Vertrag zur Auftragsdatenverarbeitung

HASOMED GmbH
Paul-Ecke-Straße 1
D-39114 Magdeburg

- nachfolgend Auftragnehmer genannt -

§ 1 Gegenstand und Dauer des Auftrages

(1) Der Auftragnehmer führt die in Anhang 1 beschriebenen Dienstleistungen für den Auftraggeber aus. Gegenstand, Art und Zweck der Datenverarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt, solange keine anderweitigen Regelungen vereinbart wurden, mit Vertragsabschluss in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.

§ 2 Weisungen des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung, sowie die Wahrung der Betroffenenrechte verantwortlich. Vertragliche und /oder gesetzliche Haftungsregeln bleiben hiervon unberührt.

(2) Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Auftraggeber dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung des Auftraggebers, es sei denn, der Auftraggeber ist durch das Recht der Europäischen Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchem Fall sind diese rechtlichen Anforderungen vor der Verarbeitung durch den Auftragnehmer, dem Auftraggeber mitzuteilen, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Weisungen die die Verarbeitung personenbezogener Daten auf den IT-Systemen des Auftragnehmers beinhalten bedürfen der Schriftform durch den Auftraggeber. Diese Weisungen sind durch den Auftragnehmer zu dokumentieren.

(5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind (BDSG, DS-GVO). Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragnehmer bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen (TOM; siehe Anhang 3) durchgeführt werden. Diese gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Betroffenenrechten steht.

(3) Der Auftragnehmer sichert zu, dass die Mitarbeiter, welche mit der Durchführung der Arbeiten betraut werden, mit den für ihn maßgeblichen Bestimmungen des Datenschutzes vertraut sind und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit und Geheimhaltung verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Der Auftragnehmer darf im Rahmen der Auftragsdatenverarbeitung nur dann auf personenbezogene Daten des Auftraggebers zugreifen, wenn dies für die Durchführung der Auftragsdatenverarbeitung notwendig ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer einen Datenschutzbeauftragten. Die Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt (siehe Anhang 1).

(6) Der Auftragnehmer darf die ihm zur Verfügung gestellten personenbezogen Daten ausschließlich innerhalb der Mitgliedsstaaten der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen, damit diese seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z. B. die Berichtigung und / oder Löschung von personenbezogen Daten, die Information und Auskunft an die betroffene Person, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Der Auftragnehmer benennt einen Ansprechpartner, der den Auftraggeber bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsdatenverarbeitung entstehen, unterstützt und teilt dem Auftraggeber dessen Kontaktdaten unverzüglich

mit. Soweit der Auftraggeber besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt der Auftragnehmer den Auftragsgeber hierbei.

(8) Bei den Daten des Auftraggebers handelt es sich in der Regel um Daten, die dem Schutzbereich des § 203 StGB unterliegen. Durch landesrechtliche Regelungen ist eine Einschaltung von Dienstleistern dennoch unter bestimmten Umständen erlaubt. Zudem dürfen nach § 203 Abs. 3 StGB mitwirkende Personen eingeschaltet werden, soweit dies erforderlich ist. Allerdings ist der Auftraggeber verpflichtet, sicherzustellen, dass alle Mitwirkenden zur Geheimhaltung verpflichtet wurden. Der Auftragnehmer verpflichtet sich daher, alle Personen, die im Rahmen der beauftragten Tätigkeit mitwirken, auf die Geheimhaltung nach § 203 StGB zu verpflichten. Dies bedeutet insbesondere, dass für die Verarbeitung nur Mitarbeiter eingesetzt werden dürfen, die durch den Auftragnehmer vorher schriftlich auf die Verschwiegenheit nach § 203 StGB verpflichtet wurden. Dem Auftragnehmer ist bekannt, dass hinsichtlich der dem Berufsgeheimnis unterliegenden Daten ein Zeugnisverweigerungsrecht nach § 53a StPO besteht. Über die Ausübung des Rechtes auf Zeugnisverweigerung entscheidet der Berufsgeheimnisträger des Auftraggebers. Dem Auftragnehmer ist bekannt, dass die dem Berufsgeheimnisträger unterliegenden Daten, die sich im Gewahrsam des Auftragnehmers zur Erhebung, Verarbeitung oder Nutzung befinden, dem Beschlagnahmeverbot des § 97 Abs. 2 S. 2 StPO unterliegen. Einer Sicherstellung ist zu widersprechen. Der Auftraggeber ist unverzüglich schriftlich zu informieren, wenn eine Beschlagnahme der Daten zu erwarten ist, bevorsteht oder erfolgt ist.

