VERTRAG ÜBER DIE AUFTRAGSVERARBEITUNG NACH ART. 28 DSGVO

Dieser Vertrag regelt die datenschutzrechtlichen Pflichten zwischen dem Auftraggeber und der Spitta GmbH, Ammonitenstraße 1, 72336 Balingen (nachfolgend: „Spitta“, „Auftragnehmer“).

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Der Vertrag zur Auftragsverarbeitung umfasst die Leistungen von Spitta, welche im Rahmen von Dienstleistungen und/oder dem Betrieb der Praxissoftware von Spitta erbracht werden.

Im Wesentlichen handelt es sich um folgende Aufgaben durch Spitta:

- Betrieb von und Support für Softwarelösungen

Der Auftragnehmer und die weiteren Subunternehmer unterliegen beim Zugriff auf Patientendaten der Geheimhaltungspflicht nach § 203 Abs. 4 StGB. Dementsprechend wird Spitta nach Ziffer 3.5 gegenüber dem Auftraggeber zur Geheimhaltung verpflichtet:

> § 203 Verletzung von Privatgeheimnissen
> (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
>
> 1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
> ….
> anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
>
> (4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Datenschutzbeauftragter bekannt geworden ist. Ebenso wird bestraft, wer
> 1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
> 2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
> 3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

1.2 Art und Zweck der Auftragsverarbeitung der jeweiligen Softwarelösung sind in den jeweiligen vertraglichen Vereinbarungen detailliert geregelt.

1.3 Die Verarbeitung umfasst die nachfolgend genannten Kategorien betroffener Personen:

- Beschäftigte
- Patienten
- Lieferanten
- Interessenten

1.4 Folgende Arten von personenbezogenen Daten sind von der Verarbeitung betroffen:

Persönliche Angaben (z.B. Adressaten, Bankdaten), Vertragsdaten, Beschäftigtendaten, Kommunikationsdaten, Nutzungsdaten aus Telemediendiensten oder Telekommunikationsdiensten, DV-Protokollierungsdaten,

Versicherungsdaten, Gesundheitsdaten. Sie variieren in Abhängigkeit von den jeweiligen Verantwortlichen und z.B. dessen Nutzung der Spitta Softwarelösung.

1.5 Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben.

1.6 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich 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 Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. Anwendungsbereich und Verantwortlichkeit

2.1 Spitta verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und/oder in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist hinsichtlich der Verarbeitung der Daten für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform an, die von Spitta bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Einzelweisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt und Spitta darf hierfür eine angemessene Vergütung verlangen.

2.3 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform.

2.4 Spitta wird den Auftraggeber unverzüglich informieren, wenn sie der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Spitta ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

3. Pflichten der Spitta

3.1 Spitta darf personenbezogene Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Sofern Spitta durch nationales oder europäisches Recht zu einer hiervon abweichenden Verarbeitung verpflichtet ist, weist er den Auftraggeber vor Beginn der Verarbeitung auf diesen Umstand hin.

3.2 Spitta wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Spitta wird die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers treffen. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogenen Daten auf Dauer gewährleisten. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten.

3.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt der Spitta vorbehalten, wobei jedoch gewährleistet sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.4 Spitta unterstützt den Auftraggeber im Rahmen der Möglichkeiten und der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten. Hierfür kann Spitta eine angemessene Vergütung verlangen.

3.5 Spitta setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Spitta gewährleistet, dass es den mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter und anderen für Spitta tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten. Die Vertraulichkeits- oder Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.6 Spitta unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Spitta trifft die erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7 Spitta ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten nach Art. 37 DSGVO zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Kontaktdaten des Datenschutzbeauftragten:

Name	Dr. Georg Schröder, LL.M.
	legal data Schröder Rechtsanwaltsgesellschaft mbH
Anschrift	Prannerstr. 1 / 80333 München
E-Mail	dsb@spitta.de

3.8 Spitta gewährleistet, ihren Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

3.9 Die Berichtigung und Löschung von personenbezogenen Daten obliegt dem Auftraggeber. Gleiches gilt für die Einschränkung der Verarbeitung von personenbezogenen Daten (Sperrung).

