

Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

zwischen

Universitätsmedizin Greifswald
Körperschaft des öffentlichen Rechts
Fleischmannstraße 8
17475 Greifswald

(Verantwortlicher im Sinne der DS-GVO, nachfolgend „Auftraggeber“ genannt)

und

(Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend „Auftragnehmer“ genannt)

Inhaltsverzeichnis

PRÄAMBEL	5
§1 DEFINITIONEN.....	5
(1) ANONYMISIERUNG	5
(2) DRITTLAND	5
(3) HAUPTVERTRAG	5
(4) UNTERAUFTRAGNEHMER	5
(5) VERARBEITUNG IM AUFTRAG	5
(6) WEISUNG	5
§2 GEGENSTAND DES AUFTRAGS.....	6
(1) ART DER DATEN (KATEGORIEN):	6
(2) KREIS DER BETROFFENEN (KATEGORIEN):.....	6
§3 VERANTWORTLICHKEIT	6
(1) AUFTRAGGEBER	6
(2) UNTERAUFTRAGNEHMER	6
(3) AUFTRAGGEBER UND AUFTRAGNEHMER	6
(4) DATENSCHUTZGESETZE	7
§4 DAUER DES AUFTRAGS.....	7
(1) LAUFZEIT	7
(2) VERARBEITUNG OHNE AV-VERTRAG	7
(3) FRISTLOSE KÜNDIGUNG	7
(4) FORM DER KÜNDIGUNG	7
§5 WEISUNGSBEFUGNIS DES AUFTRAGGEBERS	7
(1) WEISUNGSRECHT	7
(2) DOKUMENTATION	7
(3) ÄNDERUNGEN	7
(4) MÜNDLICHE WEISUNGEN	8
§6 LEISTUNGSSORT.....	8
(1) ORT DER LEISTUNGSERBRINGUNG.....	8
(2) VERLAGERUNG	8
(3) INFORMATION	8
(4) ZUSTIMMUNG	8
(5) DRITTSTAAT	8
(6) VERWEIGERUNG	8
(7) ZUGRIFF DURCH DEN AUFTRAGNEHMER	8
(8) GESETZLICHE ERFORDERNISSE UND DATENSCHUTZNIVEAU.....	8
§7 PFLICHTEN DES AUFTRAGNEHMERS.....	9
(1) VERARBEITUNG.....	9
(2) TECHNISCH-ORGANISATORISCHE MAßNAHMEN.....	9
(3) DATENSCHUTZ- UND SICHERHEITSKONZEPT	9
(4) VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN	9
(5) DATENSCHUTZFOLGEABSCHÄTZUNG	9
(6) FERNMELDEGEHEIMNIS	9
(7) VERTRAULICHKEIT	9
(8) VERSCHWIEGENHEIT DER ERFÜLLUNGSGEILFEN	10
(9) DATENSCHUTZBEAUFTRAGTER	10