§ 4 TOM (technische und organisatorische Maßnahmen)

(1) Der Auftragnehmer verpflichtet sich, für die zu verarbeiten Daten angemessene technische und organisatorische Maßnahmen zu treffen und im Anhang 3 dieses Vertrages zu dokumentieren. Die TOM haben ein dem Risiko angemessenen Schutzniveau zu entsprechen.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragnehmer darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Schutzniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragnehmer dem Auftraggeber nur wesentliche Anpassungen schriftlich mitteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Der Auftragnehmer hat auf schriftliche Anfrage an der Erstellung und Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten (VdV) des Auftraggebers mitzuwirken. Der Auftragnehmer wirkt bei der Erstellung einer Datenschutzfolgeabschätzung und ggf. vorherigen Konsultation der Aufsichtsbehörde mit. Der Auftragnehmer hat dem Auftraggeber alle erforderlichen Angaben und Dokumente auf schriftliche Anfrage offenzulegen.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragnehmer ist berechtig seine Servicepartner in Teilen oder im Ganzen mit Leistungen, im Unterauftragsverhältnis, zu beauftragen. Der Auftragnehmer darf andere, als die Servicepartner, Unterauftragnehmer nur beauftragen, wenn der Auftraggeber dies vorher schriftlich genehmigt hat.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragnehmer weitere Auftragnehmer in Teilen oder Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Postversand und Weitergabe der Kontaktdaten des Auftraggebers an Servicepartner

zur Erbringung von Serviceleistungen. Der Auftragnehmer ist jedoch verpflichtet, auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn der Auftragnehmer durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt. Bei Einschaltung von Unterauftragnehmern ist der Auftragnehmer zudem verpflichtet, die Verpflichtung der weitern mitwirkenden Personen entsprechend § 203 StGB und § 3 Abs. 8 dieses Vertrages sicherzustellen.

(4) Die Inanspruchnahme der im Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

§ 6 Kontrollrechte des Auftraggebers

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihm beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderungen von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragnehmers zu den ausgewiesenen Geschäftszeiten nach vorheriger schriftlicher Anmeldung.

§ 7 Mitteilungspflichten bei Verstößen des Auftraggebers

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich schriftlich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit Daten des Auftraggebers. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. den betroffenen Personen unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Meldepflicht unterstützen. Der Auftragnehmer wird die Verletzungen des Auftraggebers unverzüglich schriftlich melden und hierbei zumindest folgende Informationen mitteilen:

a) Eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze
b) Name und Kontaktdaten eines Ansprechpartners für weiter Informationen
c) Eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
d) Eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsdatenverarbeitung hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, soweit nicht andere gesetzliche Regelungen dem entgegenstehen.

(2) Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrages oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeber aufgrund dessen die Fortsetzung der Auftragsdatenverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers bei dem Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich schriftlich zu informieren.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des übrigen Vertrags nicht.

Anhang 1

Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

1.1	Gegenstand der Dienstleistung bei den personenbezogene Daten verarbeitet werden können
	Produkte: RehaCom, FES Stimulator, RehaGait, RehaIngest, NeXus, tDCS, Stimulette, Tobii • Telefonischer Support, Support per Fernwartungstool und Support vor Ort • Reparatur und Wartungsarbeiten
	Produkt: Praxisverwaltungssoftware - “Elefant” • Telefonischer Support und Support per Fernwartungstool im Rahmen der Praxissoftware Elefant