3.10 Personenbezogene Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Die Pflicht des Auftragnehmers zur Herausgabe von personenbezogenen Daten, auf die der Auftraggeber selbst Zugriff hat, besteht nicht.

3.11 Spitta verpflichtet sich zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

4. Pflichten des Auftraggebers

4.1 Dem Auftraggeber obliegt es, der Spitta die personenbezogenen Daten rechtzeitig zur Leistungserbringung zur Verfügung zu stellen. Er ist für die Qualität der personenbezogenen Daten verantwortlich. Der Auftraggeber hat der Spitta unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse der Spitta Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Leistungen feststellt.

4.2 Im Falle einer Inanspruchnahme durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichten sich Auftraggeber und Spitta bei der Abwehr des Anspruches sich gegenseitig zu unterstützen.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, Einschränkung der Verarbeitung oder Auskunft über die personenbezogenen Daten an den Auftragnehmer, wird Spitta die betroffenen Personen an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist.

6. Nachweismöglichkeiten

6.1 Spitta weist dem Auftraggeber auf Anfrage die Einhaltung der in Art. 28 DSGVO und diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten kann Spitta dem Auftraggeber Zertifikate und Prüfergebnisse Dritter (z.B. nach Art. 42 DSGVO oder ISO 27001) zur Verfügung stellen oder Prüfberichte des betrieblichen Datenschutzbeauftragten oder von diesen beauftragten Personen.

6.2 Sollten im Einzelfall Kontrollen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten Montag – Freitag zwischen 09:00 Uhr und 17:00 Uhr ohne Störung des Betriebsablaufs und nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von mind. 7 Bankarbeitstagen durchgeführt. Spitta darf diese von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung durch den Auftraggeber oder den von diesem beauftragen Prüfer abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zur Spitta stehen, hat Spitta gegen diesen ein Widerspruchsrecht. Der Widerspruch ist in Textform gegenüber dem Auftraggeber zu erklären.

6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Kontrolle vornehmen, gilt grundsätzlich 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung

ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

6.4 Für die Unterstützung bei der Durchführung einer Kontrolle nach 6.2 oder 6.3 darf Spitta eine angemessene Vergütung verlangen, sofern nicht Anlass der Kontrolle der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich der Spitta ist. In diesem Fall sind die Verdachtsmomente mit der Ankündigung der Kontrolle vom Auftraggeber vorzutragen. Die Höhe einer eventuellen Vergütung richtet sich nach Maßgabe der jeweils gültigen Preisliste der Spitta.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1 Der Auftraggeber stimmt zu, dass Spitta Subunternehmer hinzuzieht. Vor der Hinzuziehung oder Ersetzung von Subunternehmern informiert Spitta den Auftraggeber mit einer Frist von vier Wochen vorab in Textform. Der Auftraggeber kann der Änderung nur aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Tagen zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger Grund vor, der von Spitta nicht durch Anpassung des Auftrages beseitigt werden kann, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Über die in Anlage 2 aufgeführten, bei Vertragsschluss bereits bestehenden Subunternehmer und deren Teilleistungen erfolgt keine gesonderte Information.

7.2 Erteilt Spitta Aufträge an Subunternehmer, so obliegt es Spitta, die datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Spitta ist insbesondere dazu verpflichtet, die Subunternehmer entsprechend Ziffer 3.5 dieses Vertrags zur Geheimhaltung zu verpflichten.

7.3 Auf schriftliche Aufforderung des Auftraggebers hat Spitta jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen der Subunternehmer zu erteilen.