(10)	VERSTÖßE	10
(11)	ANTRAG AUF BERICHTIGUNG ODER LÖSCHUNG	10
(12)	ÜBERLASSENE DATENTRÄGER	10
(13)	UNTERSTÜTZUNG BEI DER ERFÜLLUNG DER BETROFFENENRECHTE	10
(14)	AUFSICHTSBEHÖRDEN	10
(15)	VERSTOß DURCH DEN AUFTRAGGEBER	11
(16)	EIGENTUM AN DEN DATEN	11
(17)	EIGENE VERARBEITUNGEN	11
(18)	EIGENE VERARBEITUNGEN	11
(19)	RECHTLICHE VERPFLICHTUNG ZUR VERARBEITUNG	11
(20)	PFLICHTERFÜLLUNG	11
§7.1 VEREINBARUNG ZUR WAHRUNG DES BERUFSGEHEIMNISSES NACH § 203 STGB		12
(1)	BERUFSGEHEIMNIS	12
(2)	BERUFSGEHEIMNIS BEI TÄTIGE PERSONEN	12
(3)	BERUFSGEHEIMNIS BEI UNTERAUFTRAGNEHMERN	12
(4)	ZEUGNISVERWEIGERUNGSRECHT	12
(5)	BESCHLAGNAHME	13
§ 8 FERNZUGRIFF BEI PRÜFUNG/WARTUNG EINES SYSTEMS ODER ANDEREN DIENSTLEISTUNGEN ÜBER FERNZUGRIFFE.....		13
(1)	FREIGABE	13
(2)	ZUSTIMMUNG	13
(3)	VERSCHLÜSSELUNG.....	13
(4)	DATENSICHERHEIT	13
(5)	DOKUMENTATION	13
(6)	DURCHFÜHRUNG	13
(7)	FEHLERANALYSE.....	13
(8)	DATENABZUG	14
(9)	TECHNISCH- UND ORGANISATORISCHE MAßNAHMEN	14
§9 PFLICHTEN DES AUFTRAGGEBERS		14
(1)	ZULÄSSIGKEIT UND BETROFFENENRECHTE	14
(2)	VERSTÖßE DURCH DEN AUFTRAGNEHMER	14
(3)	GENEHMIGTE VERFAHREN	14
(4)	INFORMATIONSPFLICHTEN.....	14
(5)	ÜBERLASSENE DATENTRÄGER	14
(6)	VERTRAULICHKEIT	15
(7)	VERSCHWIEGENHEIT DER ERFÜLLUNGSGEHILFEN	15
(8)	SICHERHEIT DER VERARBEITUNG.....	15
(9)	EINZELWEISUNGEN	15
§10 KONTROLLRECHTE DES AUFTRAGGEBERS		15
(1)	AUSWAHL DES AUFTRAGNEHMERS	15
(2)	VERSTOß DURCH DEN AUFTRAGNEHMER.....	15
(3)	AUFTRAGSKONTROLLE.....	15
(4)	INFORMATION DES AUFTRAGNEHMERS.....	16
§ 11 BERICHTIGUNG, BESCHRÄNKUNG VON VERARBEITUNG, LÖSCHUNG UND RÜCKGABE VON DATENTRÄGERN		16
(1)	BERECHTIGUNG	16
(2)	VERNICHTUNG.....	16
(3)	AUFBEWAHRUNG ODER ÜBERGABE.....	16
(4)	LÖSCHUNG ODER RÜCKGABE	16
(5)	KOSTEN.....	16
(6)	TRANSPORT	16
(7)	AUFBEWAHRUNG DER DOKUMENTATION	16

(8)	VERARBEITUNG AUF VERLANGEN.....	16
(9)	WEISUNGEN	17
(10)	LÖSCHUNG STATT RÜCKNAHME.....	17
(11)	TESTDATEN	17
§12 UNTERAUFTRAGNEHMER		17
(1)	BERECHTIGUNG	17
(2)	NACHFOLGENDE UNTERAUFTRAGNEHMER	17
(3)	ÄNDERUNGEN	17
(4)	INFORMATION DES AUFTRAGGEBERS.....	17
(5)	GENEHMIGTE UNTERAUFTRAGNEHMER	18
(6)	AUSWAHL.....	18
(7)	DURCHGRIFF DES AV-VERTRAGS.....	18
(8)	AUSKUNFTSRECHT DES AUFTRAGGEBERS.....	18
(9)	NEBENLEISTUNGEN.....	18
(10)	HAFTUNG DES AUFTRAGNEHMERS.....	18
§13 ZURÜCKBEHALTUNGSRECHT		18
§14 HAFTUNG		18
§15 SCHRIFTFORMKLAUSEL		19
§16 SALVATORISCHE KLAUSEL		19
(1)	UNWIRKSAME ODER UNDURCHFÜHRBARE BESTIMMUNGEN.....	19
(2)	ERSATZ	19
(3)	ENTSPRECHUNG VON SINN UND ZWECK.....	19
(4)	WAHL DER ERSATZBESTIMMUNG.....	19
§17 RECHTSWAHL, GERICHTSSTAND.....		19
(1)	GELTENDES RECHT	19
(2)	GERICHTSSTANDSVEREINBARUNG	19
ANLAGE(N)		20
ANLAGE 1: UNTERAUFTRAGSVERHÄLTNISSE BEIM AUFTRAGNEHMER ZUM ZEITPUNKT DER AUFTRAGSVERGABE		21
ANLAGE 2: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM)		22
I.S.D. ART. 32 DSGVO.....		22
1.	VERTRAULICHKEIT GEM. ART. 32 ABS. 1 LIT. DSGVO	22
1.1.	Zutrittskontrolle	22
1.2.	Zugangskontrolle	23
1.3.	Zugriffskontrolle	24
1.4.	Trennungskontrolle.....	25
1.5.	Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)	25
2.	INTEGRITÄT (ART. 32 ABS. 1 LIT. B DSGVO)	26
2.1.	Weitergabekontrolle.....	26
2.2.	Eingabekontrolle.....	27
3.	VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)	28
3.1.	Verfügbarkeitskontrolle	28
4.	VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DSGVO; ART. 25 ABS. 1 DSGVO)	29
4.1.	Datenschutz-Management.....	29
4.2.	Incident-Response-Management.....	30
4.3.	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO).....	31
4.4.	Auftragskontrolle (Outsourcing an Dritte).....	32

