von Dateien und zu Datensicherungsmaßnahmen, Archivierung von Daten in einem Panzerschrank, etc.

4. Weitergabekontrolle

Maßnahmen, damit gewährleistet ist, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist:

……

……

……...

Beispiele: Protokollierung der Abruf- und Übermittlungsaktivitäten; Anlegen und Fortschreiben einer Übersicht, die erkennen lässt, an welchen Stellen während welcher Zeitspannen welche personenbezogenen Daten durch Übertragungseinrichtungen übermittelt werden konnten bzw. können. Dazu gehört auch die Dokumentation der Abruf- und Übermittlungsprogramme, der Übermittlungsweg und –stellen sowie der entsprechenden Übermittlungs-Hardware.

5. Eingabekontrolle

Maßnahmen, damit gewährleistet ist, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

……

……

……...

Beispiele: Festlegung, wer Daten eingeben darf, Kennzeichnung von Erfassungsunterlagen mit Namen und Datum nach Vollzug der Eingabe; Protokollieren der Netzverwaltung, der Lese- und Schreibzugriffe auf Dateien und der gescheiterten Zugriffsversuche, der Programmaufrufe; Dokumentation der Eingabeprogramme; Freigabeverfahren und Dokumentation der aktuellen Programmversion; Plausibilitätskontrollen

6. Auftragskontrolle

Maßnahmen, damit gewährleistet ist, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können:

……

……

……...

Beispiele: Festlegung der Kompetenzen und Pflichten von Auftragnehmer und Auftraggeber, Vereinbarung über Kündigungsmöglichkeiten, Vertragsstrafe, Kontrollrechte; Auswahl des Auftragnehmers unter Sorgfalts-Gesichtspunkten; Verwendung von Form- und Merkblättern zur Sicherung vollständiger und klarer Weisungen, Schriftlichkeit von Weisungen; Datenübergabe nur gegen Quittung oder verschlüsselt, so dass nur der Auftragnehmer entschlüsseln kann; Schutzmaßnahmen gegen wechselseitige Beeinflussung von verschiedenen Aufträgen durch festgelegte Funktionstrennung im Rechenzentrum des Auftragnehmers.

7. Verfügbarkeitskontrolle

Maßnahmen, damit gewährleistet ist, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind:

……

……

……...

Beispiele: Einrichtung einer unterbrechungsfreien Stromversorgung; Verwendung von geeigneten Tresoren und/oder so genannten Wertwürfeln (die Sicherungskopien müssen in die Behältnisse passen); Restore-Funktionen testen; Daten und Programme getrennt sichern und verwahren; Betriebssystemsicherungen nach dem Update erneuern.

8. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden

Maßnahmen:

……

……

……...

Beispiele: Trennung der Datensätze durch Speicherung in physikalisch getrennten Datenbanken; unterschiedliche Verschlüsselung von Datensätzen zur Abgrenzung der Zweckbindung; Festlegung von Rollen in einem Informationssystem: Administrator, Revisor, Benutzer.