7.4 Die Regelungen in dieser Ziffer 7 gelten auch, wenn – unter Wahrung der Grundsätze von Kapitel 5 der DSGVO – ein Subunternehmer in einem Drittstaat eingeschaltet wird. Spitta erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Kapitel 5 der DSGVO im erforderlichen Maße mitzuwirken.

8. Subunternehmer (weitere Auftragsverarbeiter) Haftung

8.1 Es gelten die Haftungsbeschränkungen aus dem Hauptvertrag.

8.2 Die Vertragsparteien haften entsprechend der in Art. 82 DSGVO getroffenen Regelungen. Im Innenverhältnis gilt Art. 28 Abs. 4 Satz 2 DSGVO.

9. Informationspflichten, Schriftformklausel, Rechtswahl

9.1 Sollten die personenbezogenen Daten des Auftraggebers bei Spitta durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat Spitta den Auftraggeber unverzüglich darüber zu informieren. Spitta wird alle Dritten in diesem Zusammenhang unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der DSGVO liegen.

9.2 Änderungen und Ergänzungen dieses Vertrages und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen von Spitta – bedürfen der Schriftform, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.3 Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages zum Datenschutz den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

9.4 Es gilt deutsches Recht. Gerichtsstand ist München.

Anlage 1: Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DS-GVO)

1) Der Auftragnehmer hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

2) Diese Maßnahmen können unter anderem die Pseudonymisierung und die Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind.

3) Die Maßnahmen sollen dazu führen, dass
   a) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und,
   b) dass die Verfügbarkeit personenbezogener Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

4) Der Auftragsverarbeiter hat nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Zutrittskontrollsystem, zentrale Schlüsselverwaltung, Magnetkarte
- ✓ Schlüssel/Schlüsselvergabe ist zentral und organisatorisch klar geregelt
- ✓ Klare Zuweisung der Berechtigungen (Zugang Gebäude, Büro, Serverraum)
- ✓ Gebäudeschutz an Wochenenden und nachts gewährleistet
- ✓ Pförtner/Empfang mit Videoüberwachung
- ✓ Regelungen für Besucher (Besucherausweis, Begleitung im Gebäude)
- ✓ Videoüberwachung sensibler Bereiche des Gebäudes (Tiefgarage)
- ✓ Verschließen von Schränken und Büros bei Nichtanwesenheit

Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Dezidiertes Kennwortverfahren zum Login [z.B. Klare Passwortregelung (bestimmte Länge, Kombination aus Buchstaben und Zahlen, keine Trivialpasswörter, Änderung in regelmäßigen Abständen). Voreingestellte Passwörter müssen umgehend geändert werden]
- ✓ Automatische Sperrung (z.B. Regelung zur automatischen Sperrung des Computers nach einer bestimmten Zeit der Inaktivität (ca. 5 min) mit anschließendem erneutem Login)

- ✓ Automatischer Standby-Betrieb der lokalen Rechner
- ✓ Verschlüsselung von Datenträgern möglich
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträgern/Smartphones aus den Büroräumen heraus
- ✓ Möglichkeit der Fernlöschung von Smartphones

Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Differenzierte Berechtigungen (Profile, Rollen)
- ✓ Differenziertes Ordnerkonzept (z.B. alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können).
- ✓ Datenträger sind eindeutig zu kennzeichnen und sicher aufzubewahren.
- ✓ Sichere Löschung von Daten und/ oder Vernichtung von Datenträgern.
- ✓ Ordnung am Arbeitsplatz [Datenträger (USB-Sticks, CD-ROMs) mit vertraulichem Material dürfen nicht offen herumliegen].
- ✓ Anpassung sicherheitsrelevanter Standardeinstellungen von neuen Programmen und IT-Systemen
- ✓ Deinstallation bzw. Deaktivierung nicht benötigter sicherheitsrelevanter Programme und Funktionen (v.a. bei Smartphones)

Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Protokollierungs- und Protokollauswertungssysteme werden eingesetzt bzw. sind als Teile von bestehenden Softwareapplikationen anwendbar
- ✓ Zugriff auf Datenverarbeitungssysteme nur nach Login möglich
- ✓ Keine Weitergabe von Passwörtern
- ✓ Zusätzlich zur automatischen Sperrung: manuelle Abmeldung beim Verlassen des Büros

Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Verschlüsselung (insbes. Laptops)
- ✓ Tunnelverbindung (VPN = Virtual Private Network)
- ✓ Elektronische Signatur möglich
- ✓ Keine Benutzung von nicht freigegebener Hard-/ Software
- ✓ Keine Weiterleitung von E-Mails an private E-Mail-Accounts von Mitarbeitern
- ✓ Vorsicht beim Umgang mit Backup-Bändern
- ✓ Vorgaben an Mitarbeiter bzgl. Ausdrucken von geheimen Unterlagen (Sicherstellung, dass kein anderer Zugriff auf Ausdrucke bekommt).
- ✓ Regelung zum Einsatz von USB-Sticks und CD-ROMs

Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Eindeutige Vertragsgestaltung/Standardvertrag zu Art. 28 DS-GVO vorhanden
- ✓ Formalisierte Auftragserteilung (Auftragsformular)
- ✓ Kriterien zur Auswahl des Auftragnehmers wird stringent eingehalten
- ✓ Kontrolle der Vertragsausführung wird durch den DSB gewährleistet

Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Regelmäßiges Backup-Verfahren ist sichergestellt (Einbeziehung von Laptops und nicht vernetzten Systemen; Regelmäßige Kontrolle der Sicherungsbänder; Dokumentierung der Sicherungsverfahren)
- ✓ Getrennte Aufbewahrung von Daten ist gewährleistet
- ✓ Virenschutz/Firewall nach aktuellem Stand der Technik ist gewährleistet
- ✓ Schutz gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall im Serverraum

- ✓ Notfallplan besteht und wird regelmäßig geübt
- ✓ Notstromversorgung/Unterbrechungsfreie Stromversorgung (USV)
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträger aus den Büroräumen heraus
- ✓ Vertretungsregelungen, v.a. bzgl. Administrator

Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Physisch und/oder logisch getrennte Speicherung, Veränderung, Löschung und Übermittlung von Daten, die unterschiedlichen Zwecken dienen (Mandantenfähigkeit)
- ✓ Funktionstrennung, insbesondere zwischen Produktions- und Testdaten

Regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen

- ✓ Regelmäßige fachliche Fortbildung der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten
- ✓ Schulung der Mitarbeiter im Umgang mit der IT und zur Schärfung des IT-Sicherheitsbewusstseins
- ✓ Sicherheitshinweise werden allen Mitarbeitern in geeigneter Form bekannt gegeben und sind dauerhaft abrufbar (z.B. durch Veröffentlichung im Intranet)
- ✓ Auswertung von Meldungen und Berichten zu ungewöhnlichen Vorkommnissen
- ✓ Untersuchung erkannter oder vermuteter Verstöße gegen sicherheitsrelevante Vorgaben
- ✓ Regelmäßige Prüfung der Effektivität der bestehenden technischen und organisatorischen Maßnahmen und Prüfung, ob neue technische und organisatorische Maßnahmen erforderlich sind (beides unter Hinzuziehung des Datenschutzbeauftragten)
- ✓ Regelmäßige und anlassbezogene Kontrolle der Funktionalität der IT, einschließlich unter dem Aspekt der Zutrittskontrolle
- ✓ Eskalations- und Meldewege bei sicherheitsrelevanten Vorkommnissen
- ✓ Verfügbarkeit der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten als Ansprechpartner bei allen Fragen zur IT-Nutzung und -sicherheit.

Anlage 2: Unterauftragsverarbeiter (Subunternehmer) zum AV-Vertrag

Unterauftragsverarbeiter	Kontaktdaten	Gegenstand der Verarbeitung
eHealthExperts GmbH	Emil-Figge-Straße 85 44227 Dortmund	2nd Level Support