Präambel

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) orientiert sich am Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen von BvD, bvitg, gmds, DKG, GDD und konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den in § 2 „Gegenstand des Auftrags“ dargestellten Leistungen ergeben.

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit der Auftragserfüllung in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

Gegenstand dieses Vertrages sind ausschließlich datenschutzrechtliche Regelungen zur Auftragsverarbeitung. Strafrechtliche Bestimmungen wie beispielsweise § 203 StGB können nicht Vertragsgegenstand sein.

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG und § 1 Digitale-Dienste-Gesetz (DDG) sowie Landesdatenschutzgesetz/Landeskrankenhausgesetz. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, Landesrecht, UWG und DDG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Anonymisierung

Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)

(2) Drittland

Ein Land, welches sich außerhalb der EU/EWR befindet.

(3) Hauptvertrag

Vertrag (i.d.R. ein Dienst-, Service- oder Werkvertrag), in welchem alle Einzelheiten der Verarbeitung beschrieben sind.

(4) Unterauftragnehmer

Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

(5) Verarbeitung im Auftrag

Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

(6) Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Gegenstand des Auftrags

Die konkrete Beschreibung von Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergibt sich ebenso wie die Dauer des Auftrages aus bestehenden und künftigen Haupt-Verträgen, nach deren Inhalt personenbezogene Daten im Auftrag für den Auftraggeber durch den Auftragnehmer erhoben, verarbeitet oder genutzt werden oder bei deren Erfüllung durch den Auftragnehmer ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(1) Art der Daten (Kategorien):

- Personalstammdaten
- Patientenkontakt- und Stammdaten
- Gesundheitsdaten und Befunddaten über Patienten aus stationären, Teilstationären und ambulanten Behandlungen
- In Zusammenhang mit Patientenunterlagen Angaben zur Identität und Verantwortlichkeit von medizinischem Personal, welches beim Auftraggeber beschäftigt ist
- In Zusammenhang mit Patientenunterlagen Angaben zur Identität und Verantwortlichkeit von medizinischem Personal, welches nicht beim Auftraggeber beschäftigt ist. (z.B. Konsiliarärzte, Honorar- und Belegärzte, sowie andere externe Fachkräfte)

(2) Kreis der Betroffenen (Kategorien):

- Patienten des Auftraggebers
- Ansprechpartner
- Beschäftigte
- Konsiliarärzte, Honorar- und Belegärzte, sowie andere externe Fachkräfte, deren Dokumentationen in Patientenunterlagen enthalten sein könnten

§ 3 Verantwortlichkeit

(1) Auftraggeber

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DS-GVO).

(2) Unterauftragnehmer

Die Inhalte dieses AV-Vertrages gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Auftraggeber und Auftragnehmer

Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

(4) Datenschutzgesetze

Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 4 Dauer des Auftrags

(1) Laufzeit

Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.

(2) Verarbeitung ohne AV-Vertrag

Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Fristlose Kündigung

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Form der Kündigung

Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 5 Weisungsbefugnis des Auftraggebers

(1) Weisungsrecht

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann.

(2) Dokumentation

Die Weisungen des Auftraggebers werden vom Auftragnehmer dokumentiert und dem Auftraggeber unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

(3) Änderungen

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer wesentlichen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, steht dem Auftragnehmer ein ordentliches Kündigungsrecht bezüglich des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages zu. Verweigert der Auftragnehmer, die Änderung durchzuführen, steht auch dem Auftraggeber ein ordentliches Kündigungsrecht zu. Erfolgt eine Kündigung, so ist für die restliche Vertragslaufzeit weiterhin die vertraglich vereinbarte Leistung durch den Auftragnehmer zu erbringen.

(4) Mündliche Weisungen

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilt, sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.