1.2	Art und Zweck der Verarbeitung
	Produkte: RehaCom, FES Stimulator, RehaGait, RehaIngest, NeXus, tDCS, Stimulette, Tobii • Wartung des Systems • Unterstützung bei Problemen in der Nutzung • Wiederherstellung defekter Patientendatenbank
	Produkt: Praxisverwaltungssoftware - “Elefant” • Entwicklung und Wartung des IT-Systems • Beantwortung von Nutzerfragen im 1st und 2nd Level Support • Unterstützung bei der Installation der Anwendungssoftware Elefant • Unterstützung bei Problemen mit Schnittstellensoftware • Unterstützung bei Problemen in der Nutzung von Elefant • Unterstützung bei der Ursachenfindung bei Systemmeldungen • Reparatur und Wartung der Datenbank auf dem IT-System der Auftraggeberin

1.3	Art der Personenbezogenen Daten
	<u>Produkte:</u> <u>RehaCom, FES Stimulator, RehaGait, RehaIngest, NeXus, tDCS, Stimulette, Tobii</u> Kenntnisnahme von: • Patientendatenbank und Inhalte der Patientenakten einschließlich Trainingsergebnissen • Zugangsdaten Patientenkonten
	<u>Produkt:</u> <u>Praxisverwaltungssoftware - “Elefant”</u> Kenntnisnahme von: • Patientenliste und Inhalte der Patientenakten • Terminplan der Praxis • Abrechnungsdaten und Statistiken der Praxis

1.4	Kategorien betroffener Personen
	<u>Produkte:</u> <u>RehaCom, FES Stimulator, RehaGait, RehaIngest, NeXus, tDCS, Stimulette, Tobii</u> Kenntnisnahme von: • Arzt/Therapeut • IT/EDV • Patienten • Bezugspersonen des Patienten
	<u>Produkt:</u> <u>Praxisverwaltungssoftware - “Elefant”</u> Kenntnisnahme von: • Therapeut bzw. Arzt • Patienten • Bezugspersonen des Patienten

1.5	Kontaktdaten des Datenschutzbeauftragten der HASOMED			
	Name:	Stephan Jacobs		
	E-Mail:	datenschutz@hasomed.de	Tel.:	00 49 391 62 30 112
	Straße:	Paul-Ecke-Straße	Hausnr.:	1
	PLZ:	39114	Ort:	Magdeburg
	Land:	Deutschland		

Anhang 2

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer			Verarbeitungsstandort	Produkt	Art der Dienstleistungen
Name	**Rechtsform**	**Sitz der Gesellschaft**			
Doetsch, Norbert – Intermac Systems	Einzelunternehmen	Koblenz	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Erhardt IT Solutions	GmbH	Ludwigsburg	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Hoffmann, Jörn - "IT. u. EDV-Dienstleistungen"	Einzelunternehmen	Rüschkamp 1, 24161 Altenholz	Deutschland	Praxissoftware - "Elefant"	TI-Installation
IS Intelligent Solution GmbH	GmbH	Imstedt 22-24 22083 Hamburg	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Köhler, Björn – "PC-Officium"	Einzelunternehmern	Burgherrenstr. 7, 12101 Berlin, Deutschland	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Köhn, Hellmut – "PC-Support Berlin"	Einzelunternehmen	Berlin, Deutschland	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Krischke-IT Harald Krischke	Einzelunternehmen	Würselen	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation

Unterauftragnehmer			Verarbeitungsstandort	Produkt	Art der Dienstleistungen
Name	**Rechtsform**	**Sitz der Gesellschaft**			
Krull, Michael - "EDV-Support & Handel"	Einzelunternehmen	79252 Stegen	Deutschland, Interne Speicherung	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Liedtke, Johannes	Einzelunternehmen	Dransfeld	lokal im Firmensitz & bei Drittanbietern (Cloud, ADV liegen vor)	Praxissoftware - "Elefant"	Schulungen, TI-Installation
Mehnert, Matthias - "PIP-Erwitte"	Einzelunternehmen	59597 Erwitte	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Reimann, Lutz - "PC-Service"	Einzelunternehmen	Orber Strasse 2 14193 Berlin	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Systembetreuung Lösel GmbH	GmbH	Nauheim	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Warsideh-Frank, Gerhard - "MW Computer"	Einzelunternehmen	Weidenhäuser Str. 6 35037 Marburg	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Weber, Matthias - "der-praxis-profi.de"	Einzelunternehmen	Lindäcker 10 88433 Schemmerhofen	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation

Unterauftragnehmer			Verarbeitungsstandort	Produkt	Art der Dienstleistungen
Name	**Rechtsform**	**Sitz der Gesellschaft**			
Computer Horizonte Anja Kopp	Einzelunternehmer	Bremervörder Str. 28 28219 Bremen	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Emden-EDV Holger Emden	Einzelunternehmer	Malchiner Straße 37 12359 Berlin	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Fa. datenstrom Thomas Klug		Hildegardstr. 6 42897 Remscheid	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Fa. Tecont Leipzig GmbH Dr. Torsten Greiner	GmbH	Apelsteinallee 12-14 04416 Wachau	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Praxis-Service *"Adam"* Adam Toth	Einzelunternehmer	Weiherstr. 10 41061 Mönchengladbach	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Softbyte ITK & Healthcare Consulting Emil Volkmer		Haardstr. 17 67161 Gönnheim	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation
Systembetreuung Hoenicke Christoph Hoenicke		Olof-Palme-Platz 4 18439 Stralsund	Deutschland	Praxissoftware - "Elefant"	HASOMED Praxis-Check, TI-Installation

Anhang 3

Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DS-GVO der HASOMED GmbH

Inhaltsverzeichnis

1. Zutrittskontrollmaßnahmen

um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- ✓ Alarmanlage mit Anschluss an Sicherheitsdienst
- ✓ Manuelles Schließsystem
- ✓ Videoüberwachung des Hauptzuganges und der Außenbereiche
- ✓ Bewegungsmelder in den Fluren und Sicherheitsbereichen
- ✓ Sicherheitsschlösser an allen Außentüren
- ✓ Personifizierte Schlüsselregelung (Schlüsselausgabe usw.)
- ✓ Firmeninternes Reinigungspersonal
- ✓ Eigener klimatisierter, fensterloser Serverraum

2. Zugangskontrollmaßnahmen

um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- ✓ Automatische Sperrung des Desktops nach fünf Minuten
- ✓ Zuordnung von Benutzerrechten
- ✓ Erstellen von Benutzerprofilen
- ✓ Passwortvergabe
- ✓ Authentifikation mit Benutzername / Passwort
- ✓ Zuordnung von Benutzerprofilen zu IT-Systemen
- ✓ Einsatz von VPN-Technologie
- ✓ Sicherheitsschlösser
- ✓ Personifizierte Schlüsselregelung (Schlüsselausgabe etc.)
- ✓ Firmeninternes Reinigungspersonal
- ✓ Einsatz von Anti-Viren-Software
- ✓ Einsatz einer Software-Firewall
- ✓ Einsatz einer Hardware-Firewall
- ✓ Einsatz von Intrusion-Detection-Systemen

3. Zugriffskontrollmaßnahmen

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

- ✓ Erstellen eines Berechtigungskonzepts
- ✓ Verwaltung der Rechte durch firmeninterne Systemadministratoren
- ✓ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ✓ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel 6-monatlich mit zehn Stellen, Ziffern und Sonderzeichen
- ✓ Sichere Aufbewahrung von Datenträgern
- ✓ Löschung von Datenträgern vor Wiederverwendung
- ✓ Nicht mehr benötigte Papierunterlagen werden geschreddert und dann entsorgt

4. Eingabekontrollmaßnahmen

sodass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht worden sind:

- ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

5. Auftragskontrollmaßnahmen

sodass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- ✓ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und Verschwiegenheit)
- ✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ✓ Regelmäßige Schulungen der Mitarbeiter zum Thema Datenschutz
- ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

6. Verfügbarkeitskontrollmaßnahmen

sodass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- ✓ Unterbrechungsfreie Stromversorgung (USV)
- ✓ Klimaanlage in Serverräumen
- ✓ Geräte zur Überwachung von Temperatur in Serverräumen
- ✓ Schutzsteckdosenleisten in Serverräumen
- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Erstellen eines Backup- & Recoverykonzepts
- ✓ Testen von Datenwiederherstellung
- ✓ Erstellen eines Notfallplans
- ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ✓ Serverräume befinden sich nicht unterhalb von sanitären Anlagen
- ✓ In Hochwassergebieten: Serverräume über der Wassergrenze

7. Trennungsgebot

Maßnahmen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- ✓ Festlegung von Datenbankrechten
- ✓ Trennung von Produktiv- und Testsystem