Arbeitshilfe zur Präzisierung

technischer und organisatorischer Maßnahmen

beim Einsatz externer Dienstleister

bei der

Verarbeitung von Patientendaten

1. Auflage, Januar 2023

Inhalt

1 Präambel

Seit dem 1. Juni 2022 gilt die Neuregelung zu Art. 27 Abs. 4 und 6 BayKrG. Damit wurde seitens des Landesgesetzgebers für Kliniken die Möglichkeit eröffnet, bei externen Dienstleistern Gesundheitsdaten von Patienten datenschutzkonform zu verarbeiten. Um weiterhin bewährte Schutzelemente (Vertraulichkeit, Integrität, Verfügbarkeit) zu gewährleisten, verweist die Gesetzesbegründung auf die Schaffung eines Regelwerkes zur Präzisierung der technischen und organisatorischen Maßnahmen.

Gemäß dem gesetzlichen Auftrag hat die BKG diese Arbeitshilfe erarbeitet, die den bayerischen Kliniken eine Orientierung gibt, welche Rahmenbedingungen bei der Auslagerung von Dienstleistungen und insbesondere IT-Dienstleistungen geprüft werden müssen, um bei der Verarbeitung von Patientendaten durch externe Dienstleister den gebotenen Schutz der Patientendaten zu gewährleisten.

Kliniken sollten damit - sofern sie die Empfehlungen dieser Arbeitshilfe einhalten - gegenüber Betroffenen und Aufsichtsbehörden vereinfacht nachweisen können, dass die datenschutzrechtlichen Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, Datenminimierung, Intervenierbarkeit, Transparenz und Nichtverkettung bei der Auftragsverarbeitung eingehalten werden.

Dem Bayerische Landesbeauftragte für den Datenschutz (BayLfD) und dem Bayerische Landesamt für Datenschutzaufsicht (BayLDA) wurde diese Arbeitshilfe vorgelegt. Diese haben uns umfassend beraten und wertvolle datenschutzrechtliche Hinweise und Ergänzungen gegeben, die wir eingearbeitet haben.

Die Arbeitshilfe konzentriert sich auf Dienstleistungen, die im Klinikalltag regelmäßig vorkommen, und ist nicht abschließend. Sofern erforderlich, werden neue Dienstleistungen im Laufe der Zeit ergänzt.

2 Allgemeine Voraussetzungen zur Auftragsverarbeitung

Auch wenn mit der Streichung des Art. 27 Abs. 4 Satz 6 und mit der Neuregelung in Abs. 6 BayKrG die Verarbeitungen von sensiblen Patientendaten durch externe Dienstleister ermöglicht wurde, bedeutet dies nicht, dass das bisher geltende Schutzniveau unterschritten werden darf. Auch durch die Neuregelung ist der Einsatz von externen Dienstleistern, die keine Krankenhäuser sind, nicht völlig freigestellt, sondern gemäß der Datenschutz-Grundverordnung (DS-GVO) an bestimmte Voraussetzungen gebunden.

Deshalb wird im neugefassten Art. 27 Abs. 6 BayKrG explizit auf die notwendigen Regelungstatbestände aus Art. 28 (Auftragsverarbeiter) und Art. 32 DS-GVO (Sicherheit der Verarbeitung) verwiesen, damit Patientendaten nicht unberechtigt verwendet oder übermittelt werden können.

Auch der Bayerische Landesbeauftragte für den Datenschutz weist in seiner 43. Aktuellen Kurz-Information mit dem Titel „Auftragsverarbeitung bei bayerischen öffentlichen Krankenhäusern“, Stand: 1. Juni 2022, explizit darauf hin, dass Auftragsverarbeitungsverhältnisse insoweit nun auch mit anderen Auftragsverarbeitern als Krankenhäusern begründet werden dürfen. Die Gesetzesänderung mache aber auch bewusst, dass bayerische öffentliche Krankenhäuser Patientendaten betreffende Auftragsverarbeitungsverhältnisse mit externen IT-Dienstleistern nun noch mehr als bislang aktiv gestalten müssen, was keine "banale" Aufgabe sei. Die 43. Aktuelle Kurz-Information zählt hierzu auch eine Reihe von Gestaltungsimpulsen auf (Sensibilität, Umfang, Kreis der Beteiligten, sinkende Einflussmöglichkeiten, Cybercrime-Attacken, Datenübermittlungen in Drittländer, Einsatz von Subunternehmern, Rolle des Verantwortlichen bei der Verarbeitung).
Im Grundsatz gilt deshalb, dass der Einsatz eines externen Dienstleisters zur Verarbeitung von Patientendaten immer dann in Betracht gezogen werden sollte, wenn bisherige und zukünftige Verarbeitungen nicht anders zufriedenstellend zu lösen und zugleich unter Beachtung des Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DS-GVO erforderlich sind.

Ausgelagert werden können nur Verarbeitungen, die rechtmäßig sind, d. h. dass die Zulässigkeit der Verarbeitung entweder aufgrund eines gesetzlichen Erlaubnistatbestands oder einer Einwilligung der betroffenen Person gegeben sein muss (bzgl. Gesundheitsdaten besteht für die Einwilligung ein Ausdrücklichkeitserfordernis, vgl. Art. 9 Abs. 2 Buchst. a DSGVO).
Als gesetzlicher Erlaubnistatbestand kann unter bestimmten Voraussetzungen auch eine Interessensabwägung, Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO, in Betracht kommen. Sorgfältig und nachweislich zu prüfen ist in diesem Fall, dass die Verarbeitung zur Wahrung der berechtigten Interessen der Klinik erforderlich ist und die datenschutzbezogenen Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Sofern die Verarbeitung auf diese Rechtsgrundlage gestützt wird, steht der betroffenen Person nach Art. 21 Abs. 1 DS-GVO ein Widerspruchsrecht dagegen zu. Insb. durch festgelegte TOMs ist sicherzustellen, dass jede legitime Ausübung des Widerspruchsrechts (auf dessen Bestehen die verantwortliche Klinik gemäß Art. 21 Abs. 4 DS-GVO in jedem Fall hinzuweisen hat,) be-

rücksichtigt wird und in der Folge weitere Verarbeitungen für die Zukunft unterbleiben. In diesem Kontext ist darüber hinaus grundsätzlich zu beachten, dass Art. 21 Abs. 6 DS-GVO der betroffenen Person zudem ein Widerspruchsrecht einräumt, falls die sie betreffenden personenbezogenen Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gem. Art. 89 Abs. 1 DS-GVO verarbeitet werden.

Unabdingbare Grundlage für die Inanspruchnahme der Dienste eines Auftragsverarbeiters durch bayerische Krankenhäuser sind zum einen der rechtmäßige Abschluss eines Auftragsverarbeitungsvertrages (AV-Vertrages) gemäß Art. 28 Abs. 3 DS-GVO und zum anderen angemessene technische und organisatorische Maßnahmen zur Sicherstellung des Schutzniveaus, wie sie insbesondere in Art. 32 DS-GVO beschrieben sind. Zudem nutzen Kliniken im Rahmen einer Auftragsverarbeitung regelmäßig neue Betriebsmittel für die Datenverarbeitung, die vor ihrem Einsatz datenschutzrechtlich auf Erforderlichkeit und Verhältnismäßigkeit zu prüfen sind.

2.1 Abschluss eines Auftragsverarbeitungsvertrages gemäß Art. 28 DS-GVO

Die Auftragsverarbeitung beruht regelmäßig auf einem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter. Ein Auftragsverarbeiterist gemäß Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

Nach Maßgabe von Art. 28 DS-GVO ist die Auftragsverarbeitung für alle Formen der Datenverarbeitung in allen Rechtsbereichen zulässig. Allerdings ist es dem nationalen Gesetzgeber auf Grundlage der sogenannten „Öffnungsklauseln“ der Datenschutz-Grundverordnung (vgl. z. B. Art 6 Abs. 2 und 3, Art. 9 Abs. 3 und 4 DS-GVO) möglich, spezifischere Bestimmungen zur Auftragsverarbeitung im öffentlichen Bereich zu treffen. Insbesondere in besonders sensiblen Bereichen kann hierdurch die Zulässigkeit der Auftragsverarbeitung eingeschränkt sein. Jede öffentliche Stelle, die den Einsatz eines Auftragsverarbeiters erwägt, sollte daher sorgfältig prüfen, ob bereichsspezifische Vorschriften besondere Voraussetzungen für eine Auftragsverarbeitung vorsehen oder diese im Einzelfall ausschließen.

Gewählt werden dürfen nur geeignete Dienstleister. Deshalb ist bereits im Vorfeld auf die sorgfältige Auswahl des Auftragsverarbeiters zu achten. Zu prüfen sind dabei Kriterien wie vor allem die Zuverlässigkeit, Betriebsbereitschaft, Qualifikation der Mitarbeiter, Zertifizierungen, vorhandene Sicherheitsstandards etc.

Zwischen dem Krankenhaus als Verantwortlichem und dem IT-Dienstleister ist eine wirksame und eindeutige Vereinbarung nach Art. 28 DS-GVO – schriftlich oder elektronisch – abzuschließen.

Der AV-Vertrag legt unter anderem fest, welche Aufgaben der externe Dienstleister auf Weisung des Verantwortlichen (d. h. der jeweiligen Klinik) zu erfüllen hat. Dabei sind die Mindestinhalte gemäß Art. 28 Abs. 3 Satz 2 DS-GVO vertraglich festzulegen.

Diese rechtsverbindlichen Mindestinhalte umfassen insbesondere

- die Art und die Zwecke der Datenverarbeitung,

- die zu verarbeitenden Datenkategorien
- die betreffenden Personenkategorien,
- die Weisungsbefugnisse des Verantwortlichen,
- die Regelung von Vertraulichkeits- und Verschwiegenheitsverpflichtungen,
- Angaben zu Unterbeauftragungen, einschließlich der Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters
- Regelungen zum Thema Drittlandstransfer,
- die Regelung und die Hinweispflicht bezüglich der Betroffenenrechte (z. B. Auskunfts-, Informations- und Widerspruchsrechte),
- die Rückgabe und Löschung von personenbezogenen Daten,
- die Haftung,
- die uneingeschränkte Unterstützungspflicht einschließlich der Zurverfügungstellung aller erforderlichen Informationen durch den Auftragsverarbeiter, damit der Verantwortliche seinen datenschutzrechtlichen Pflichten (im Sinne einer vertrauensvollen Zusammenarbeit insb. durch notwenige Kontrollen und Weisungen) umfänglich nachkommen kann.

Der Klarheit halber sollte auch vertraglich festgelegt werden, welche Kompetenzen beim Verantwortlichen verbleiben z. B. hinsichtlich Datenzugriff bei Insolvenz, Pfändung etc. Außerdem empfiehlt sich die Angabe der Kontaktdaten der beiderseitigen Ansprechpartner im AV-Vertrag.

2.2 Darstellung der technischen und organisatorischen Maßnahmen

Technische und organisatorische Maßnahmen dienen dazu, die Rechte und Freiheiten der betroffenen Personen, also deren Grundrecht auf informationelle Selbstbestimmung zu schützen. Der Schutzbedarf der verarbeiteten Daten wird teilweise normativ besonders geregelt.

Gesundheitsdaten gehören laut Definition zu den sogenannten besonderen Kategorien personenbezogener Daten (vgl. Art. 9 Abs. 1 DS-GVO), d. h. zu den **Datenarten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind und daher einen besonderen Schutz verdienen** (siehe Erwägungsgrund 51 Satz 1 DS-GVO). Diese besonderen Datenkategorien sind insbesondere dadurch gekennzeichnet, dass bei deren rechtswidriger Verarbeitung die betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann. In diesem Zusammenhang zeigt die Praxiserfahrung, dass betroffene Personen bei bestimmten Krankheiten speziell die sozial stigmatisierende Auswirkung einer unrechtmäßigen Offenlegung ihrer personenbezogenen Patientendaten befürchten.

Vor diesem Hintergrund sind die Anforderungen an zu ergreifende Schutzmaßnahmen bei Patientendaten im Hinblick auf die Risikobewertung (Schadenspotential und Eintrittswahrscheinlichkeit) höher, als bei personenbezogenen Daten, die einem geringeren Schutzbedarf unterliegen.

Abgestimmt auf den Schutzbedarf der Patientendaten sowie auf das damit einhergehende Verarbeitungsrisiko ist ein Datenschutz-Risikomanagement und ggf. eine Datenschutz-Folgenabschätzung (DSFA) für einen oder mehrere ähnliche Verarbeitungsvorgänge durchzuführen.

Die zu ergreifenden notwendigen technischen und organisatorischen Maßnahmen, um die Gewährleistungsziele, wie Verfügbarkeit, Integrität und Vertraulichkeit sicherzustellen, sind gemessen an dem sehr hohen Schutzbedarf der Patientendaten nach deren Geeignetheit, Wirksamkeit und der Möglichkeit zur hinreichenden Reduzierung von Risiken zu beurteilen. Dabei sind bestehende Risiken insbesondere in den Schwachstellen-Bereichen des unerwünschten Datenverlustes, der ungeplanten Verarbeitungsstörung, der unerwünschten Datenänderung sowie des unbefugten Datenzugriffs zu betrachten. Entsprechend zu betrachten sind die relevanten Risiken in den Bereichen der weiteren vier Gewährleistungsziele.

In der im Anhang beigefügten Checkliste können die notwendigen Schritte zur Auslagerung einer Dienstleistung zur eigenen Kontrolle überprüft werden.

3 Externe Dienstleistungen mit Patientenbezug

Im Folgenden sollen typische Dienstleistungen mit Verarbeitungen von Patientendaten dargestellt werden, die bislang nur eingeschränkt mit Hilfe von externen Dienstleistern durchgeführt werden konnten.

Die Liste ist nicht abschließend und wird bei Bedarf ergänzt!

Neue Möglichkeiten zur Auftragsverarbeitung von Patientendaten können demnach bei folgenden Verarbeitungen bestehen:

- Externe Rechenzentren und Serverstandorte
- Patientenportal für ein digitales Aufnahme- und Entlassmanagement
- Externe Wartung und Fernwartung
- Externe Scandienstleister
- Externe Archivierung von Patientendokumenten
- Externe Entsorgung von Patientendokumenten
- Externe Wirtschaftlichkeitsberechnungen, Benchmarking mit Patientendaten

Diese Verarbeitungskonstellationen werden im Folgenden näher erläutert, einschließlich der jeweiligen besonderen datenschutzrechtlichen Aspekte. Dabei ist zu beachten, dass erst durch die wirksame Umsetzung von technischen und organisatorischen Maßnahmen, die in der Regel zuvor im Wege einer datenschutzrechtlichen Risikoanalyse ermittelt wurden, für die jeweils betrachtete Verarbeitung ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Technische und organisatorische Maßnahmen reduzieren Risiken auf ein angemessenes Niveau und sorgen dafür, dass die Gewährleistungsziele dauerhaft erfüllt werden. Im Folgenden werden übergreifende und für alle Konstellationen gleichermaßen in Betracht kommende allgemeine sowie in der jeweiligen Konstellation besonders zu berücksichtigende technische und organisatorische Maßnahmen aufgeführt, die zwar nicht abschließend, aber im jeweils dargestellte Verarbeitungskontext typischerweise risikoreduzierend wirken.

3.1 Allgemeine technische und organisatorische Maßnahmen

Bei jeder Verarbeitungskonstellation, die in dieser Arbeitshilfe behandelt wird, sind insbesondere folgende Anforderungen und Schutzmaßnahmen zu beachten:

- Sorgfältige Auswahlentscheidung: Die Anbieter sind im Hinblick auf ihre technischen und organisatorischen Maßnahmen zum Schutz der Patientendaten vor Abschluss eines AV-Vertrages sorgfältig zu prüfen. Es dürfen nur solche Anbieter gewählt werden, die die Anforderungen an die IT-Sicherheit und den Datenschutz speziell hinsichtlich medizinischer Daten erfüllen können. Die Verantwortlichkeit verbleibt in jedem Fall bei der Klinik!
- Abschluss eines rechtskonformen AV-Vertrages nach Art. 28 DSGVO
- Die Einbeziehung von Unterauftragsverarbeitern ist im AV-Vertrag zu regeln. Änderungen oder zusätzliche Unterauftragsverarbeitungsverhältnisse müssen stets vom Verantwortlichen (Klinik) genehmigt werden. Die effektive Wahrnehmung der Kontrollfunktion und der Weisungsbefugnis des Verantwortlichen erfordert dabei die vorherige Unterrichtung über geplante weitere Unterauftragsverarbeitungsverhältnisse sowie über etwaig vorgesehene Vertragsänderungen.
- Die Einbeziehung von Auftragsverarbeitern und/oder Unterauftragsverarbeitern aus Drittstaaten dürfte überwiegend zu einer Übermittlung personenbezogener Daten in Drittländer führen. Grundsätzlich ist eine Drittstaat-Übermittlung nur zulässig, wenn geeignete Garantien entsprechend Art. 45 ff. DS-GVO bestehen, die ein Datenschutzniveau garantieren, das dem in der europäischen Union entspricht.
- Insbesondere die Übermittlung von medizinischen Daten in Drittstaaten erfordert die Prüfung weiterer effektiver Schutzmaßnahmen. Sofern auch mit zusätzlichen Sicherheitsmaßnahmen (Verschlüsselung, Pseudonymisierung etc.) der Schutz der medizinischen Daten nicht gewährleistet ist, ist eine Datenübermittlung in Drittstaaten zu unterlassen.
- Besondere Probleme stellen sich in der Praxis bei US-amerikanischen Anbietern von Cloud-Diensten (z. B. Amazon Web Services, Microsoft Azure, Google Cloud, etc.). Nach amerikanischem Recht sind diese als sog. Electronic Communications Service Provider im Sinne der Regelungen in 50 U.S. Code § 1881 a („FISA 702“) einzustufen. Unternehmen, die unter diese Regelung fallen, können von US-Behörden zur Datenherausgabe verpflichtet werden. Dies ist deshalb problematisch, weil der Europäische Gerichtshof in seinem Schrems-II-Urteil (C-311/18, Rn. 180, 181) entschieden hat, dass die von FISA 702 den US-Behörden eingeräumten Datenzugangsmöglichkeiten über das nach dem Recht der europäischen Union zulässige Maß hinausgehen. Infolgedessen ist eine Übermittlung personenbezogener Daten an Empfänger, die unter FISA702 fallen, auf Grundlage etwa von Standarddatenschutzklauseln oder anderen Garantien im Sinne des Art. 46 DS-GVO nicht zulässig, wenn auch mit „zusätzlichen Maßnahmen“ ein Zugriff nicht verhindert werden kann.
- Für Vor-Ort-Kontrollen bei Auftragsverarbeitern oder Unterauftragsverarbeitern sind Krankhausbeschäftigten oder -beauftragten der erforderliche Zugang und die

notwendige Unterstützung zu gewähren. Vor-Ort-Kontrollen sind durch die Krankenhäuser bedarfsgerecht durchzuführen.

- Festlegung von Ansprechpartnern für jede Vertragspartei
- Die Prinzipien von Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DS-GVO) und durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) müssen vom Verantwortlichen und somit auch vom Auftragsverarbeiter eingehalten werden. Auftragsverarbeiter müssen daher Voreinstellungen stets datenschutzfreundlich wählen und Wechselwirkungen mit bestehenden Einstellungen transparent machen.
- Das Einbringen von Weiterentwicklungen muss modular erfolgen und, soweit technisch realisierbar, durch die verantwortliche Klinik auch abwählbar sein. Durch Auftragsverarbeiter stillschweigend eingeführte Änderungen können bewirken, dass eine beauftragte Dienstleistung personenbezogene Daten neuen oder geänderten Verarbeitungen unterwirft, bevor die Klinik überhaupt die Möglichkeit hat, dem entgegenzuwirken. Auftragsverarbeiter sollten daher die Weiterentwicklung, Änderung und Abkündigung von Eigenschaften ihrer Dienste in transparent dargelegten und planbaren Zyklen vornehmen, damit sich Kliniken auf die Kontinuität des Betriebs verlassen können. Nur so wird den Kliniken die Möglichkeit gegeben, ihre Maßnahmen und Prozesse zur Datenschutzkonformität, insbesondere zur Gewährleistung der Betroffenenrechte, schritthaltend fortzuentwickeln.
- Die technischen und organisatorischen Maßnahmen, welche die Auftragsverarbeitung absichern, müssen entsprechend dem hohen Sicherheitsniveau für Patientendaten ausführlich dargestellt, risikoorientiert geprüft und nachgewiesen werden sowie den Anforderungen an die Sicherheit der verarbeiteten medizinischen Daten genügen. **Allerdings genügt diese Arbeitshilfe alleine nicht, um dieser Verpflichtung der verantwortlichen Kliniken nachzukommen; sie stellt lediglich eine diesbezügliche Hilfestellung dar.** Im Ergebnis hat bei Hochrisikoverarbeitungen der erforderliche Nachweis des Verantwortlichen in Form einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) zu erfolgen oder in einer geeigneten anderen Form (z.B. in Form einer allgemeinen datenschutzrechtlichen Risikoanalyse).
- Beschäftigte des Auftragsverarbeiters sowie ggf. der Unterauftragsverarbeiter dürfen auf Patientendaten nur im erforderlichen Umfang (Wartungsarbeiten, Administratorentätigkeit, Protokollierungen etc.) Zugriff haben (vgl. Art. 5 Abs. 1 Buchst. c DS-GVO).
- Verpflichtung der relevanten Beschäftigten des Auftragsverarbeiters und gegebenenfalls der Unterauftragsverarbeiter auf das Datengeheimnis (Verschwiegenheitsverpflichtung).
- Bei der Verarbeitung von Gesundheitsdaten für mehrere Einrichtungen muss eine strikte Mandantentrennung erfolgen.
- Sofern die Gesundheitsdaten auf Servern des Auftragsverarbeiters und/oder eines Unterauftragsverarbeiters verarbeitet werden, sollte der betreffende Dienstleister über entsprechende technische Sicherheitszertifikate und -nachweise verfügen.

- Die Möglichkeit geeigneter Schutzmaßnahmen für den unmittelbaren Schutz personenbezogener Daten, wie die Anonymisierung, Pseudonymisierung oder Verschlüsselung, ist stets zu betrachten, in wiederkehrenden Zeitabständen neu zu bewerten und so früh wie möglich umzusetzen.
- Die Ausgestaltung von regelmäßig umzusetzenden Standard-Schutzmaßnahmen ist geeignet zu beschreiben, zu dokumentieren und nachzuweisen. Hierzu gehören insbesondere die Konzeption für das Rollen- und Berechtigungsmanagement, die Authentifizierungsverfahren, das Patchmanagement, das Testen, die Sicherheitsprüfungen, der Malware-Schutz, die Sensibilisierung und Schulung relevanter Personen, die Protokollierung, die Datensicherung (Backup), das Notfallmanagement sowie das Löschen und die Vernichtung relevanter Daten.
- Es sind datenschutzkonforme Vereinbarungen zur Rückgabe, Löschung und Vernichtung der personenbezogenen Daten bei Beendigung der Auftragsverarbeitung zu treffen (vgl. Art. 5 Abs. 1 Buchst. e DS-GVO).

3.2 Externe Rechenzentren und Serverstandorte

Die zunehmende Digitalisierung, Komplexität und der Umfang der digitalen medizinischen Daten bringt es mit sich, dass Kliniken an den Rand ihrer räumlichen, organisatorischen und personellen Kapazitäten gelangen und deshalb auf vielen Ebenen auf die Unterstützung durch externe IT-Dienstleister angewiesen sind.

Ein zentraler Punkt hierbei ist insbesondere der Betrieb des Rechenzentrums und der Server einer Klinik. Cloud-Computing, bei dem IT-Ressourcen je nach Verfügbarkeit überall, -auch außerhalb des EWR-, genutzt werden ist für Auftragsverarbeitungen mit Patientendaten nicht geeignet und hier nicht gemeint.

Neuregelung

Mit der Änderung des Art. 27 BayKrG ist es nunmehr möglich, den Rechenzentrumsbetrieb und den Standort der Server zu einem IT-Dienstleister auszulagern. Sofern die eigenen Kapazitäten nicht mehr ausreichen, ist es künftig nicht mehr zwingend erforderlich, dass der Betreiber des Serverraumes/Rechenzentrums ein Krankenhaus ist bzw. der IT-Dienstleister selbst in den Räumen eines Krankenhauses tätig ist. Die große Bedeutung der Patientendaten für die betroffene Person wie auch für das Krankenhaus und die hohe Sensibilität dieser Daten erfordern aber gerade in diesem Bereich eine besondere, am Erforderlichkeitsmaßstab ausgerichtete Risiko-/Kosten- und Nutzenabwägung zwischen dem Eigenbetrieb und der Auslagerung an einen externen Dienstleister. Überwiegend empfiehlt es sich, nur einzelne Bereiche an IT-Dienstleister auszulagern.

Besondere technische und organisatorische Maßnahmen

Neben den allgemeinen technischen und organisatorischen Maßnahmen (TOM) unter Punkt 3.1 sollten bei dieser Verarbeitung folgende besondere TOM beachtet werden.

- Die Klinik legt alle Anforderungen und die rechtlichen Gründe fest, die es ermöglichen, den Auftragsverarbeiter zu wechseln oder die ausgelagerte Dienstleistung wieder in die eigene IT-Infrastruktur zurückzuholen. Im AV-Vertrag sollten insbesondere konkrete Regelungen festgehalten werden, mit denen sich die notwendige Portabilität gewährleisten lässt.
- Der Auftragsverarbeiter muss seine Dienstleistungen als einzelne, klar voneinander abgrenzbare Verarbeitungsvorgänge möglichst modular anbieten. So können Kliniken durch selektive Vereinbarung, Konfiguration oder Nutzung von Funktionalitäten bedarfsgerecht auf die beauftragten Verarbeitungen einwirken.
- Weitere besondere TOM?

  Diese Liste ist nicht abschießend. Hier können weitere besondere technische und organisatorische Maßnahmen ergänzt werden.

3.3 Patientenportal für ein digitales Aufnahme- und Entlassmanagement

Durch das Krankenhauszukunftsgesetz (KHZG) soll die Digitalisierung der Krankenhäuser vorangetrieben werden. Dazu werden vom Bund und den Ländern Fördergelder für Investitionen bereitgestellt.

Nach § 14a Absatz 2 Satz 1 des Krankenhausfinanzierungsgesetzes (KHZG) und § 19 Krankenhausstrukturfonds-Verordnung (KHSFV) werden eine Reihe von Vorhaben, insbesondere zur Digitalisierung der Prozesse und Strukturen im Verlauf eines Krankenhausaufenthalts von Patientinnen und Patienten, gefördert:

Dazu zählt auch die Einrichtung von Patientenportalen für ein digitales Aufnahme-, Behandlungs- sowie Entlass- und Überleitungsmanagement, die einen digitalen Informationsaustausch zwischen den Leistungserbringern und den Leistungsempfängern sowie zwischen den Leistungserbringern, den Pflege- oder Rehabilitationseinrichtungen und den Kostenträgern vor, während und nach der Behandlung im Krankenhaus ermöglichen.

Neuregelung

Förderfähige Maßnahmen nach dem KHZG müssen auch im Hinblick auf die IT-Sicherheit und den Datenschutz dem hohen Sicherheitsstandard, der für Patientendaten gilt, entsprechen. Die Einbeziehung von externen Dienstleistern, die über das entsprechende technische und organisatorische Know-how verfügen, bei der Entwicklung und zum Betrieb eines Patientenportals, ist mit der Änderung in Art. 27 BayKrG möglich und überwiegend wohl notwendig. Wegen der hohen Sensibilität der zu verarbeitenden Gesundheitsdaten sind die Anforderungen an die Auswahl eines geeigneten Dienstleisters besonders hoch. Idealerweise erfolgt die Festlegung der Anforderungen an die IT-Sicherheit und den Datenschutz bereits bei der Entwicklung des Patientenportals. Diese Anforderungen können schrittweise konkretisiert und individuell an die jeweiligen Erfordernisse des Krankenhauses angepasst werden.

Besondere technische und organisatorische Maßnahmen

Neben den allgemeinen technischen und organisatorischen Maßnahmen (TOM) unter Punkt 3.1 sollten bei dieser Verarbeitung folgende besondere TOM beachtet werden.

- Die ggf. erforderlichen digitalen Einwilligungen der Portalnutzer (Patienten) werden datenschutzkonform verwaltet, insb. auf aktuellem Stand gehalten sowie effektiv und einwilligungskonform genutzt.
- Im Regelfall wird der Betrieb des Portals für 7x24 gewährleistet. Die eingesetzten IT-Systeme und Netzwerkdienste werden laufend überwacht.
- Kliniken steht ein Ticketsystem zur Störungsmeldung zur Verfügung. Hierbei kann der Stand der Entstörung durch den Auftragsverarbeiter grundsätzlich vom Verantwortlichen mitverfolgt werden.

- Im Rahmen der Kontrolle über den Datenfluss muss eine Mandantentrennung erfolgen. Wenn eine physische Trennung nicht umsetzbar ist, müssen andere geeignete technische und organisatorische Maßnahmen implementiert werden. Für einen eventuell notwendigen Datenaustausch zwischen den Mandanten (Leistungserbringern) müssen sichere, regelmäßig verschlüsselte Kommunikationskanäle definiert werden.
- Weitere besondere TOM?

  Diese Liste ist nicht abschießend. Hier können weitere besondere technische und organisatorische Maßnahmen ergänzt werden.

3.4 Externe Wartung, Fernwartung

Die Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, stellt ebenfalls eine Auftragsverarbeitung dar.

Neuregelung

Die Änderung in Art. 27 BayKrG ermöglicht es, externe Dienstleister für die Wartung, Fernwartung von Medizingeräten, Servern etc., bei denen medizinische Daten verarbeitet werden, einzusetzen. Grundsätzlich ist auch bei der externen Wartung bzw. Fernwartung darauf zu achten, dass kein unnötiger Zugriff auf personenbezogene Daten durch Beschäftigte des Dienstleisters möglich ist bzw. die Möglichkeit der Kenntnisnahme zu minimieren ist. Im Hinblick auf die im Vordergrund stehende erforderliche Dienstleistung, d. h. den technischen Betrieb der IT-Systeme zu gewährleisten, ist der Zugriff durch technisches Personal soweit wie möglich zu kontrollieren.

Besondere technische und organisatorische Maßnahmen

Neben den allgemeinen technischen und organisatorischen Maßnahmen (TOM) unter Punkt 3.1 sollten bei dieser Verarbeitung folgende besondere TOM beachtet werden.

- Möglichkeiten zum Fernzugang eines IT-Systems bieten neue Angriffsflächen. Im Umgang mit Dienstleistern, die sich per Fernwartung auf Systeme schalten, sind eingespielte Sicherheitsabläufe im Betrieb besonders wichtig.
- Begrenzung der Fernwartungszugänge nur auf die konkret zu wartenden Systeme, nicht auf das komplette Netzwerk
- Freischaltung der Fernwartungszugriffe nur für den konkreten Zweck und Dauer
- Datenübertragungsmöglichkeiten müssen deaktiviert werden, sofern sie für die Fernwartung nicht erforderlich sind.
- Protokollierung der Fernwartungszugriffe und regelmäßige Kontrolle der Protokolle
- Absicherung der Fernwartungszugänge (z. B. VPN, TLS)
- Sperren des Fernwartungszugriffs nach Beendigung des AV-Vertrages
- Kenntnisnahme von patientenbezogenen Daten soweit möglich vermeiden bzw. auf das notwendige Maß reduzieren (Art. 5 Abs. 1 Buchst. c DS-GVO); soweit möglich, soll nur an Testsystemen gearbeitet werden.
- Weitere besondere TOM?

  Diese Liste ist nicht abschießend. Hier können weitere besondere technische und organisatorische Maßnahmen ergänzt werden.

3.5 Externe Scandienstleister

Um Platz zu sparen und einen schnelleren Zugriff auf Patientendokumente zu haben, werden entweder einzelne papiergebundene Dokumente oder komplette papiergebundene Akten nach Abschluss der Behandlung nachträglich gescannt und/oder zu einer Gesamtdokumentation zusammengefügt. Rechtlich ist hierbei zu beachten, dass gescannte Dokumente generell bei einer gerichtlichen Überprüfung dem richterlichen Augenscheinsbeweis unterliegen, was bedeutet, dass gescannte Dokumente nicht dem Beweiswert eines Originals entsprechen. Der Beweiswert lässt sich jedoch erhöhen, wenn das Scannen nach einem anerkannten zertifizierten Verfahren erfolgt und sichergestellt werden kann, dass Ausgangs- und Enddokumente nicht verändert werden können, bzw. Änderungen sichtbar sind.

Neuregelung

Durch die Änderung in Art. 27 BayKrG sind einige Einschränkungen beim Einsatz externer Dienstleister weggefallen. Damit können Patientenakten auch außerhalb des Krankenhauses, ohne Beteiligung eines Krankenhausmitarbeiters und ohne Verbleib der Schlüsselgewalt beim Krankenhaus, in den Räumen eines externen Dienstleisters gescannt werden. Auch ein zentralisiertes Scannen in den Räumen eines Krankenhauses, das die Scandienstleistung für andere Krankenhäuser als Auftragsverarbeiter mit einem externen Dienstleister als Unterauftragsverarbeiter durchführt, ist nicht mehr zwingend erforderlich. Sofern sich solche Lösungen aber bewährt haben, sollten sie weiterhin fortgeführt werden.

Besondere technische und organisatorische Maßnahmen

Neben den allgemeinen technischen und organisatorischen Maßnahmen (TOM) unter Punkt 3.1 sollten bei dieser Verarbeitung folgende besondere TOM beachtet werden.

- Es ist ein sicherer Transport der papiergebundenen Akten zu gewährleisten; dazu gehört zumindest, die Akten in verschlossenen Behältern zu transportieren.
- Die Behälter sind beim Scandienstleister entsprechend zu verwahren und dürfen nur von den dafür autorisierten Mitarbeitern des Scandienstleisters geöffnet und gescannt werden.
- Die Akten der verschiedenen Krankenhäuser müssen beim Scandienstleister getrennt gehalten und verwahrt werden.
- Weitere besondere TOM?

  Diese Liste ist nicht abschießend. Hier können weitere besondere technische und organisatorische Maßnahmen ergänzt werden.

3.6 Externe Archivierung von Patientendokumenten

Bei behandlungsbezogenen Dokumenten wird – auch über spezialgesetzliche Sonderregelungen (z.B. Röntgenverordnung u.a.) hinaus – teilweise eine Empfehlung für eine 30-jährige Aufbewahrung ausgesprochen. Dies ergibt sich aus Gründen der Beweissicherung, da Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, gemäß § 199 Abs. 2 Bürgerliches Gesetzbuch (BGB) spätestens in 30 Jahren verjähren. An der empfohlenen 30-jährigen Aufbewahrungsdauer für Patientenunterlagen hat sich auch seit Inkrafttreten der DS-GVO nichts geändert. Auch das sog. „Recht auf Löschung“ in Art. 17 DS-GVO steht dieser Empfehlung nicht entgegen, da zur Rechtfertigung der Weiterverarbeitung der Daten auf das Recht zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen bzw. Rechten zurückgegriffen werden kann. In bestimmten Spezialbereichen (wie etwa im Rahmen der Corona-Pandemie aufgrund von Verordnungen oder Vollzugsvorschriften) kann jedoch gleichwohl für einzelne Fallgruppen (bspw. hinsichtlich vorzulegender Testnachweise) eine kürzere Aufbewahrungsfrist gelten, die entsprechend zu beachten ist.

Dauer und Umfang der archivierten Patientenakten erfordert in den Kliniken enorme personelle, räumliche und technische Ressourcen, die i.d.R. in einer Klinik knapp sind.

Neuregelung

Durch die Neuregelung in Art. 27 BayKrG können Patientenakten (Papierakten, digitale Daten) bei externen Dienstleistern gelagert bzw. gespeichert werden, ohne dass die Klinik die Schlüsselgewalt darüber haben muss.

Für **papiergebundene Archive** ist es damit nicht mehr zwingend erforderlich, dass das Papierarchiv auf dem Gelände der Klinik bzw. in angemieteten Räumen durch Personal des Krankenhauses verwaltet werden muss. Auch die permanente Beaufsichtigung von externen Mitarbeitern, die bei Transportdiensten, Einsortieren/Ausgeben von Akten beteiligt sind, durch Personal des Krankenhauses ist nicht mehr zwingend erforderlich.

Zur Verwaltung von **digitalen Archiven**, wie z. B bei digital erstellten Röntgenaufnahmen etc., können mit der Neuregelung auch IT-Dienstleister und Cloudanbieter beauftragt werden, die die Daten – nicht nur verschlüsselt zur Langzeitarchivierung – auf externen Servern verwalten.

Besondere technische und organisatorische Maßnahmen

Neben den allgemeinen technischen und organisatorischen Maßnahmen (TOM) unter Punkt 3.1 sollten bei dieser Verarbeitung folgende besondere TOM beachtet werden.

- Zugriffe sind restriktiv und bezogen auf den Archivzweck zu vergeben.
- Die Lesbarkeit der archivierten Unterlagen ist während der gesamten Archivzeit zu gewährleisten.

- Weitere besondere TOM?

  Diese Liste ist nicht abschießend. Hier können weitere besondere technische und organisatorische Maßnahmen ergänzt werden.

3.7 Externe Entsorgung von Patientendokumenten

Bis zur Neuregelung des Art. 27 BayKrG war der Einsatz von externen Auftragsverarbeitern bei der datenschutzgerechten Entsorgung von patientenbezogenen Unterlagen nur unter engeren Voraussetzungen möglich. Die Entsorgung musste entweder der Dienstleister vor Ort im Krankenhaus durchführen, ggf. unter Aufsicht eines Krankenhausmitarbeiters, oder, sofern dies beim externen Dienstleister erfolgte, musste ein Krankenhausmitarbeiter entweder den Transport begleiten, selber durchführen oder die Entsorgung beaufsichtigen.

Neuregelung

Mit der Neuregelung des Art. 27 Abs. 4 und 6 BayKrG fallen gewisse Beschränkungen seit dem 01.06.2022 weg.

Damit kann der Entsorgungsdienstleister ohne Begleitung und Aufsicht eines Krankenhausmitarbeiters die Entsorgung in seinem Betrieb extern oder vor Ort im Krankenhaus durchführen.

Die Grundsätze für die Verarbeitung von personenbezogenen Daten sind weiterhin einzuhalten, d.h. die Entsorgung muss so stattfinden, dass durch geeignete technische und organisatorische Maßnahmen die Vertraulichkeit der Unterlagen gewahrt bleibt.

➔ Dies gilt für den gesamten Entsorgungsvorgang und seine Vorphasen (Sammlung und Lagerung) und sämtliches Entsorgungsgut.

Entsorgungsgut:

- Patientenakten
- patientenbezogene Papierdokumente außerhalb der Patientenakte (Medikationspläne, Labor- und Untersuchungsanforderungen, patientenbezogene Abrechnungsunterlagen)
- Verbrauchsgüter mit patientenbezogenen Beschriftungen zur medizinischen Behandlung, z. B. Infusionsflaschen etc.
- digitale Datenträger mit patientenbezogenen Daten (Festplatten, DVD, USB-Sticks, Disketten, etc.)

Besondere technische und organisatorische Maßnahmen

Neben den allgemeinen technischen und organisatorischen Maßnahmen (TOM) unter Punkt 3.1 sollten bei dieser Verarbeitung folgende besondere TOM beachtet werden.

- Festlegung von Schutzklassen und Sicherheitsstufen nach DIN 66399 für die Datenträgerentsorgung - Akten mit sensiblen Patientendaten unterfallen der Sicherheitsstufe 4, Schutzklasse 3. Daran haben sich die technischen Maßnahmen zur Vernichtung zu richten.
- Ggf. datenschutzgerechte Vernichtung (Schreddern) bereits vor Ort auf den Stationen

- Festlegungen zur datenschutzgerechten Sammlung und Lagerung von Patientendokumenten (zentral oder dezentral) – Zugangs- und Zugriffsbeschränkungen
- Lagerung in verschlossenen, speziell gekennzeichneten Behältern oder Containern
- Festlegung zum Ort der Entsorgung (vor Ort oder extern)
- Bei externer Entsorgung - Transport in geschlossenen Sicherheitsbehältern, Festlegung des Zeitpunkts der Vernichtung, ggf. Zwischenlagerung, Zugangs- und Zugriffskontrolle beim Entsorger
- Entsorgungsprotokolle durch den Dienstleister
- Mitarbeiterinformation und ggf. Dienstvereinbarung betreffend die korrekte Trennung, Sammlung und Lagerung von Datenträgern
- Weitere besondere TOM?
  Diese Liste ist nicht abschießend. Hier können weitere besondere technische und organisatorische Maßnahmen ergänzt werden.

3.8 Externe Wirtschaftlichkeitsberechnungen, Benchmarking mit Patientendaten

Fallbezogene Daten von voll- und teilstationären Fällen, die im Rahmen des § 21 Krankenhausentgeltgesetzes (KHEntgG) auch an das Institut für das Entgeltsystem im Krankenhaus (InEK) zu übermitteln sind, enthalten Datensätze, die Krankenhäuser auch im Rahmen ihrer eigenen Wirtschaftlichkeitsberechnungen und für eigene Kennzahlen verwenden. Für kurzfristige und langfristige unternehmerische Entscheidungen sind solche aussagekräftigen Auswertungen und Kennzahlen unabdingbar. Externe Dienstleister, die sich auf Wirtschaftlichkeitsberechnungen auf der Grundlage des sog. § 21 KHEntgG - Datensatzes spezialisiert haben, verfügen über das Know-how und über entsprechend aufbereitete Datensätze.

Neuregelung

Bislang war nicht hinreichend geklärt, ob die Verwendung von reduzierten und pseudonymisierten Daten aus dem § 21 KHEntgG - Datensatz durch externe Dienstleister möglich sein konnte. Hintergrund dafür war, dass anonymisierte und pseudonymisierte Daten nicht immer eindeutig voneinander abzugrenzen sind. Zudem haben rein anonymisierte Daten, also rein statistische Daten, nicht immer den erforderlichen Mehrwert für eine Klinik, da sich daraus kaum konkrete klinikspezifische Rückschlüsse ziehen lassen.

Mit der Novelle des Art. 27 BayKrG und der bewährten Vorgehensweise, dass die Anonymisierung oder Pseudonymisierung bereits im Krankenhaus stattfinden und eine Fallrückführung über eine sog. Mappingtabelle weiterhin nur im eigenen Krankenhaus erfolgen kann, dürfte nunmehr der Einsatz eines externen Dienstleisters in diesem Bereich unter bestimmten Voraussetzungen datenschutzkonform möglich sein.

Besondere technische und organisatorische Maßnahmen

Neben den allgemeinen technischen und organisatorischen Maßnahmen (TOM) unter Punkt 3.1 sollten bei dieser Verarbeitung folgende besondere TOM beachtet werden.

Im Vorfeld ist die jeweilige Rolle der an der Verarbeitung beteiligten Akteure zu prüfen. Möglicherweise handelt es sich hierbei nicht immer nur um ein weisungsgebundenes Auftragsverhältnis, sondern um eine gemeinsame Verantwortlichkeit oder eine eigenständige Fachdienstleistung. Danach haben sich dann auch die notwendigen Nachweise und Vereinbarungen zu richten. Sofern es sich um eine Auftragsverarbeitung handelt und ein Vertrag gemäß Art. 28 DSGVO geschlossen werden soll, sind folgende Anforderungen zu beachten.

- Die Vereinbarung hat die zweckgebundene Verarbeitung der Daten für Auswertungszwecke der betreffenden Klinik zu beschreiben.
- Eine zweckfremde Datennutzung durch den Dienstleister muss zwingend auf Daten ohne Personenbezug begrenzt und im Übrigen ausdrücklich untersagt sein.

- Technisch ist die Datenverarbeitung so zu gestalten, dass der Datenzugriff des Dienstleisters erst möglich ist, nachdem die Daten um nicht notwendige Datenparameter bereinigt und pseudonymisiert wurden.
- Der Dienstleister hat die entsprechende Software zur Pseudonymisierung zur Verfügung zu stellen.
- Die Mappingtabelle hat stets beim Krankenhaus zu verbleiben.

- Weitere besondere TOM?
  Diese Liste ist nicht abschießend. Hier können weitere besondere technische und organisatorische Maßnahmen ergänzt werden.

Anhang: Checkliste

1. Planung Auftragsverarbeitung

☐ Welche Verarbeitungsvorgänge sollen ausgelagert werden?

- Beschreibung und Abgrenzung der betroffenen Verarbeitungen
- Beschreibung der von der beabsichtigten Auftragsverarbeitung berührten Verarbeitungstätigkeiten
  (Rechtsgrundlage der Verarbeitung, Kategorien betroffener Personen und deren personenbezogener Daten, Verarbeitung nur im Rahmen bestehender Weisungen des Verantwortlichen usw.)
- Erforderlichkeit und Verhältnismäßigkeit der je Verarbeitungsvorgang grundsätzlich in Frage kommenden Betriebsmittel

☐ Klarheit, welche datenschutzrechtlichen Rollen existieren?
Insbesondere Abgrenzung Verantwortlichkeit, Auftragsverarbeiter sowie ggf. gemeinsame Verantwortlichkeit.

☐ Anforderungen der Informationssicherheit und des Datenschutzes erhoben?

- Nutzung bestehender Standards, Methoden und Good-Practice-Ansätze
- Bei Erforderlichkeit einer Datenschutz-Folgenabschätzung (DSFA): Beginn der DSFA und ablaufgerechte, iterative Konkretisierung
- Berücksichtigung der allgemeinen und ggf. der besonderen technischen und organisatorischen Maßnahmen (aus dieser Arbeitshilfe)

☐ Klarheit, welche Aufgaben die Klinik auch weiterhin selbst (d. h. ohne Inanspruchnahme eines externen Dienstleisters) erfüllen muss?
Die Klinik kann nicht alles aus der Hand geben, weil sie im datenschutzrechtlichen Sinne und bei funktioneller Betrachtung die Verantwortliche bleibt: Es entspricht dem Wesen der Auftragsverarbeitung, dass die Verantwortliche – der die Wahrnehmung ihrer Kernaufgaben selbst vorbehalten bleibt – dem Auftragsverarbeiter Weisungen erteilt und deren Einhaltung kontrolliert.

2. Vergabe Auftragsverarbeitung

☐ Vergabeunterlagen vollständig und hinreichend konkret?

- Nutzung bestehender Muster und Standards (z.B. EVB-IT-Vertragsvorlagen)
- AV-Vertrag (Art. 28 DS-GVO)
- Ggf. für bestimmte Teilbereiche der Verarbeitung eine separate Vereinbarung zur gemeinsamen Verantwortlichkeit (Art. 26 DS-GVO)

- Regelung der Zusammenarbeit der Vertragsparteien für die Erstellung der datenschutzrechtlichen Nachweise (z. B. DSFA-Erstellung aus zwei Teilen)

☐ Bedarfsgerechte Präsentation und ggf. Schaffung einer ergänzenden Beurteilungsbasis für den Erfüllungsgrads bzgl. der gestellten Anforderungen?

3. Durchführung Auftragsverarbeitung

☐ Anpassung der Unterlagen für die Umsetzung der Informationspflichten gemäß Art. 13, 14 DS-GVO?

☐ Unterrichtung des Auftragsverarbeiters über (insb. nach Art. 28 Abs. 3 Unterabs. 1 Buchst. h, Unterabs. 2 und Abs. 4 DSGVO) bestehende Unterstützungs- und Informationspflichten gegenüber der verantwortlichen Klinik insb. mit dem Ziel, die Durchführung von Überprüfungen (einschließlich Inspektionen, ggf. durch vom Verantwortlichen beauftragte Prüfer) zu ermöglichen sowie hinsichtlich der (beabsichtigten) Inanspruchnahme von weiteren Auftragsverarbeitern (Unterauftragsverarbeitung)?

☐ Wahrnehmung der Weisungs- und Kontrollpflichten durch die Klinik?

☐ Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen?

☐ Einhaltung der vereinbarten Regelungen?

☐ Bedarfsgerechte Überprüfung und ggf. Aktualisierung der datenschutzrechtlichen Nachweise?

4. Beendigung Auftragsverarbeitung

☐ Rückgabe, Löschung und/oder Vernichtung der personenbezogenen Daten, die im Rahmen der Beauftragung vom Auftragsverarbeiter und ggf. von dessen Unterauftragsverarbeiter verarbeitet wurden?

4 Ergänzende Literatur

Zur weiteren Prüfung der Auswahl eines Dienstleisters empfehlen sich als weitere Hilfestellungen folgende Veröffentlichungen.

Aktuelle Kurz-Information 43: Auftragsverarbeitung bei bayerischen öffentlichen Krankenhäusern, Stand: 1. Juni 2022, Link: https://www.datenschutz-bayern.de/datenschutzreform2018/aki43.html)

Checkliste des Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) und des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) zu Cybersicherheit für medizinische Einrichtungen, Checkliste mit Prüfkriterien nach Art. 32 DS-GVO, Stand: 22. Juli 2020, Link: Cybersicherheit für medizinische Einrichtungen (bayern.de)

Checkliste des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) zu Good Practice bei technischen und organisatorischen Maßnahmen, Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit, Stand: 13. Oktober 2020, Link: Checkliste Technische und organisatorische Maßnahmen (bayern.de)

Orientierungshilfe „Auftragsverarbeitung“ des Bayerischen Landesbeauftragten für den Datenschutz, Stand 1. April 2019, Link: Orientierungshilfe Auftragsverarbeitung (datenschutz-bayern.de)

Leitfaden zum Outsourcing kommunaler Informationstechnologie, Veröffentlichung des Bayerischen Landesbeauftragte für den Datenschutz, 29.03.2021, Link: outsourcing.pdf (datenschutz-bayern.de)

Literatur zur Datenschutzfolgeabschätzung des bayerischen Landesbeauftragten für den Datenschutz, unter folgendem Link: BayLfD: Datenschutz-Folgenabschätzung (DSFA) (datenschutz-bayern.de)

Maßnahmenkatalog zur Verbesserung der IT-Sicherheit in bayerischen Krankenhäusern, Ausgabe 2020/2021, Universität der Bundeswehr München, Link: ausgabe2020-2021-epdf-1.pdf (unibw.de)

IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit, Bundesamt für Sicherheit in der Informationstechnik (BSI), Link: BSI - IT-Grundschutz-Kompendium (bund.de)