§ 6 Leistungsort

(1) Ort der Leistungserbringung

Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) erbringen, etwaige Unterauftragnehmer an den mit dem Auftraggeber in Anhang 1 vereinbarten Leistungsstandorten der Unterauftragnehmer in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).

(2) Verlagerung

Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

(3) Information

Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

(4) Zustimmung

Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

(5) Drittstaat

Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.

(6) Verweigerung

Bei einer Leistungserbringung in einem sicheren Drittstaat wird der Auftraggeber seine Zustimmung zur Verlagerung nicht unbillig verweigern. Die Einhaltung der diesbezüglichen Vorgaben der DS-GVO wird durch den Auftragnehmer gewährleistet.

(7) Zugriff durch den Auftragnehmer

Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

(8) Gesetzliche Erfordernisse und Datenschutzniveau

Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung

personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 7 Pflichten des Auftragnehmers

(1) Verarbeitung

Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) Technisch-organisatorische Maßnahmen

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO resultierenden Maßnahmen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt im Anlage 2 zu diesem Vertrag.

(3) Datenschutz- und Sicherheitskonzept

Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.

(4) Verzeichnis der Verarbeitungstätigkeiten

Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(5) Datenschutzfolgeabschätzung

Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

(6) Fernmeldegeheimnis

Die Wahrung des Fernmeldegeheimnisses entsprechend § 3 TDDDG muss vom Auftragnehmer gewährleistet werden. Dazu muss der Auftragnehmer alle Personen, die auftragsgemäß auf Daten des Auftraggebers mittels Mittel der Telekommunikation wie Telefon oder E-Mail zugreifen können, auf das Fernmeldegeheimnis verpflichten und über die sich daraus ergebenden besonderen Geheimhaltungspflichten belehren.

(7) Vertraulichkeit

Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von

Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

(8) Verschwiegenheit der Erfüllungsgehilfen

Weiterhin sind alle Personen des Auftragnehmers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftraggebers zu verpflichten und müssen auf die Regelungen des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) hingewiesen werden.

(9) Datenschutzbeauftragter

Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit

benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(10) Verstöße

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Artt. 33, 34 DS-GVO.

(11) Antrag auf Berichtigung oder Löschung

Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(12) Überlassene Datenträger

Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

(13) Unterstützung bei der Erfüllung der Betroffenenrechte

Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert.

(14) Aufsichtsbehörden

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(15) Verstoß durch den Auftraggeber

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(16) Eigentum an den Daten

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DS-GVO liegen.

(17) Eigene Verarbeitungen

Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden.

(18) Eigene Verarbeitungen

Der Auftragnehmer speichert keine Patientendaten auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.

(19) Rechtliche Verpflichtung zur Verarbeitung

Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, so teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Die Mitteilung hat zu unterbleiben, wenn das einschlägige nationale Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.

(20) Pflichterfüllung

Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

§ 7.1 Vereinbarung zur Wahrung des Berufsgeheimnisses nach § 203 StGB

(1) Berufsgeheimnis

Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.

Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1.

Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Berufsgeheimnis bei tätigen Personen

Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z. B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

(3) Berufsgeheimnis bei Unterauftragnehmern

Der Auftragnehmer ist berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist.

Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zur Geheimhaltung verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.

Des Weiteren werden Subunternehmer, über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmenschutz gemäß § 97 StPO informiert; dies beinhaltet auch den Hinweis bzgl. des Rechts des Berufsgeheimnisträgers, über dieses Recht zu entscheiden und der damit verbundenen Pflicht des AN, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

(4) Zeugnisverweigerungsrecht

Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der

Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(5) Beschlagnahme

Der Auftragnehmer wird darauf hingewiesen, dass die in seinem Gewahrsam befindlichen Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

§ 8 Fernzugriff bei Prüfung/Wartung eines Systems oder anderen Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) Freigabe

Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.

(2) Zustimmung

Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.

(3) Verschlüsselung

Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

(4) Datensicherheit

Vor Durchführung von Fernzugriffen werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(5) Dokumentation

Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abubrechen.

(6) Durchführung

Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(7) Fehleranalyse

Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) des

Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.

(8) Datenabzug

Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (USB-Speichersticks oder ähnliche Geräte) kopiert werden.

(9) Technisch- und organisatorische Maßnahmen

Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

§ 9 Pflichten des Auftraggebers

(1) Zulässigkeit und Betroffenenrechte

Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(2) Verstöße durch den Auftragnehmer

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Genehmigte Verfahren

Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(4) Informationspflichten

Dem Auftraggeber obliegen die aus Artt. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

(5) Überlassene Datenträger

Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Vertraulichkeit

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(7) Verschwiegenheit der Erfüllungsgehilfen

Weiterhin sind alle Personen des Auftraggebers bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Auftragnehmers zu verpflichten und müssen auf die Regelungen des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) hingewiesen werden.

(8) Sicherheit der Verarbeitung

Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

(9) Einzelweisungen

Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen. Sofern der vereinbarte Leistungsumfang überschritten wird, ist hierzu vorab eine gesonderte schriftliche Vereinbarung zu treffen.

§ 10 Kontrollrechte des Auftraggebers

(1) Auswahl des Auftragnehmers

Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichend Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Er dokumentiert das Ergebnis seiner Auswahl.

Hierfür kann er beispielsweise:

- datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und -prüfzeichen berücksichtigen,
- schriftliche Selbstauskünfte des Auftragnehmers einholen,
- sich ein Testat eines Sachverständigen vorlegen lassen oder
- sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

(2) Verstoß durch den Auftragnehmer

Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden.

(3) Auftragskontrolle

Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer

unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(4) Information des Auftragnehmers

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 11 Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern

(1) Berechtigung

Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

(2) Vernichtung

Sofern eine Vernichtung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber. Dies gilt nicht, sofern im Haupt-Vertrag bereits eine entsprechende Regelung getroffen worden ist.

(3) Aufbewahrung oder Übergabe

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

(4) Löschung oder Rückgabe

Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder diesem zurückgeben, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für alle Daten, die Betriebs- oder Geschäftsgeheimnisse des Auftraggebers beinhalten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(5) Kosten

Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostentragung.

(6) Transport

Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

(7) Aufbewahrung der Dokumentation

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(8) Verarbeitung auf Verlangen

Der Auftraggeber kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung (Sperrung) und Herausgabe von

Daten durch den Auftragnehmer verlangen, solange der Auftragnehmer die Möglichkeit hat, diesem Verlangen zu entsprechen.

(9) Weisungen

Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag anders vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(10) Löschung statt Rücknahme

Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

(11) Testdaten

Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung bzgl. einer Löschung nicht erforderlich, diese müssen gelöscht werden.

§ 12 Unterauftragnehmer

(1) Berechtigung

Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Dies gilt in gleicher Weise für den Fall, dass weitere Unterauftragsverhältnisse durch Unterauftragnehmer begründet werden. Der Auftragnehmer stellt sicher, dass eine entsprechende Genehmigung des Auftragsgebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt.

(2) Nachfolgende Unterauftragnehmer

Die nachfolgenden Regelungen finden sowohl für den Unterauftragnehmer als auch für alle in der Folge eingesetzten weiteren Unterauftragnehmer entsprechende Anwendung.

(3) Änderungen

Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(4) Information des Auftraggebers

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

(5) Genehmigte Unterauftragnehmer

Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage 1 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

(6) Auswahl

Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(7) Durchgriff des AV-Vertrags

Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

(8) Auskunftsrecht des Auftraggebers

Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(9) Nebenleistungen

Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

(10) Haftung des Auftragnehmers

Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

§ 13 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 14 Haftung

Die Haftung richtet sich nach gesetzlichen Bestimmungen der Artt. 82ff. DSGVO. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben hiervon unberührt.

§ 15 Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 16 Salvatorische Klausel

(1) Unwirksame oder undurchführbare Bestimmungen

Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(2) Ersatz

An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(3) Entsprechung von Sinn und Zweck

Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(4) Wahl der Ersatzbestimmung

Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

§ 17 Rechtswahl, Gerichtsstand

(1) Geltendes Recht

Es gilt deutsches Recht.

(2) Gerichtsstandsvereinbarung

Gerichtsstand ist der Sitz des Auftraggebers.

.....

.....

Anlage(n)

Anlage 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Anlage 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Anlage 1: Unterauftragsverhältnisse beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Unterauftragnehmer		
Name und Anschrift	Beschreibung der Teilleistung	Ort der Leistungserbringung

Anlage 2: Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☐ Schlüsselregelung / Liste
☐ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Protokoll der Besucher
☐ Chipkarten / Transpondersysteme	☐ Mitarbeiter- / Besucherausweise
☐ Manuelles Schließsystem	☐ Besucher in Begleitung durch Mitarbeiter
☐ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☐ Sorgfalt bei Auswahl Reinigungsdienste
☐ Absicherung der Gebäudeschächte	☐
☐ Türen mit Knauf Außenseite	☐
☐ Klingelanlage mit Kamera	☐
☐ Videoüberwachung der Eingänge	☐

Weitere Maßnahmen bitte hier beschreiben:

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Login mit Benutzername + Passwort	☐ Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	☐ Erstellen von Benutzerprofilen
☐ Anti-Viren-Software Server	☐ Zentrale Passwortvergabe
☐ Anti-Virus-Software Clients	☐ Richtlinie „Sicheres Passwort“
☐ Anti-Virus-Software mobile Geräte	☐ Richtlinie „Löschen / Vernichten“
☐ Firewall	☐ Richtlinie „Clean desk“
☐ Intrusion Detection Systeme	☐ Allg. Richtlinie Datenschutz und / oder Sicherheit
☐ Mobile Device Management	☐ Mobile Device Policy
☐ Einsatz VPN bei Remote-Zugriffen	☐ Anleitung „Manuelle Desktopsperre“
☐ Verschlüsselung von Datenträgern	☐
☐ Verschlüsselung Smartphones	☐
☐ Gehäuseverriegelung	☐
☐ BIOS Schutz (separates Passwort)	☐
☐ Sperre externer Schnittstellen (USB)	☐
☐ Automatische Desktopsperre	☐
☐ Verschlüsselung von Notebooks / Tablet	☐

Weitere Maßnahmen:

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Aktenschredder (mind. Stufe 3, cross cut)	☐ Einsatz Berechtigungskonzepte
☐ Externer Aktenvernichter (DIN 32757)	☐ Minimale Anzahl an Administratoren
☐ Physische Löschung von Datenträgern	☐ Datenschutztresor
☐ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐ Verwaltung Benutzerrechte durch Administratoren
☐	☐
☐	☐

Weitere Maßnahmen:

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung von Produktiv- und Testumgebung	☐ Steuerung über Berechtigungskonzept
☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☐ Festlegung von Datenbankrechten
☐ Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze sind mit Zweckattributen versehen
☐	☐
☐	☐

Weitere Maßnahmen:

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen (mögl. verschlüsselt)	☐ Interne Anweisung, personenbezogenen Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren /pseudonymisieren
☐	☐
☐	☐

Weitere Maßnahmen :

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten 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 personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Email-Verschlüsselung	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ Einsatz von VPN	☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☐ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☐
☐	☐
☐	☐

Weitere Maßnahmen:

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☐	☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
☐	☐ Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Feuer- und Rauchmeldeanlagen	☐ Backup & Recovery-Konzept (ausformuliert)
☐ Feuerlöscher Serverraum	☐ Kontrolle des Sicherungsvorgangs
☐ Serverraumüberwachung Temperatur und Feuchtigkeit	☐ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☐ Serverraum klimatisiert	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☐ USV	☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐ Schutzsteckdosenleisten Serverraum	☐ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☐ Getrennte Partitionen für Betriebssysteme und Daten
☐ RAID System / Festplattenspiegelung	☐
☐ Videoüberwachung Serverraum	☐
☐ Alarmmeldung bei unberechtigttem Zutritt zu Serverraum	☐
☐	☐
☐	☐

Weitere Maßnahmen:

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für Datenschutz-Management im Einsatz	☐ Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	☐ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☐ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
☐ Anderweitiges dokumentiertes Sicherheitskonzept	☐ Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt
☐ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☐ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
☐	☐ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
☐	☐ Formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☐
☐	☐

Weitere Maßnahmen:

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von Firewall und regelmäßige Aktualisierung	☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☐ Einsatz von Spamfilter und regelmäßige Aktualisierung	☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☐ Einsatz von Virens Scanner und regelmäßige Aktualisierung	☐ Einbindung von ☐ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	☐ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☐ Intrusion Prevention System (IPS)	☐ Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☐	☐
☐	☐

Weitere Maßnahmen:

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐
☐ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	☐
☐	☐
☐	☐

Weitere Maßnahmen:

4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
☐	☐ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
☐	☐ Schriftliche Weisungen an den Auftragnehmer
☐	☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellopflicht
☐	☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☐ Regelung zum Einsatz weiterer Subunternehmer
☐	☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus