

8 Datenverarbeitung im Auftrag für Zwecke der Forschung oder Qualitätssicherung



Unter welchen rechtlichen Bedingungen können die im Rahmen der Behandlung dokumentierten Daten in pseudonymisierter Form im Rahmen einer Datenverarbeitung im Auftrag für Zwecke der Forschung oder Qualitätssicherung übermittelt werden, wenn die behandelnde Einrichtung Auftraggeber ist und

- *der Auftragnehmer seinen Sitz in Deutschland hat?*
- *der Auftragnehmer seinen Sitz im EU-Ausland hat?*

8.1 Allgemeine Einordnung der Auftragsdatenverarbeitung im Kontext der Sekundärnutzung

8.1.1 Zulässigkeit der Forschung oder Qualitätssicherung durch die Behandlungseinrichtung

Die Einschaltung eines Auftragsdatenverarbeiters ändert nichts an der Verantwortung der behandelnden Einrichtung für die Zulässigkeit der Verarbeitung personenbezogener Daten. Das gilt auch für eine Auftragsdatenverarbeitung für Zwecke der Forschung oder Qualitätssicherung. Die Behandlungseinrichtung muss gewährleisten, dass die grundsätzlichen Zulässigkeitsvoraussetzungen, wie sie beim Datenumgang zu den genannten Zwecken ausschließlich im eigenen Haus gelten, auch bei

der Einschaltung von Auftragnehmer vorliegen. Insoweit kann auf die Antworten zu den vorigen Fragen verwiesen werden. Die rechtlichen Bedingungen für die Einschaltung eines Auftragnehmers müssen zusätzlich erfüllt werden. Auf diese wird im Folgenden eingegangen.

8.1.2 Personenbezug für den Auftragnehmer?

Ein besonderer Rechtfertigungsbedarf für die Einschaltung eines Auftragnehmers besteht im vorliegenden Kontext von Datenschutz und Schweigepflicht jedoch nur dann, wenn dieser die ihm übertragenen Daten einer Person, insbesondere einem Patienten, zuordnen kann.⁷⁶⁷ Nach der Fragestellung sollen vorliegend die im Rahmen der Behandlung dokumentierten Daten jedoch lediglich in pseudonymisierter Form an den Auftragnehmer übertragen werden. Hier wird davon ausgegangen, dass die Pseudonymisierung noch in der Behandlungseinrichtung erfolgt und der Auftragnehmer im Gegensatz zu dieser nicht über die Zuordnung des Pseudonyms zum Patienten verfügt, gleich ob diese Zuordnung über eine Einwegfunktion (Hashwerte) oder listenmäßig über einen zufällig gewählten Referenzwert erfolgt.⁷⁶⁸

Wenn man den absoluten Ansatz des Personenbezugs in subjektiver (stellenbezogener) Hinsicht vertreten würde, es also genügen lässt, wenn nur eine Stelle den Personenbezug eines Datums herstellen kann, um auch für alle anderen Stellen eine solchen anzunehmen, dann läge auch hier gleichwohl eine weiter rechtlich zu legitimierende Übertragung personenbezogener Daten an den Auftragnehmer vor. Wenn man jedoch, wie vorliegend in der Antwort zu Frage 1 des Gutachtens in Kapitel I.2, von der Relativität des Personenbezugs ausgeht, muss dies keineswegs der Fall sein. Nach der hier vertretenen Auffassung kommt es auf die Möglichkeiten zur Herstellung des Personenbezugs durch die jeweils zu betrachtende Stelle an.

Aufgrund der Pseudonymisierung sind vorliegend die an den Auftragnehmer übertragenen Daten für diesen nicht direkt einer bestimmten Person zugeordnet. Fraglich ist allerdings, ob die Daten trotz Pseudonymisierung für ihn noch bestimmbar sind oder ob sie sich überhaupt nicht mehr oder jedenfalls nicht mehr mit verhältnismäßigem Aufwand einer natürlichen Person, hier dem Patienten, zuordnen lassen.

Vertritt man insoweit, also in objektiver (mittelbezogener) Hinsicht, einen absoluten Ansatz, dann dürften die Daten für den Auftragnehmer überhaupt nicht mehr einer Person zuzuordnen sein, wenn ein Personenbezug für diesen ausgeschlossen werden soll. Der Zugriff auf die Zuordnung bei der Behandlungseinrichtung ist dabei allerdings nicht in Betracht zu ziehen, soweit dieser nicht vorgesehen ist und hinreichende faktische Hürden (wie getrennte IT-Systeme mit getrennten Zugriffsrechten) bestehen, denn ansonsten würde man wieder zum absoluten Ansatz in subjektiver Hinsicht gelangen.

⁷⁶⁷ Zum Datenschutz für die u.U. ebenfalls betroffenen Beschäftigten einer Behandlungseinrichtung s.u. Kap. I.15, S. 321ff.

⁷⁶⁸ Zu den verschiedenen Formen der Pseudonymisierung s. LfD Bayern, Orientierungshilfe: Pseudonymisierung in der medizinischen Forschung, Stand 29.11.2005, abrufbar unter www.datenschutz-bayern.de; s.a. U. Schneider, in: Krauskopf, SGB V, § 299 Rdnr. 12ff.

Da bei bloßer Pseudonymisierung jedoch der Fallbezug der Datensätze erhalten bleibt, wird man jedenfalls bei Datensätzen, die komplex genug sind, eine Re-Identifizierung beispielsweise durch Mustervergleich mit anderen Quellen je nach Zusatzwissen der außenstehenden Stelle (wie des Auftragnehmers) dennoch kaum vollständig ausschließen können. Insofern führt eine Pseudonymisierung für diejenigen Stellen, die nicht im Besitz der Zuordnungsvorschrift sind, in der Regel nicht zu einer absoluten, sondern nur zu einer relativen (faktischen) Anonymisierung, bei welcher die Zuordnung lediglich nicht mehr mit verhältnismäßigem Aufwand herzustellen ist. Überträgt man den relativen Ansatz allerdings von der Referenzstelle auf die in Betracht zu ziehenden objektiven Referenzmittel der Re-Identifizierung, dann genügt auch deren Unverhältnismäßigkeit, um den Personenbezug auszuschließen. Dieser durchweg relative Ansatz wurde zu Beginn des Gutachtens angenommen, wenn auch verbunden mit Empfehlungen zur Risikoversorge, die gewährleisten sollen, dass sich das verbleibende Re-Identifizierungsrisiko möglichst nicht realisiert.⁷⁶⁹ Unter diesem Gesichtspunkt ist zunächst sicherzustellen, dass sich durch

- die Art der Erstellung der Pseudonyme,
- den Umfang des Datenumgangs mit den Pseudonymen und
- den Umfang der zum Pseudonym gespeicherten Daten

keine unverhältnismäßigen Re-Identifizierungsrisiken für die betroffenen Patienten ergeben, wobei insbesondere zu berücksichtigen ist, über welches Zusatzwissen der Datenempfänger in der Regel verfügt.⁷⁷⁰ Wenn dies gewährleistet ist, dann müssen die pseudonymen Daten beim Empfänger nicht als personenbezogen betrachtet werden.⁷⁷¹ Vorliegend dürften im Übrigen jedenfalls auch vertragliche Vereinbarungen mit Re-Identifizierungsverboten für den Auftragnehmer samt gewisser Kontrollmöglichkeiten für den Auftraggeber angezeigt sein, welche nicht vollständig den Vorschriften über die Auftragsdatenverarbeitung entsprechen müssen, sich aber an diesen orientieren sollten.

Nimmt man hingegen an, dass der Personenbezug nur durch eine absolute Anonymisierung ausgeschlossen wird, so dürfte dieser auch nach Pseudonymisierung selbst für Außenstehende ohne Zugriff auf die Zuordnungsfunktion noch vorliegen.⁷⁷² Dies hätte zur Folge, dass dann die Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag vollständig angewandt werden müssten.

Vor diesem Hintergrund sollen trotz Pseudonymisierung die jeweils einschlägigen Vorschriften über die Auftragsdatenverarbeitung kurz dargestellt werden, um zumindest Orientierungspunkte für die Ausgestaltung entsprechender Rechtsbeziehungen zwischen Behandlungseinrichtung und Auftragnehmer zu erhalten.

769 S. oben S. 12ff. (Antwort auf Frage 1 des Pflichtenheftes).

770 LfD Hessen, 29. Tätigkeitsbericht 2000, Abschnitt 9.2.3.5 (Stellungnahme zum Kompetenznetz Parkinson).

771 So auch der LfD Hessen, 30. Tätigkeitsbericht 2001, Abschnitt 26.6, zum Kompetenznetz Parkinson bezüglich langfristig pseudonymisierten Patientendaten; s.a. soeben Fn. 770.

772 So z.B. Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 152ff., für verschlüsselte Daten, da die Entschlüsselung angesichts der Möglichkeiten der Kryptoanalyse und steigender Rechnerkapazitäten nie gänzlich ausgeschlossen werden kann; dies gelte jedenfalls für Patientendaten mit ihrer hohen Sensibilität. Als Zusatzargument ließe sich hierfür anführen, dass Gesundheitsdaten eine lange „Wertigkeit“ haben können, also auch nach Jahren nicht unbedingt an Aussagekraft verlieren, so z.B. bei chronischen Krankheiten, vgl. Schneider, Datenschutz in der vernetzten Medizin, in Grätzel von Grätz (Hg.), Vernetzte Medizin, S. 136, 148.

8.1.3 Offenbaren im Sinne der Schweigepflicht (§ 203 StGB)

Soweit beim Auftragnehmer ein Personenbezug gegeben ist, liegt nach herrschender Meinung bei grundsätzlich geheimzuhaltenden Patientendaten auch ein Offenbaren an diesen durch die Behandlungseinrichtung im Sinne der nach § 203 Abs. 1 Nr. 1 StGB sanktionierten Schweigepflicht vor.⁷⁷³ Sind die Behandlungsdaten beim Auftragnehmer noch einer bestimmten natürlichen Person, also direkt einem Patienten zugeordnet, ist diese Ansicht unumstritten. Eine solche Situation liegt vorliegend jedoch aufgrund der vorgegebenen Pseudonymisierung nicht vor. Diese Daten könnten allenfalls noch mittelbar einem (dann lediglich bestimmbar) Patienten zugeordnet werden, was jedenfalls für die Anhänger eines durchgehend absoluten Ansatzes des Personenbezugs ausreicht. Die Befürworter einer rein relativen Sichtweise des Personenbezugs, die sowohl in subjektiver als auch in objektiver Hinsicht hier vertreten wird, müssen hingegen mit der personenbezogenen Datenweitergabe auch ein Offenbaren ablehnen.⁷⁷⁴

Von Anhängern einer Auffassung des Personenbezugs, der zwar in subjektiver Hinsicht relativ ist, also von den Möglichkeiten der jeweils betrachteten Stelle abhängt, in objektiver Hinsicht aber absolut, also die bloße Möglichkeit der Re-Identifizierung genügen lässt, auch wenn diese mit unverhältnismäßigem Aufwand verbunden sein mag, wird im Hinblick auf das Offenbaren nach § 203 StGB allerdings teils eine vom Datenschutzrecht abweichende Lösung vertreten. Trotz des insoweit angenommenen Personenbezugs im Sinne des Datenschutzrechts und des entsprechenden Rechtfertigungsbedarfs gerade bei der Datenübertragung an eine andere Stelle, sei es als Datenübermittlung oder Auftragsdatenverarbeitung, wird hier ein Offenbaren im Sinne der Schweigepflicht auch bei bloß relativ anonymisierten Daten verneint. Solche Daten liegen bei effektiver Pseudonymisierung vor, bei der Außenstehende regelmäßig keinen Zugriff auf die Pseudonymzuordnung haben. Namentlich *Hermeler* begründet dies, wenn auch für die – allerdings vergleichbare – hochwertige Verschlüsselung, unter anderem mit dem strafrechtlichen Bestimmtheitsgebot und der daraus folgenden Notwendigkeit, Strafvorschriften restriktiv auszulegen, wohingegen die Datenschutzvorschriften ihrem Schutzzweck entsprechend extensiv auszulegen seien.⁷⁷⁵ Für die restriktivere Auslegung spricht auch der Wortlaut der in § 203 StGB vorausgesetzten Tathandlung, nämlich des „Offenbarens“, das eine gewisse Offenkundigkeit des Personenbezugs nahelegt, selbst wenn man insoweit nicht die tatsächliche Kenntnisnahme fordert, sondern auf die bloße (aber offenkundige) Möglichkeit der Kenntnisnahme abstellt.⁷⁷⁶ In diesem Fall könnte trotz datenschutzrechtlichem Personenbezug und dementsprechendem Rechtfertigungsbedarf kein Offenbaren eines Patien-

773 Alkemade u.a., Der Gehilfe des Arztes, S. 10f. m.w.N. Zwar ist nicht jedes personenbezogene Datum ein Geheimnis im Sinne von § 203 StGB. Allerdings sind Patientendaten regelmäßig nicht offenkundig und damit geheim zu halten. Und das geschützte Geheimnis hat eine andere Person zu betreffen (vgl. Fischer, StGB, § 203 Rdnr. 3ff.), diese muss also bestimmt oder zumindest bestimmbar sein.

774 So auch Alkemade u.a., Der Gehilfe des Arztes, S. 11, wenn „die Daten vor ihrer Bearbeitung durch externe Mitarbeiter durch den Geheimnisträger oder dessen Gehilfen anonymisiert oder pseudonymisiert werden“.

775 Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 136ff. (zu § 203 StGB), S. 152ff. (allgemein zu Verschlüsselung und Personenbezug), S. 181ff. (zum Datenschutz im engeren Sinne, wo sie auf S. 183 explizit von extensiver Auslegung des § 11 BDSG im Hinblick auf die Kenntnisnahmemöglichkeiten des Auftragnehmers von personenbezogenen Daten spricht).

776 Zu den unterschiedlichen Rechtsmeinungen zum Erfordernis tatsächlicher Kenntnisnahme bzw. der reinen Möglichkeit hierzu s. oben S. 48ff. Die Pseudonymisierung kann für Dritte, welche die Zuordnungsvorschrift nicht kennen, zudem u.U. die Herstellung des Personenbezugs nicht nur erschweren, sondern ausschließen, so dass insoweit dann keine Möglichkeit der Kenntnisnahme mehr besteht.

tengeheimnisses vorliegen und folglich auch keine Befugnis nach § 203 StGB nötig sein.

Im Folgenden soll jedoch – auch wenn dies nach hier vertretener Auffassung eigentlich nicht nötig wäre – zur weiteren Aufklärung und Absicherung die restriktivste Auffassung weiter verfolgt werden, nach welcher trotz Pseudonymisierung sowohl eine Übertragung personenbezogener Daten im Wege der Auftragsdatenverarbeitung vorliegt als auch ein Offenbaren von Patientengeheimnissen nach § 203 StGB. In diesem Fall ist nach der sogenannten Zwei-Schranken-Theorie neben einer datenschutzrechtlichen Erlaubnis auch eine gesondert zu prüfende Befugnis im Sinne des § 203 StGB für die Rechtmäßigkeit der Datenübertragung erforderlich.⁷⁷⁷ Dabei ist nicht jede datenschutzrechtliche Erlaubnisnorm eine gesetzliche Befugnis zum Offenbaren von Patientendaten. Um den besonderen Schutz, den § 203 StGB bezweckt, nicht zu umgehen, können nur Vorschriften, die den Kontext der Arzt-Patienten-Beziehung einbeziehen, eine solche Befugnis darstellen.

Dies führt dazu, dass allgemeine Regelungen zur Auftragsdatenverarbeitung, wie sie in § 11 BDSG oder den LDSG enthalten sind, keine Befugnis nach § 203 StGB darstellen.⁷⁷⁸ Zwar unterliegen auch berufsmäßig tätige Gehilfen der behandelnden Ärzte gemäß § 203 Abs. 3 S. 2 StGB der Schweigepflicht und sind innerhalb einer Einrichtung zur Mitarbeit und damit zum Mitwissen befugt, weshalb insoweit kein unbefugtes Offenbaren vorliegt.⁷⁷⁹ Hierzu zählt auch internes IT-Personal. Allerdings können externe Stellen und damit IT-Dienstleister nach wohl noch herrschender Meinung nicht als solche Gehilfen eingestuft werden.⁷⁸⁰

Als Offenbarungsbefugnis im Sinne von § 203 StGB kommen damit neben der Einwilligung⁷⁸¹ gesetzliche Regelungen in Betracht, die sich auf die Offenbarung fremder Geheimnisse, vorliegend also von Patientengeheimnissen, erstrecken.⁷⁸² In einigen Bundesländern existieren spezielle gesetzliche Regelungen zur Auftragsdatenverarbeitung für Krankenhäuser; diese können dann auch als Befugnis im Sinne von

777 BGH, Urt. v. 11.12.1991 – VIII ZR 4/91, BGHZ 116, 268, = NJW 1992, 737, Rdnr. 26–28; Dix, in: Simitis (Hg.), BDSG, § 1 Rdnr. 175ff., 186f.; Cierniak, in: Joeks/Miebach (Hg.), Münchner Kommentar, StGB, § 203 Rdnr. 51; Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 84ff. Nur einen von mehreren normativen Ansätzen stellt dabei § 1 Abs. 3 S. 2 BDSG dar. Eine sehr ausführliche dogmatische Begründung liefert Beyerle, Rechtsfragen medizinischer Qualitätskontrolle, S. 121ff.

778 Petri, in: Simitis (Hg.), BDSG, § 11 Rdnr. 44f.; Alkemade u.a., Der Gehilfe des Arztes, S. 11.

779 Fischer, StGB, § 203 Rdnr. 10.

780 Fischer, StGB, § 203 Rdnr. 10 m.w.N. Diese Konsequenz der Zwei-Schranken-Theorie des deutschen Rechts dürfte europarechtskonform sein, denn im Rahmen von Art. 8 Abs. 3 Datenschutzrichtlinie 95/46/EG können die Mitgliedstaaten auch über die Ausgestaltung von über das allgemeine Datenschutzniveau hinausgehenden Geheimhaltungspflichten für Gesundheitsdaten entscheiden. Auch EuGH, Urt. v. 22.11.2012 – C-119/12 (Probst), CR 2013, 25, ändert diese Einschätzung nicht, denn dieses bezieht sich nur darauf, dass das TK-Geheimnis nach Art. 6 Abs. 2, 5 E-Kommunikations-Datenschutzrichtlinie 2002/58/EG bei weisungskonformer Auftragsverarbeitung eingehalten werden kann und nicht auf die weiteren Spielräume der Mitgliedstaaten nach Art. 8 Datenschutzrichtlinie 95/46/EG (s. dazu oben S. 16). Kritisch dagegen Alkemade u.a., Der Gehilfe des Arztes, S. 11ff., auch vor europarechtlichem Hintergrund, S. 18f. Bereits nach geltendem deutschen Recht eine Gehilfenstellung annehmend: Heghmanns/Niehaus, NStZ 2008, 57, 61f. Für die herrschende Meinung spricht aber zudem, dass der Gesetzgeber 2006, als die Rechtsprobleme beim Outsourcing im Gesundheitswesen bereits allgemein bekannt waren, für den externen Datenschutzbeauftragten in § 203 Abs. 2a StGB eine Sonderregelung eingeführt hat, welche die Strafbarkeit auf diesen erstreckt, woraus in diesem Zusammenhang gefolgert wird, dass Mitteilungen an den für die jeweilige Stelle bestellten Datenschutzbeauftragten kein unbefugtes Offenbaren darstellt (s.a. § 4f Abs. 2 S. 3 Hs. 2 BDSG). Auf IT-Dienstleister wurde diese Ausnahme allerdings nicht ausgedehnt, wobei zuzugeben ist, dass diese, soweit sie weisungsgebunden sind, eher unter den Gehilfenbegriff fallen könnten als ein per Gesetz weisungsfreier Datenschutzbeauftragter (vgl. § 4f Abs. 3 S. 2 BDSG).

781 Fischer, StGB, § 203 Rdnr. 32ff., wobei insoweit geringere Formerfordernisse als nach Datenschutzrecht gelten. Die mutmaßliche Einwilligung dürfte in vorliegendem Kontext jedenfalls bei einwilligungsfähigen Patienten als Rechtfertigungsgrund ausscheiden (auch Fischer, a.a.O., Rdnr. 36, bezeichnet den Anwendungsbereich als „schmal“).

782 Fischer, StGB, § 203 Rdnr. 37ff.

§ 203 StGB angesehen werden.⁷⁸³ Diese Spezialvorschriften der Landeskrankenhaus- oder entsprechender Gesetze, die in aller Regel die Auftragsdatenverarbeitung an zusätzliche Bedingungen knüpfen, sind allerdings auch zu beachten, wenn man zwar von keinem Offenbaren, wohl aber von einer personenbezogenen Datenübertragung ausgeht. Auf sie soll im nachfolgenden Kapitel I.8.2 weiter eingegangen werden.⁷⁸⁴

8.1.4 Allgemeine Charakteristika der Auftragsdatenverarbeitung

8.1.4.1 Datenübertragung an Auftragnehmer innerhalb des EWR: kein Übermitteln

Auch bei Annahme eines Personenbezugs liegt allerdings bei Weitergabe der Daten an einen Auftragnehmer nicht zwingend ein besonders rechtfertigungsbedürftiges Übermitteln vor. Denn ein Übermitteln ist nach Datenschutzrecht lediglich die Weitergabe an einen Dritten außerhalb der ursprünglich verantwortlichen Stelle (prototypisch im deutschen Recht: § 3 Abs. 4 S. 2 Nr. 3 BDSG). Als Dritter gilt jedoch nicht der Auftragsdatenverarbeiter, dessen Sitz innerhalb des Europäischen Wirtschaftsraums (EU und EFTA) liegt (§ 3 Abs. 8 S. 3 BDSG).⁷⁸⁵

Die Untergliederung der Fragestellung nach Sitz in Deutschland oder im EU-Ausland erweist sich damit jedenfalls im Anwendungsbereich des BDSG (u.a. für private Arztpraxen und Kliniken des Bundes) als nicht relevant. Aufgrund der Datenschutzrichtlinie 95/46/EG und des europäischen Binnenmarktes für personenbezogene Daten gilt dies prinzipiell auch für sonstige Behandlungseinrichtungen. Selbst im Bereich der öffentlichen und kirchlichen Kliniken dürften keine Ausnahmeregelungen greifen, denn diese sind üblicherweise in gewissem Wettbewerb zu privaten Kliniken tätig und auch dieser Wirtschaftszweig fällt grundsätzlich in den Anwendungsbereich des Gemeinschafts- bzw. Unionsrechts und damit auch in den der Datenschutzrichtlinie 95/46/EG (vgl. Art. 3 Abs. 2 der Richtlinie), aus welcher insoweit eine grundsätzliche Gleichbehandlungspflicht folgt.⁷⁸⁶

In datenschutz-, rechts- bzw. geschäftspolitischer Hinsicht wäre angesichts der weitgehend nicht harmonisierten Datenzugriffsrechte der Sicherheitsbehörden, die in manchen Ländern der Europäischen Union deutlich extensiver genutzt werden als in anderen, unter Umständen allerdings eine Beschränkung der Auftragsdatenverarbeitung beispielsweise auf die EWR-Vertragsstaaten im Schengen-Raum erwägenswert.⁷⁸⁷

⁷⁸³ Alkemade u.a., Der Gehilfe des Arztes, S. 17, 8ff.

⁷⁸⁴ S. sogleich S. 266ff.

⁷⁸⁵ Prototypisch für das deutsche Recht: § 3 Abs. 8 S. 3 BDSG. S.a. Art. 2 Buchst. f (Auftragsverarbeiter kein Dritter), Art. 25ff. (Sonderregeln für Drittlandübermittlungen) und Erwägungsgrund 60 der Datenschutzrichtlinie 95/46/EG.

⁷⁸⁶ Zur Anwendung der Datenschutzrichtlinie 95/46/EG auf kirchliche Einrichtungen, in diesem Fall sogar unabhängig von wirtschaftlicher Betätigung: EuGH, Ur. v. 06.11.2003 – C-101/01 (Lindqvist), Slg. 2003, I-12971 = RDV 2004, 16.

⁷⁸⁷ Der Schengen-Raum bezieht sich auf die verstärkte Zusammenarbeit vieler EU-Mitglieder (und EWR-Vertragsstaaten) als einem Pfeiler eines „Raums der Freiheit, der Sicherheit und des Rechts“. Vor allem das Vereinigte Königreich und Irland wirken hieran nur sehr begrenzt mit und werden daher nicht zum sogenannten Schengen-Raum gezählt. Zur Idee eines „Schengen-Netzes“ angesichts der massiven Ausspähung der Datenkommunikation durch Geheimdienste wie die NSA der USA oder den britischen GCHQ vgl. u.a. o.V., Brüssel unterstützt Merks Vorstoß für „Schengen-Netz“, heise news, 17.02.2014.

8.1.4.2 Externe Dienstleistung als Auftragsdatenverarbeitung, nicht Funktionsübertragung

Bei der Auftragsdatenverarbeitung bleibt die Verantwortung für den Umgang mit personenbezogenen Daten beim (Haupt-)Auftraggeber als verantwortlicher Stelle. Der Auftraggeber kann dieser Verantwortung nur gerecht werden, wenn er Zweck und wesentliche Mittel des Datenumgangs bestimmt.⁷⁸⁸ Der Auftragnehmer darf als Auftragsdatenverarbeiter also lediglich ausführende, insbesondere EDV-technische Hilfstätigkeiten übernehmen und dabei Entscheidungen von untergeordneter Bedeutung über die Einzelheiten des Mitteleinsatzes (wie z.B. die konkrete Soft- und Hardware) treffen. Ein größerer Entscheidungsspielraum darf ihm nicht zukommen, ansonsten läge eine sogenannte Funktionsübertragung vor, die wiederum als besonders rechtfertigungsbedürftige Übermittlung und nicht mehr als bloße Auftragsdatenverarbeitung einzustufen ist.

Diese grundlegenden Anforderungen, die erfüllt sein müssen, um überhaupt von Auftragsdatenverarbeitung ausgehen zu können, können jedoch bei der vorliegend insbesondere zu betrachtenden Datenverarbeitung in der Cloud grundsätzlich eingehalten werden. Die Behandlungseinrichtung muss mit dem Zweck des Einsatzes für Forschung oder Qualitätssicherung allerdings der Datenverarbeitung eine gewisse Struktur vorgeben, damit sich auch die Ergebnisse der Datenverarbeitung in diesem Zweckrahmen bewegen. Auch sind die Grenzen der Cloud so zu bestimmen, dass die Privilegierung der Auftragsdatenverarbeitung (keine besonders rechtfertigungsbedürftige Übermittlung) innerhalb des EWR nicht verspielt wird. Dafür sollten die Rechenzentrumsstandorte, auf deren Ressourcen grundsätzlich zurückgegriffen werden kann, bekannt sein und benannt werden.

Das entsprechende Bestimmungsrecht des Auftraggebers schließt nicht aus, dass der Cloud-Anbieter bzw. der Auftragnehmer hier standardisierte Vertragsbedingungen vorgibt.⁷⁸⁹ Diese müssen allerdings konkrete und verbindliche Aussagen zu den genannten Punkten enthalten, so dass die Behandlungseinrichtung in Kenntnis aller relevanten Umstände eine freie Entscheidung über den Abschluss eines entsprechenden Vertrages treffen kann.⁷⁹⁰ Auch sind Mechanismen vorzusehen, die es den verantwortlichen Behandlungseinrichtungen ermöglichen, die Einhaltung der genannten Bedingungen faktisch zu kontrollieren,⁷⁹¹ was gegebenenfalls auch durch eine gemeinsame Auditierung des Anbieters sichergestellt werden kann.

8.1.5 Fehlender Personenbezug: Entbehrlichkeit einer besonderen Erlaubnis, Sinnhaftigkeit vertraglicher Absicherungen

Wenn man der vorliegend vertretenen Auffassung folgt, dass durch effektive Pseudonymisierung innerhalb der Behandlungseinrichtung der Personenbezug für den

⁷⁸⁸ Basierend auf Art. 2 Buchst. d Datenschutzrichtlinie 95/46/EG grundlegend hierzu: Art. 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, Working Paper 169, 264/10/DE.

⁷⁸⁹ Kritisch dagegen das ULD Schleswig-Holstein in seiner Verbotsverfügung gegenüber dem Hausärzterverband bezüglich der standardisiert vorgegebenen Rechenzentrumsleistungen für die Abrechnung von Verträgen über die hausarztzentrierte Versorgung, Anordnung vom 21.07.2010, insbes. Abschnitte 5.1 und 6.

⁷⁹⁰ U. Schneider, in Krauskopf, SGB V, § 295 Rdnr. 25dff.

⁷⁹¹ Prototypisch für das deutsche Recht § 11 Abs. 2 S. 4 BDSG; im Grundsatz ist dies nach Art. 17 Abs. 2 Hs. 2 Datenschutzrichtlinie 95/46/EG zwingend: „der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung der Maßnahmen“.

Auftragnehmer ausgeschlossen wird, dann sind sowohl datenschutzrechtliche Erlaubnis als auch Schweigepflicht-bezogene Befugnis entbehrlich, gleich ob sich Erlaubnis und Befugnis allein auf das Gesetz oder auf eine Willenserklärung des Betroffenen, also eine datenschutzrechtliche Einwilligung oder eine Schweigepflichtentbindung, stützen.

Einwilligung und Schweigepflichtentbindung wären aber im Rahmen der bereits dargestellten allgemeinen und teils auch länderspezifischen Bedingungen zur Absicherung zulässig.

Soweit man zwar noch einen Personenbezug im Sinne des Datenschutzrechts annimmt, aber ein Offenbaren im Sinne der Schweigepflicht ablehnt, sind Einwilligung und Schweigepflichtentbindung grundsätzlich ebenfalls entbehrlich. Bei der Schweigepflichtentbindung gilt dies dann ohne jede weitere Bedingung, denn mangels Offenbaren läge schon kein – ggf. durch eine Entbindungserklärung des Patienten – zu rechtfertigender Bruch der Schweigepflicht vor; insoweit wäre dann auch keine gesundheitsspezifische gesetzliche Befugnis erforderlich. Gleiches würde gelten, wenn man zwar ein Offenbaren annimmt, aber eine Schweigepflichtenbindung einholt.⁷⁹²

Eine rechtfertigungsbedürftige Datenweitergabe (technische Übertragung) im Sinne des Datenschutzrechts läge unter den Annahmen aus dem vorigen Absatz aber gleichwohl vor. Soweit eine rechtmäßige Auftragsdatenverarbeitung und damit keine Übermittlung vorliegt, muss aber auch dieser Vorgang nicht gesondert über einen gesetzlichen Erlaubnistatbestand oder eine Einwilligung gerechtfertigt werden. Denn auch die Vorschriften über die Auftragsdatenverarbeitung entfalten bei deren Beachtung insoweit Rechtfertigungswirkung und schließen bei einem Auftragnehmer im EWR eine Übermittlung aus. Auch müssten die gesetzlichen Grundlagen der Auftragsdatenverarbeitung nicht spezifisch das Arzt-Patienten-Verhältnis einbeziehen, wenn man kein Offenbaren im Sinne der Schweigepflicht annähme. Damit könnte auch die allgemeine Norm zur Auftragsdatenverarbeitung in § 11 BDSG, soweit anwendbar, als Grundlage herangezogen werden. Wenn allerdings die Landeskrankenhaus- oder vergleichbare Gesetze vorrangig sind, sind nach wie vor deren spezifisch auf Patientendaten gemünzten Vorschriften über die Auftragsdatenverarbeitung unabhängig von einem Offenbaren im Sinne der Schweigepflicht maßgeblich.

Selbst wenn man der soeben im ersten Absatz vertretenen Auffassung folgt und keinen Personenbezug für den Auftragnehmer annimmt, empfiehlt es sich aus Gründen der Rechtssicherheit und einer der möglichen Re-Identifizierung vorbeugenden Risikovorsorge aber für die Behandlungseinrichtung, eine Vereinbarung mit dem Auftragnehmer abzuschließen, welche die jeweils anwendbaren Vorschriften zur Auftragsdatenverarbeitung möglichst weitgehend umsetzt.

8.2 Gesundheitsspezifische Regelungen zur Auftragsdatenverarbeitung

Nach den vorstehenden Ausführungen können nur solche Regelungen zur Auftragsdatenverarbeitung als Offenbarungsbefugnis im Sinne der Schweigepflicht nach § 203

⁷⁹² Die Schweigepflichtentbindung unterliegt nicht den strengeren Formvorschriften der datenschutzrechtlichen Einwilligung (i.d.R. Schriftform). Im Sinne der Rechtssicherheit ist aber auch hier die Schriftform zu empfehlen.

StGB angesehen werden, die einen spezifischen Bezug zum Arzt-Patienten-Verhältnis oder zumindest zu Gesundheitsdaten haben. Zwar wird hier angesichts der vorgängigen internen Pseudonymisierung vertreten, dass eine solche Offenbarungsbefugnis mangels Personenbezug für den Auftragnehmer genauso wenig wie eine datenschutzrechtliche Erlaubnis für die Datenübertragung nötig ist. Gleichwohl soll im Folgenden hilfsweise auf möglicherweise heranzuziehende Regelungen eingegangen werden, welche auch als Orientierung für die zur Sicherheit in jedem Fall abzuschließenden Vereinbarungen mit den Auftragnehmern dienen können.

8.2.1 Keine gesundheitsspezifische Auftragsdatenverarbeitung im BDSG

Im BDSG fehlen gesundheitsspezifische Regelungen zur Auftragsdatenverarbeitung. Die allgemeine Vorschrift zur Auftragsdatenverarbeitung nach § 11 BDSG kann nicht als Befugnis zum Offenbaren im Sinne von § 203 StGB herangezogen werden.⁷⁹³ Damit scheidet eine Offenbarungsbefugnis über die Regelungen zur Auftragsdatenverarbeitung für Arztpraxen, Kliniken des Bundes und diejenigen übrigen (privaten) Kliniken, auf welche nur das BDSG anwendbar ist, aus.⁷⁹⁴

Dies gilt letztlich auch für die Bestimmungen in § 28 Abs. 6–8 BDSG, die zwar spezifisch auf Gesundheitsdaten gemünzt sind. Doch bleiben besondere Berufsgeheimnisse wie die ärztliche Schweigepflicht gemäß § 1 Abs. 3 S. 2 BDSG von diesem unberührt, so dass selbst diese gesundheitsspezifischen Regelungen keine Offenbarungsbefugnisse darstellen. Daher kommt es auch nicht darauf an, ob man von diesen Übermittlungsbefugnissen „a maiore ad minus“ (letztlich also erst recht) auf eine Berechtigung zur gesundheitsdatenbezogenen Auftragsdatenverarbeitung schließen kann.⁷⁹⁵

8.2.2 Landeskrankenhaus- oder vergleichbare Gesetze

Die bereichsspezifischen Datenschutzvorschriften der Länder für den Krankenhausbereich enthalten jedoch vielfach Sonderregelungen zur Auftragsdatenverarbeitung im Hinblick auf Patientendaten, welche auch als Befugnis im Rahmen von § 203 StGB herangezogen werden können.⁷⁹⁶ Allerdings enthalten diese Regelungen besondere Restriktionen gegenüber der Auftragsdatenverarbeitung im Allgemeinen, welche sowohl bezüglich der Rechtmäßigkeit im Hinblick auf den Datenschutz als auch die Schweigepflicht gemäß § 203 StGB zu beachten sind.⁷⁹⁷

8.2.2.1 Baden-Württemberg

Im Anwendungsbereich des LKHG BW, also für alle Krankenhäuser in Baden-Württemberg mit Ausnahme solcher des Bundes, regelt § 48 LKHG BW die Verarbeitung

⁷⁹³ Petri, in: Simitis (Hg.), BDSG, § 11 Rdnr. 44f.; s.a. oben Fn. 778.

⁷⁹⁴ Welche Kliniken dies sind, kann der Übersicht 1 zum anwendbaren Datenschutzrecht entnommen werden.

⁷⁹⁵ Dahinter würde folgender Gedanke stecken: Wenn schon eine – einschneidendere, rechtfertigungsbedürftigere – Übermittlung von Gesundheitsdaten an einen selbständig verantwortlichen Dritten zulässig ist, muss erst recht die Einschaltung eines weisungsgebundenen Auftragsdatenverarbeiters erlaubt sein. Neben den Voraussetzungen von § 28 Abs. 6–8 BDSG müssten in diesem Fall auch die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG eingehalten werden.

⁷⁹⁶ Alkmade u.a., Der Gehilfe des Arztes, S. 17, 8ff., wo diese Regelungen sehr knapp dargestellt werden.

⁷⁹⁷ Es sei denn, es liegen eine datenschutzrechtliche Einwilligung sowie eine (ggf. in der Einwilligung inkludierte) Schweigepflichtentbindung vor.

von Patientendaten im Auftrag eines der genannten Krankenhäuser. Nach § 48 Abs. 1 LKHG BW sind Patientendaten im Krankenhaus selbst oder durch ein anderes Krankenhaus zu verarbeiten.

Im Auftrag eines Krankenhauses durch ein Rechenzentrum dürfen Patientendaten gemäß § 48 Abs. 2 LKHG BW automatisiert verarbeitet werden, wenn

1. die für Auftraggeber und Auftragnehmer zuständige Datenschutzaufsichtsbehörde hiervon benachrichtigt wird,
2. der Auftragnehmer seinen Mitarbeitern, soweit ihnen aus zwingenden Gründen eine Zugriffsberechtigung auf Patientendaten eingeräumt wird, eine § 203 StGB entsprechende Schweigepflicht auferlegt und
3. die nach dem Bundesdatenschutzgesetz oder dem Landesdatenschutzgesetz für die Verarbeitung von personenbezogenen Daten im Auftrag erforderlichen technischen und organisatorischen Maßnahmen schriftlich festgelegt werden.

Im Übrigen stellt § 48 Abs. 2 Nr. 3 Hs. 2 LKHG BW klar, dass die Vorschrift des § 3a Landesverwaltungsverfahrensgesetz (LVwVfG) BW über die elektronische Kommunikation mit Behörden keine Anwendung findet. Insoweit gelten also für die Krankenhäuser die allgemeinen Maßgaben von Datenschutz und Datensicherheit, nach denen die elektronische Kommunikation ähnlich wie in § 3a LVwVfG BW zwischen den Kommunikationspartnern aber auch gesondert eröffnet oder vereinbart werden muss und die bei einer Kommunikation über offene Netze ebenfalls eine Authentifizierung der Kommunikationspartner (wenn auch nicht zwingend durch qualifizierte elektronische Signaturen wie in § 3a Abs. 2 LVwVfG BW vorgesehen) sowie eine starke Verschlüsselung vorschreiben. Dies ergibt sich schon aus dem Verweis in Nr. 3 Hs. 1 auf die nach dem BDSG (§ 9)⁷⁹⁸ oder dem LDSG (dort ebenfalls § 9)⁷⁹⁹ erforderlichen technischen und organisatorischen Maßnahmen der Datensicherheit.

Subsidiär, also nachrangig, gelten überdies, auch ohne expliziten Verweis in § 48 LKHG BW, die allgemeinen Vorschriften zur Auftragsdatenverarbeitung, je nach Art der Klinik also § 11 BDSG oder § 7 LDSG BW.⁸⁰⁰ Denn § 48 LKHG BW bestimmt nur bereichsspezifisch zusätzliche Anforderungen an die Verarbeitung von Patientendaten im Auftrag von Krankenhäusern ohne den Gesamtkomplex der Auftragsdatenverarbeitung abschließend regeln zu wollen.

Die nach § 48 Abs. 2 Nr. 1 LKHG BW zu benachrichtigenden Datenschutzaufsichtsbehörden ergeben sich für die dem LKHG BW unterworfenen Kliniken aus der weiter vorne abgedruckten Übersicht zum auf Kliniken anwendbaren Datenschutzrecht sowie zur zuständigen Datenschutzaufsicht.⁸⁰¹ Für die Kliniken selbst ist dies in der Regel der baden-württembergische Landesbeauftragte für den Datenschutz. Für die eingeschalteten Rechenzentren wäre deren zuständige Aufsichtsbehörde im Einzelfall zu prüfen; bei Rechenzentren der öffentlichen Hand wird sich in der Regel die gleiche Aufsichtsbehörde wie bei öffentlichen Kliniken, bei privaten Rechenzentren regelmäßig die gleiche wie bei Privatkliniken am jeweiligen Sitz ergeben.⁸⁰² Da pri-

798 Gültig für alle Kliniken in Baden-Württemberg mit Ausnahme derjenigen nach folgender Fn. 799.

799 Für Kliniken, die als Regiebetrieb ohne eigene Rechtspersönlichkeit einer öffentlichen Stelle des Landes zugeordnet sind.

800 Die Anwendung von BDSG oder LDSG folgt dem in den Fn. 798, 799 beschriebenen Muster, wie es sich auch aus der Übersicht 1 ergibt.

801 S. vorne Seite 81ff.

802 Auch insoweit hat also die Übersicht 1 auf S. 82ff. eine Indizwirkung.

mär die Klinik als Auftraggeber für die Einhaltung von § 48 LKHG BW verantwortlich ist, sollte sich diese auch von der Benachrichtigung der für den Auftragnehmer, also das Rechenzentrum zuständigen Datenschutzaufsichtsbehörde überzeugen, selbst wenn diese Benachrichtigung vom Auftragnehmer ausgeht. Die Klinik sollte den Auftragnehmer hierauf vertraglich verpflichten und sich möglichst auch eine Kopie der Benachrichtigung vorlegen lassen. Die eigene Datenschutzaufsichtsbehörde muss die Klinik natürlich selbsttätig benachrichtigen.

Aus § 48 Abs. 2 Nr. 2 LKHG BW ergibt sich zunächst, dass Mitarbeiter des Auftragnehmers nur aus zwingenden Gründen, also soweit unbedingt erforderlich, Zugriffsrechte auf Patientendaten erhalten dürfen. Zudem muss der Auftragnehmer seinen Mitarbeitern dann eine „§ 203 StGB entsprechende Schweigepflicht auferlegt“ werden. Fraglich ist, was unter einer entsprechenden Schweigepflicht zu verstehen ist. Dazu wird einerseits ausgeführt, dass diese „nicht hinter § 203 StGB zurückbleiben“ dürfe, andererseits soll sie sich „im Wesentlichen [...] mit der aus dem Datengeheimnis resultierenden Schweigepflicht decken“.⁸⁰³

Von den Rechtsfolgen her ist ein Verstoß gegen das Datengeheimnis, jedenfalls das gemäß § 5 BDSG, schwächer sanktioniert als es § 203 StGB vorsieht. Denn auch bei einem vorsätzlichen Verstoß, soweit dieser nicht gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht durchgeführt wurde,⁸⁰⁴ droht beim unbefugten Umgang mit nicht allgemein zugänglichen Daten (entsprechend den nach § 203 StGB geschützten Privatgeheimnissen) lediglich ein Bußgeld (§ 43 Abs. 2 Nr. 1 BDSG) und nicht wie bei § 203 Abs. 1 StGB eine Freiheitsstrafe bis zu einem Jahr.

Angesichts der Zwei-Schranken-Theorie können auch der Umfang der Geheimhaltungsverpflichtungen und damit die Voraussetzungen für eine zulässige Datenweitergabe nach Datenschutz und Schweigepflicht durchaus unterschiedlich sein. Zwar stellt § 49 LKHG BW klar, dass eine Weitergabe unter den Voraussetzungen der §§ 45 bis 48 LKHG BW nicht unbefugt ist, was insoweit zu einer Deckungsgleichheit beider Regelungskreise führt.⁸⁰⁵ Allerdings gelten diese Regelungen für den Auftragnehmer nicht unmittelbar, auch wenn für die Zulässigkeit die Rechtslage beim Auftraggeber maßgeblich ist, was sich aber nicht automatisch auf die Verpflichtung der Mitarbeiter des Auftragnehmers auf das allgemeine Datengeheimnis erstreckt.⁸⁰⁶

Die rechtssicherste Lösung ist daher die förmliche Verpflichtung der zugriffsberechtigten Mitarbeiter des Auftragnehmers nach dem Verpflichtungsgesetz. Dies führt dazu, dass sich diese in Verbindung mit § 11 Abs. 1 Nr. 4 StGB nach § 203 Abs. 2 S. 1 Nr. 2, 6 StGB strafbar machen können, welcher so nah an den Voraussetzungen des § 203 Abs. 1 Nr. 1 StGB ist und überdies die identischen Rechtsfolgen zeitigt, dass man an einer Entsprechung nicht zweifeln kann. Die förmliche Verpflichtung nach dem Verpflichtungsgesetz ist jedoch mit einigem Verwaltungsaufwand verbunden. Sie ist von der Verpflichtung auf das Datengeheimnis nach allgemeinem Datenschutz-

803 Bezeichnenderweise beides vertreten von Sieper, in: Bold/Sieper, LKHG BW, § 48 Rdnr. 8.

804 Liegen diese Qualifikationen vor, kommt es von den Rechtsfolgen her allerdings zu einem Gleichklang von § 44 BDSG und § 203 Abs. 1, 5 StGB: Freiheitsstrafe bis zu drei Jahren.

805 Wohl zu weitgehend eine vollständige Deckungsgleichheit andeutend Sieper, in: Bold/Sieper, LKHG BW, § 49 Rdnr. 2.

806 Zudem könnte es zirkulär sein, in § 49 LKHG BW festzuhalten, dass bei Einhaltung u.a. von § 48 LKHG BW auch die Schweigepflicht nach § 203 StGB gewährt wird, um dann in § 48 Abs. 2 Nr. 2 LKHG BW wiederum auf eine § 203 StGB entsprechende Geheimhaltungspflicht zu verweisen, wenn letztere doch wieder nach Maßgabe der in § 49 LKHG BW genannten Vorschriften des LKHG BW und damit auch von dessen § 48 bestimmt wird.

recht (§ 5 BDSG, § 6 LDSG BW) zu unterscheiden. Die förmliche Verpflichtung wird nach § 1 VerpflG grundsätzlich von der verantwortlichen öffentlichen Stelle (Abs. 4) mündlich vorgenommen (Abs. 2), worüber eine Niederschrift anzufertigen ist (Abs. 3). Zudem ist dieser Weg nur für Kliniken öffentlicher Träger gangbar.

Eine Entsprechung fordert allerdings nicht zwingend eine vollständige Übereinstimmung der Regelungen. Zudem sieht § 48 Abs. 2 Nr. 2 LKHG BW eine Verpflichtung durch den Auftragnehmer vor, welcher zwar – bei durchaus existierenden öffentlichen Rechenzentren – auch eine öffentliche Stelle sein kann, typischerweise aber nicht ist. Vor diesem Hintergrund ist eine Lösung vertretbar, in welcher der Auftragnehmer die Verpflichtung seiner Mitarbeiter auf das allgemeine Datengeheimnis (§ 5 BDSG oder § 6 LDSG) für diejenigen mit Zugriff auf Patientendaten eines Krankenhauses durch eine krankenhausspezifische Zusatzverpflichtung präzisiert, in welcher die nach § 203 StGB und dem LKHG BW verpflichtenden Schutzmaßnahmen kurz erläutert werden. Das Krankenhaus sollte diese Zusatzverpflichtung in der Vereinbarung über die Auftragsdatenverarbeitung vorschreiben und ein Muster vorgeben. Idealerweise sollten Kopien aller unterzeichneten Zusatzverpflichtungen an das Krankenhaus gehen oder dem Auftraggeber die zugriffsberechtigten Mitarbeiter zumindest namentlich benannt werden.

Zuletzt stellt § 48 Abs. 3 LKHG BW fest, dass sich die Patientendaten im ausschließlichen Gewahrsam des Krankenhauses befinden, in dessen Auftrag sie verarbeitet werden. Diese Fiktion soll ein Beschlagnahmeverbot nach § 97 StPO begründen, welcher nach Abs. 2 S. 1 grundsätzlich vorschreibt, dass ein solches nur für Gegenstände im Gewahrsam eines Zeugnisverweigerungsberechtigten (wie eines Arztes) gilt. Eine rein landesrechtliche Fiktion könnte dieses Erfordernis wohl nicht umgehen. Allerdings erweitert § 97 Abs. 2 S. 2 StPO das Beschlagnahmeverbot ohnehin auf Krankenanstalten und Dienstleister, die für die Zeugnisverweigerungsberechtigten personenbezogene Daten erheben, verarbeiten oder nutzen, so dass es auf die Wirkung der landesrechtlichen Regelung nicht ankommt.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR⁸⁰⁷ keine gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.2.2.2 Bayern

Art. 27 LKHG BY ordnet Sonderregeln für den Datenschutz in bayerischen Krankenhäusern an.

Krankenhäuser können nach Art. 27 Abs. 4 S. 2 Hs. 2 LKHG BY zu Zwecken der Forschung anderen Personen die Nutzung von Patientendaten gestatten, wenn dies zur

807 Das subsidiär anwendbare LDSG BW nimmt in seinem § 3 Abs. 5 nur Stellen, die in einem Mitgliedstaat der europäischen Union personenbezogene Daten im Auftrag verarbeiten vom Begriff des Dritten, an den eine Weitergabe zu erfolgen hat, um als Übermittlung zu gelten, aus. Der territoriale Anwendungsbereich dieser Ausnahme wurde mittlerweile allerdings in Umsetzung internationaler Abkommen erweitert, zunächst durch das multilaterale EWR-Abkommen auf die EFTA-Mitglieder mit Ausnahme der Schweiz, also Island, Liechtenstein und Norwegen. Auf verwaltungstechnische Probleme bei der Bestimmung der zuständigen Aufsichtsbehörde für die Auftragnehmer in den genannten ausländischen Staaten kann vorliegend nicht weiter eingegangen werden; in jedem der einbezogenen Länder existiert aufgrund eines durch die Abkommen vorgegeben vergleichbaren Datenschutzniveaus aber eine solche Aufsichtsbehörde.

Durchführung des Forschungsvorhabens erforderlich ist und die Patientendaten im Gewahrsam des Krankenhauses verbleiben. Diese Personen sind dann zur Verschwiegenheit zu verpflichten, Art. 27 Abs. 4 S. 3 LKHG BY. Dabei könnte es sich um einen privilegierten Sonderfall der Datenübermittlung (durch Gewährung von Zugriffsrechten) handeln, wenn die zugriffsberechtigten Personen in gewissem Umfang eigenverantwortlich (z.B. im Rahmen der Verbundforschung) mit den Patientendaten umgehen. Dabei wäre es jedoch eine schwierig zu meisternde Herausforderung, den Gewahrsam des Krankenhauses nicht zu brechen und einen tatsächlichen Datenabfluss zu vermeiden.⁸⁰⁸ Soweit ein rein weisungsgebundener Datenumgang durch einen solchen Zugriff ermöglicht wird, z.B. im Rahmen der rein technischen (Fern-)Wartung einer Forschungsdatenbank, liegt aber auch ein Fall der Auftragsdatenverarbeitung vor, auf den subsidiär die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG (bei privater Trägerschaft) oder Art. 6 LDSG BY (bei öffentlicher Trägerschaft) anzuwenden sind.

Nach Art. 27 Abs. 4 S. 5 des LKHG BY kann sich das Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen, wenn es sicherstellt, dass beim Auftragnehmer die besonderen Schutzmaßnahmen nach Art. 27 Abs. 6 LKHG BY eingehalten werden, und solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden. Unter besonderen Schutzmaßnahmen im Sinne des Art. 27 Abs. 6 LKHG BY sind Schutzmaßnahmen technischer und organisatorischer Art zu verstehen, durch die sichergestellt werden muss, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können. Zu beachten ist hierbei jedoch, dass sich das Krankenhaus zur Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, nur anderer Krankenhäuser bedienen darf (Art. 27 Abs. 4 S. 6 LKHG BY); diese Beschränkung greift daher auch bei Forschung und Qualitätssicherung. Vor diesem Hintergrund erfordert jede Datenverarbeitung durch einen Cloud-Anbieter zu diesen Zwecken, soweit personenbezogene Daten in die Cloud gegeben werden, eine Einwilligung der betroffenen Patienten. Subsidiär sind auch hier die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG (bei privater Trägerschaft) oder Art. 6 LDSG BY (bei öffentlicher Trägerschaft) zu beachten.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits erörterten Grundsätzen, auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR keine gesondert zu rechtfertigende Datenübermittlung darstellt und im Rahmen der eben genannten Vorschrift erlaubt ist.

Zwar ist das Datenschutzniveau innerhalb des EWR im Gesundheitswesen eingeschränkter harmonisiert als in vielen anderen Bereichen, da Art. 8 der Datenschutzrichtlinie den Mitglieds- bzw. Vertragsstaaten insoweit größere Spielräume lässt. Da für die Zulässigkeit der Datenverarbeitung aber der Sitz des Auftraggebers und nicht der des Auftragnehmers maßgeblich ist, wirkt sich dieser Unterschied vorliegend kaum aus. Für die allgemeinen gesetzlichen Vorgaben zur Datensicherheit ist zwar

808 S. oben S. 140.

grundsätzlich der Sitz des Auftragnehmers maßgeblich (Art. 17 Abs. 3 Spiegelstrich 2 Datenschutzrichtlinie 95/46/EG).

Aufgrund Art. 27 Abs. 4 S. 5 LKHG BY müssen dem Auftragnehmer jedoch vertraglich auch die in Bayern maßgeblichen besonderen Schutzmaßnahmen technischer und organisatorischer Art nach Art. 27 Abs. 6 LKHG BY aufgegeben werden. Vor diesem Hintergrund dürften im Allgemeinen auch keine zwingenden Anhaltspunkte für eine Beeinträchtigung der schutzwürdigen Interessen des Betroffenen ersichtlich sein. Allerdings ist die Beschränkung auf Krankenhäuser als Auftragnehmer nach Art. 27 Abs. 5 S. 6 LKHG BY auch im EU- bzw. EWR-Ausland zu beachten.

8.2.2.3 Berlin

§ 24 Abs. 7 S. 1 des LKHG BE stellt den Grundsatz auf, dass Patientendaten im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus zu verarbeiten sind. Abweichend hiervon dürfen andere Stellen Patientendaten im Auftrag des Krankenhauses nur verarbeiten, wenn durch technische Schutzmaßnahmen sichergestellt ist, dass der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf Patientendaten den Personenbezug herzustellen (§ 24 Abs. 7 S. 2 LKHG BE). Soll die Archivierung von elektronischen Patientendokumentationen durch Dritte außerhalb des Krankenhauses erfolgen, ist dies nach § 24 Abs. 7 S. 3 LKHG BE nur zulässig, wenn das Krankenhaus zuvor eine Verschlüsselung der Patientendaten nach dem Stand der Technik vorgenommen hat.

Weiterhin finden bei der Auftragsdatenverarbeitung, z.B. im Hinblick auf den Inhalt der abzuschließenden Verträge oder die durchzuführenden Kontrollen, § 11 BDSG (bei privater Trägerschaft) oder § 3 LDSC BE (bei öffentlicher Trägerschaft) subsidiär Anwendung, was durch § 27 Abs. 7 S. 4 LKHG BE explizit klargestellt wird.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits, auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR keine gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.2.2.4 Brandenburg

Das KHEG BB enthält keine Regelung in Bezug auf die Auftragsdatenverarbeitung.

Nach § 27 Abs. 1 KHEG BB sind daher insoweit die Vorschriften der LDSC BB zu beachten. In § 11 LDSC BB, der subsidiär auf Krankenhäuser in öffentlicher und privater Trägerschaft anzuwenden ist, finden sich Regelungen zur Auftragsdatenverarbeitung, welche sich aber nicht ausdrücklich auf Gesundheitsdaten beziehen und welche daher vor dem Hintergrund der Schweigepflicht nach § 203 StGB nicht als Offenbarungsbefugnis gelten. Soweit man daher von einem Offenbaren ausgeht und keine Schweigepflichtentbindung vorliegt, führt die Einhaltung dieser allgemeinen datenschutzrechtlichen Vorschrift über die Auftragsdatenverarbeitung insgesamt nicht zu einer Rechtmäßigkeit des Outsourcings.

8.2.2.5 Bremen

§ 10 Abs. 1 KHD SG HB⁸⁰⁹ stellt den Grundsatz auf, dass Patientendaten im Krankenhaus zu verarbeiten sind. Eine Verarbeitung im Auftrag ist demnach nur zulässig, wenn die Wahrung der Datenschutzbestimmungen des KHD SG HB auch bei der verarbeitenden Stelle sichergestellt ist und diese sich insoweit der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft. Letztlich müssen die entsprechenden Verpflichtungen des Krankenhauses damit vertraglich auch dem Auftragnehmer „übergestülpt“ werden.⁸¹⁰

Die besondere Schutzbedürftigkeit von Patientendaten aus dem medizinischen Bereich ist im Rahmen der nach § 7 Abs. 4 LD SG HB frühestmöglich durchzuführenden Pseudonymisierung (getrennten Speicherung des Patientenbezugs) und Anonymisierung (Löschung des Patientenbezugs) zu berücksichtigen (§ 10 Abs. 2 KLD SG HE HB).

Der Zugriff auf Patientendaten durch Auftragnehmer ist im Rahmen der Prüfung oder Wartung von Datenverarbeitungsanlagen und von automatisierten Verfahren abweichend von § 9 Abs. 4 LD SG HB nur zulässig, wenn das Krankenhaus im **Einzel-fall zuvor die Daten zum Zugriff freigegeben** hat (§ 10 Abs. 3 KHD SG HB). Im Rahmen der nach § 7 Abs. 4 LD SG HB zu treffenden technischen und organisatorischen Maßnahmen⁸¹¹ ist auch sicherzustellen, dass Auftragnehmer bei der Administration technischer Vorkehrungen zur Abwehr von Angriffen auf das Datenverarbeitungssystem so weit möglich nicht Zugriff auf Patientendaten nehmen können (§ 10 Abs. 4 S. 1 KHD SG HB).

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 9 LD SG HB (bei öffentlicher und privater Trägerschaft) zu beachten.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.2.2.6 Hamburg

Für die Auftragsdatenverarbeitung regelt § 9 Abs. 1 LKHG HH, dass das Krankenhaus mit der Speicherung und der weiteren Verarbeitung von Patientendaten eine Stelle außerhalb des Krankenhauses beauftragen darf, wenn diese sich verpflichtet, die für das Krankenhaus geltenden Datenschutzbestimmungen einzuhalten. Die Stelle ist unter besonderer Berücksichtigung der Eignung der von ihr getroffenen Maßnahmen zur Datensicherung sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei, falls erforderlich, ergänzende Maßnahmen zur Datensicherung festzulegen sind.

⁸⁰⁹ Das Gesetz tritt gemäß § 14 KHD SG HB mit Ablauf des 31. Dezember 2015 außer Kraft.

⁸¹⁰ Für die Empfänger von Datenübermittlungen ergibt sich dies ausdrücklich aus § 4 Abs. 3 KHD SG HB. Zwar fallen unter den Begriff des Empfängers nach allgemeiner datenschutzrechtlicher Terminologie auch Auftragsdatenverarbeiter, doch nimmt § 4 Abs. 3 KHD SG HB hier ausdrücklich auf die Empfänger bestimmter Übermittlungen Bezug, so dass eine direkte Erstreckung der Norm ausscheidet. Über § 10 Abs. 1 KHD SG HB dürfte sich jedoch das gleiche Ergebnis herleiten lassen.

⁸¹¹ Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle.

Die beauftragte Stelle darf die überlassenen Daten nach § 9 Abs. 2 LKHG HH nicht anderweitig verarbeiten. Weiterhin darf sie die Daten nicht länger aufbewahren, als es das Krankenhaus bestimmt. Spätestens bei der Beendigung des Auftrags sind die Daten zurückzugeben oder zu löschen.

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG⁸¹² oder § 3 LDSC HH⁸¹³ zu beachten.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.2.2.7 Hessen

Im LKHG HE⁸¹⁴ findet sich keine Regelung für die Auftragsdatenverarbeitung. Nach § 12 Abs. 1 LKHG HE finden somit die Vorschriften des LDSC HE Anwendung.

§ 4 LDSC HE regelt die Auftragsdatenverarbeitung. Nach § 4 Abs. 2 S. 4 LDSC HE hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach § 10 LDSC HE erforderlichen technischen und organisatorischen Maßnahmen der Datensicherheit getroffen wurden; dabei sind die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen, sowie bei der Verarbeitung der in § 7 Abs. 4 LDSC HE genannten (sensiblen Gesundheits-)Daten zu beachten. Durch den expliziten Bezug auf besondere Berufsgeheimnisse, zu denen auch die ärztliche Schweigepflicht zählt, sowie auf sensible Daten, zu denen auch solche zur Gesundheit zählen, kann in § 4 LDSC HE im Gegensatz zu den Regeln zur Auftragsdatenverarbeitung im BDSG sowie vielen anderen LDSC insoweit auch eine Befugnisnorm im Sinne von § 203 StGB gesehen werden. Dies gilt wohl allerdings nur bei Auftragsvergabe an öffentliche Stellen, denn gemäß § 4 Abs. 2 S. 5 LDSC HE darf ein Auftrag zur Datenverarbeitung an nicht-öffentliche Stellen nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen. Bezüglich der Vergabe an nicht-öffentliche Stellen wird also klargestellt, dass hier Berufsgeheimnisse weiterhin entgegenstehen können, so dass insoweit auch der indirekte Bezug auf Gesundheitsdaten nicht mehr für eine Einstufung als Offenbarungsbefugnis ausreicht.

Die datenverarbeitende Stelle (Auftraggeber) bleibt nach § 4 Abs. 1 S. 1 LDSC HE für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz sowie für die Erfüllung ihrer sich aus § 8 LDSC HE ergebenden Pflichten auch dann verantwortlich, wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden.

Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten, § 4 Abs. 1 S. 2 LDSC HE. Ist der Auftragnehmer der

812 Bei Krankenhäusern in privater Trägerschaft sowie Krankenhäusern in öffentlicher Trägerschaft, die aber in privater Rechtsform (z. B. als GmbH) geführt werden.

813 Bei Krankenhäusern in öffentlicher Trägerschaft, welche in öffentlich-rechtlicher Rechtsform (z. B. als Eigenbetrieb des Staates Hamburg oder als Anstalt öffentlichen Rechts) geführt werden.

814 Dieses Gesetz tritt gemäß § 41 Satz 2 LKHG HE mit Ablauf des 31. 12. 2015 außer Kraft.

Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber nach § 4 Abs. 1 S. 3 LDSG HE unverzüglich darauf hinzuweisen.

Weiterhin ist der der Auftragnehmer nach § 4 Abs. 2 S. 1 LDSG HE unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen (§ 4 Abs. 2 S. 1 LDSG HE).

Reine Privatkliniken sind vom Anwendungsbereich des LDSG HE ausgeschlossen (§ 3 Abs. 6 S. 2 LDSG HE), sodass es für sie bei der Anwendung des § 11 BDSG bleibt, der allerdings keine Offenbarungsbefugnis enthält.

Bezüglich des Sitzes des Auftragnehmers ordnet § 4 Abs. 3 S. 1 LDSG HE an, dass sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden (also bei privaten Auftragnehmern oder Auftragnehmern in anderen Bundesländern oder im Ausland), der Auftraggeber verpflichtet ist, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Außerdem hat der Auftraggeber den Hessischen Datenschutzbeauftragten in diesen Fällen vorab über die Beauftragung zu unterrichten (§ 4 Abs. 3 S. 2 LDSG HE). Die Beschränkung auf den EWR ist allerdings auch dann zu beachten, denn ansonsten läge eine besonders rechtfertigungsbedürftige Übermittlung vor.

8.2.2.8 Mecklenburg-Vorpommern

§ 39 des LKHG MV regelt die Datenverarbeitung im Auftrag. Demnach darf der Krankenhausträger die Verarbeitung von Patientendaten einem Auftragnehmer übertragen, wenn

1. Störungen im Betriebsablauf sonst nicht vermieden werden können,
2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann⁸¹⁵ oder
3. das Krankenhaus seinen Betrieb einstellt.

§ 39 Abs. 1 S. 2 LKHG MV schreibt vor, dass vor der Erteilung eines Auftrags zur Verarbeitung von Patientendaten außerhalb des Krankenhauses zu prüfen ist, ob der Zweck auch mit verschlüsselten oder pseudonymisierten Patientendaten erreicht werden kann.

Eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer ist außerhalb des Krankenhauses nach § 39 Abs. 2 LKHG MV nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt.

Nach § 39 Abs. 3 LKHG ist der Auftragnehmer vom Krankenhausträger sorgfältig auszuwählen. Außerdem sind die Einzelheiten des Auftrags und die vom Auftrag-

⁸¹⁵ § 39 Abs. 1 S. 1 Nr. 1, 2 LKHG MV entsprechen dabei weitgehend der Regelung für eine Datenverarbeitung durch nicht-öffentliche Stellen im Auftrag von gesetzlichen Krankenkassen in § 80 Abs. 5 SGB X, dessen Auslegung und Anwendung insoweit ergänzend herangezogen werden kann.

nehmer zu treffenden technischen und organisatorischen Sicherungsmaßnahmen schriftlich zu vereinbaren. Eine Abschrift der Vereinbarung hat der Krankenhausträger dem Landesbeauftragten für den Datenschutz unverzüglich zu übersenden.

Der Auftragnehmer darf gemäß § 39 Abs. 4 S. 1 LKHG MV die ihm überlassenen Patientendaten nur im Rahmen des Auftrags und der Weisungen des Krankenhausträgers verarbeiten.

Eine Übertragung des Auftrags auf Dritte oder die Erteilung von Unteraufträgen ist nur mit Zustimmung des Krankenhausträgers zulässig, wobei in einem solchen Fall § 39 Abs. 2 bis 4 LKHG MV entsprechend gelten, § 39 Abs. 5 S. 1 und 2 LKHG MV.

Übernimmt ein Auftragnehmer nach einer Betriebseinstellung eines Krankenhauses den gesamten Bestand der Patientendaten, gelten für ihn als verantwortliche Stelle hinsichtlich der Verarbeitung dieser Daten die Vorschriften des Datenschutz-Abschnitts des LKHG MV (§ 39 Abs. 6 S. 1 LKHG MV). Bei der Übernahme ist gemäß § 39 Abs. 6 S. 2 LKHG MV vertraglich sicherzustellen, dass die Patientinnen und Patienten für die Dauer von zehn Jahren nach Abschluss der Behandlung oder Untersuchung auf Verlangen in gleicher Weise wie bisher beim Krankenhaus Auskunft und Einsicht erhalten.

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 4 LDSG MV (bei öffentlicher und privater Trägerschaft) zu beachten.

Bezüglich des Sitzes des Auftragnehmers ordnet § 39 Abs. 4 S. 2 LKHG MV an, dass sofern die §§ 32 bis 38 LKHG MV für den Auftragnehmer nicht gelten, der Krankenhausträger sicherzustellen hat, dass der Auftragnehmer diese Vorschriften entsprechend anwendet und sich insoweit der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft. Die Beschränkung auf den EWR ist allerdings auch dann zu beachten, denn ansonsten läge eine besonders rechtfertigungsbedürftige Übermittlung vor.

8.2.2.9 Niedersachsen

Das LKHG NI enthält keine bereichsspezifische Regelung für Krankenhäuser in Bezug auf die Auftragsdatenverarbeitung. Insoweit wird auch bezüglich der Auftragsdatenverarbeitung auf das BDSG verwiesen,⁸¹⁶ welches allerdings – wie gesehen – keine Offenbarungsbefugnis enthält.⁸¹⁷

8.2.2.10 Nordrhein-Westfalen

§ 7 GDSG NW regelt die Datenverarbeitung im Auftrag von Kliniken in NRW.⁸¹⁸ § 7 Abs. 1 GDSG NW stellt den Grundsatz auf, dass Patientendaten grundsätzlich in der Einrichtung oder öffentlichen Stelle zu verarbeiten sind; eine Verarbeitung im Auftrag ist nur nach Maßgabe des § 7 Abs. 2 bis 4 GDSG NW zulässig.

Nach § 7 Abs. 2 GDSG NW ist die Verarbeitung von Patientendaten im Auftrag nur zulässig, wenn sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge

816 Für öffentliche Kliniken als Wettbewerbsunternehmen vermittelt durch § 2 Abs. 3 LDSG NI.

817 S. soeben S. 267.

818 Ausgenommen reine Privatkliniken, für welche hier ausschließlich das BDSG gilt.

der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können.⁸¹⁹

Außerdem hat sich der Auftraggeber gemäß § 7 Abs. 3 S. 1 GDSC NW vor der Vergabe eines Auftrages zur Verarbeitung von Patientendaten zu vergewissern, dass beim Auftragnehmer die Wahrung der Datenschutzbestimmungen dieses Gesetzes und der ärztlichen Schweigepflicht sichergestellt ist.

Patientendaten aus dem ärztlichen Bereich sind vom Auftragnehmer in physisch getrennten Dateien zu verarbeiten, § 7 Abs. 3 S. 2 GDSC NW. Weiterhin darf der Auftragnehmer Patientendaten nur im Rahmen der Weisungen des Auftraggebers verarbeiten und der Auftraggeber hat erforderlichenfalls dem Auftragnehmer Weisungen zur Ergänzung seiner technischen und organisatorischen Einrichtungen und Maßnahmen zu erteilen (§ 7 Abs. 3 S. 3 und 4 GDSC NW).

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG (bei reinen Privatkliniken) oder § 11 LDSC NW (bei öffentlicher Trägerschaft und Plankrankenhäusern in privater Trägerschaft) zu beachten.

Sofern der Auftragnehmer eine nicht-öffentliche Stelle ist, ordnet § 7 Abs. 4 S. 1 GDSC NW an, dass der Auftraggeber sicherzustellen hat, dass der Auftragnehmer sich, sofern die Datenverarbeitung im Geltungsbereich des GDSC NW durchgeführt wird, der Kontrolle durch den Landesbeauftragten für den Datenschutz unterwirft. Bei einer Auftragsdurchführung außerhalb des Geltungsbereichs dieses Gesetzes ist die zuständige Datenschutzkontrollbehörde zu unterrichten (§ 7 Abs. 4 S. 2 GDSC NW). Weitere Maßgaben hinsichtlich des Sitzes des Auftragnehmers enthält das GDSC NW nicht. Die Beschränkung auf den EWR ist allerdings auch hier zu beachten, denn ansonsten läge eine besonders rechtfertigungsbedürftige Übermittlung vor.

8.2.2.11 Rheinland-Pfalz

Zur Verarbeitung von Patientendaten kann sich das Krankenhaus nach § 36 Abs. 9 S. 1 LKHG RP anderer Personen oder Stellen bedienen, wenn die Einhaltung der Datenschutzbestimmungen dieses Gesetzes sowie eine § 203 StGB entsprechende Schweigepflicht bei der Auftragnehmerin oder beim Auftragnehmer sichergestellt ist.⁸²⁰ Das Krankenhaus ist hierbei nach § 36 Abs. 9 S. 2 LKHG RP verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der bei der Auftragnehmerin oder beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen der Datensicherung zu erteilen.

Die Auftragserteilung bedarf nach § 36 Abs. 9 S. 3 LKHG RP der vorherigen Zustimmung durch die zuständige Behörde.⁸²¹

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG (bei privater Trägerschaft) oder § 4 LDSC RP (bei öffentlicher Trägerschaft) zu beachten.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung

819 Ähnlich der Rechtslage nach § 39 Abs. 1 S. 1 Nr. 1, 2 LKHG MV (s.o. S. 275, Fn. 815) soll auch hier auf § 80 Abs. 5 SGB X verwiesen werden, dessen Auslegung und Anwendung insoweit ergänzend herangezogen werden kann.

820 Insbesondere zum Erfordernis der § 203 StGB entsprechenden Schweigepflicht siehe die Ausführungen zum LKHG BW oben S. 269f.

821 Mit dieser Behörde dürfte im Kontext des LKHG RP die Krankenhausaufsicht und nicht die Datenschutzaufsicht gemeint sein.

an einen Auftragnehmer innerhalb des EWR keine gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.2.2.12 Saarland

Gemäß § 13 Abs. 7 S. 1 LKHG SL⁸²² dürfen Patientendaten von Personen und Stellen außerhalb des Krankenhauses in seinem Auftrag nur verarbeitet werden, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der Datenverarbeitung hierdurch kostengünstiger besorgt werden können.⁸²³ Letzteres kann bei externer Datenverarbeitung und Nutzung von Cloud-Computing, welches vorhandene Ressourcen möglichst effizient allokiert, durchaus der Fall sein.

Die Krankenhausleitung kann dem beauftragten Unternehmen nach § 13 Abs. 7 S. 2 LKHG SL in jeder Phase der Verarbeitung von Patientendaten Weisungen erteilen. Sie hat das beauftragte Unternehmen unter besonderer Berücksichtigung der Eignung und Zuverlässigkeit sorgfältig auszuwählen (§ 13 Abs. 7 S. 3 LKHG SL). Das beauftragte Unternehmen muss nach § 13 Abs. 7 S. 4 und 5 LKHG SL insbesondere dafür Sorge tragen, dass von ihm getroffene technische und organisatorische Maßnahmen die Gewähr dafür bieten, das Patientengeheimnis zu wahren, und dass die Mitarbeiterinnen und Mitarbeiter sich zur Verschwiegenheit verpflichten.

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG (bei privater Trägerschaft) oder § 5 LDSC SL (bei öffentlicher Trägerschaft) zu beachten.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR keine gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.2.2.13 Sachsen

§ 33 Abs. 10 S. 1 LKHG SN bestimmt, dass sich das Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen kann, wenn sichergestellt ist, dass diese die Datenschutzbestimmungen dieses Gesetzes und die § 203 Strafgesetzbuch entsprechende Schweigepflicht einhalten. Das Krankenhaus ist hierbei jedoch nach § 33 Abs. 10 S. 2 LKHG SN verpflichtet, erforderlichenfalls den Auftragnehmer anzuweisen, Technik und Organisation der Datensicherung zu ergänzen.

Die Auftragserteilung bedarf der vorherigen Zustimmung durch die zuständige (Krankenhausaufsichts-)Behörde (§ 33 Abs. 10 S. 3 LKHG SN).

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG (bei privater Trägerschaft sowie bei Krankenhäusern in öffentlicher Trägerschaft mit eigener Rechtspersönlichkeit) oder § 7 LDSC SN (bei Krankenhäusern in öffentlicher Trägerschaft ohne eigene Rechtspersönlichkeit) zu beachten.

822 Dieses Gesetz tritt gemäß § 46 Abs. 3 LKHG SL mit Ablauf des 30.06.2015 außer Kraft.

823 Vgl. auch hierzu § 80 Abs. 5 SGB X; s. oben S. 275, Fn. 815.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR keine gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.2.2.14 Sachsen-Anhalt

Das LKHG ST enthält keine Regelung in Bezug auf die Auftragsdatenverarbeitung. Insoweit wird auch bezüglich der Auftragsdatenverarbeitung auf das BDSG verwiesen, welches allerdings keine Offenbarungsbefugnis enthält.⁸²⁴

8.2.2.15 Schleswig-Holstein

In Schleswig-Holstein gibt es lediglich ein Ausführungsgesetz zum KHG, aber kein Landeskrankenhausgesetz mit Regelungen zur Auftragsdatenverarbeitung oder auch nur allgemein zum Patientendatenschutz. Auch insoweit wird letztlich bezüglich der Auftragsdatenverarbeitung auf das BDSG verwiesen, welches allerdings keine Offenbarungsbefugnis enthält.⁸²⁵

8.2.2.16 Thüringen

§ 27b Abs. 1 S. 1 LKHG TH statuiert den Grundsatz, dass Patientendaten im Krankenhaus zu verarbeiten sind. Nach § 27b Abs. 1 S. 2 LKHG TH ist eine Verarbeitung und Nutzung durch eine andere Stelle im Auftrag nur zulässig, wenn

1. sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatisierten Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können,⁸²⁶
2. die Einhaltung der Datenschutzbestimmungen dieses Gesetzes sowie eine den Voraussetzungen des § 203 des Strafgesetzbuchs entsprechende Schweigepflicht beim Auftragnehmer sichergestellt ist und
3. der Auftraggeber der Aufsichtsbehörde nach § 32 Abs. 2 LKHG TH rechtzeitig vor Auftragserteilung Art, Umfang und die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag schriftlich angezeigt hat.

Im Vertrag über die Auftragsdatenverarbeitung ist nach § 27b Abs. 2 LKHG TH sicherzustellen, dass vom Auftraggeber oder von dessen Datenschutzkontrollbehörde veranlasste Kontrollen vom Auftragnehmer jederzeit zu ermöglichen sind.

Eine Datenverarbeitung in der Cloud könnte vorliegend wiederum die Bedingung erfüllen, dass sie dort erheblich kostengünstiger erbracht werden kann als im Krankenhaus selbst. Die übrigen Bedingungen müssten durch eine entsprechende vertragliche Gestaltung und die Anzeige bei der Aufsichtsbehörde erfüllt werden.

⁸²⁴ S. oben S. 267.

⁸²⁵ S. oben S. 267.

⁸²⁶ Vgl. auch hierzu § 80 Abs. 5 SGB X; s. oben S. 275, Fn. 815.

Subsidiär sind die Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG (bei privater Trägerschaft) oder § 8 LDSG TH (bei öffentlicher Trägerschaft) zu beachten.

Bezüglich des Sitzes des Auftragnehmers nimmt die Vorschrift keine besonderen Einschränkungen vor. Daraus folgt nach den bereits auch vor dem Hintergrund der Datenschutzrichtlinie 95/46/EG erörterten Grundsätzen, dass eine Datenübertragung an einen Auftragnehmer innerhalb des EWR keine gesondert zu rechtfertigende Datenübermittlung darstellt und nach der genannten Vorschrift erlaubt ist.

8.3 Zusammenfassende Bewertung

Nach hier vertretener Auffassung schließt eine effektive Pseudonymisierung innerhalb der Behandlungseinrichtung den Personenbezug der an den Auftragnehmer übertragenen pseudonymen Daten aus. Voraussetzung ist selbstverständlich, dass die Zuordnung des Pseudonyms zur Person des Patienten nicht mit übertragen, sondern geheim gehalten wird. Dies führt dazu, dass weder eine Übertragung personenbezogener Daten an den Auftragnehmer im Sinne des Datenschutzrechts stattfindet, welche als Datenübermittlung oder Auftragsdatenverarbeitung zu qualifizieren und zu rechtfertigen wäre, noch ein Offenbaren von Patientengeheimnissen nach § 203 StGB, für welche eine spezifische Befugnis notwendig wäre. Damit ist keine gesetzliche Grundlage und auch keine Einwilligung oder Schweigepflichtentbindung des Patienten für diesen Vorgang erforderlich.

Allerdings verbleiben trotz effektiver einrichtungsinterner Pseudonymisierung, welche für Außenstehende in der Regel einer relativen (faktischen) Anonymisierung gleichkommt, gewisse Risiken der Re-Identifizierung. Diese sollten im Sinne der Risikovorsorge durch Maßnahmen reduziert werden, die sich zumindest an den Vorschriften über die Auftragsdatenverarbeitung orientieren, ohne diese jedoch zwingend in jedem einzelnen Punkt, insbesondere im Hinblick auf die besonderen Restriktionen der Landeskrankenhausgesetze, vollständig erfüllen zu müssen. Zu diesen Maßnahmen gehört insbesondere der Abschluss eines Vertrages mit dem Auftragnehmer, in welchem ein Re-Identifizierungsverbot und flankierende Datenschutzmaßnahmen (wie Kontrollrechte) klar verankert sind, sowie die Kontrolle der tatsächlichen Einhaltung dieser Maßgaben. Diese Kontrolle muss allerdings nicht zwingend durch jede Behandlungseinrichtung einzeln für sich vorgenommen werden, sondern kann auch über Prüfungsgemeinschaften erfolgen, welche einen unabhängigen Auditor hierfür heranziehen.⁸²⁷

Im Sinne der Rechtssicherheit ideal, wenn auch aufgrund der vorliegend nur entsprechenden Anwendung der Vorschriften über die Auftragsdatenverarbeitung bzw. deren bloßer Orientierungswirkung nicht zwingend, wäre die Ausrichtung der jeweils abgeschlossenen Verträge an den jeweiligen Vorschriften der einzelnen Bundesländer, insbesondere also auch den LKHG. Dies würde jedoch die Erstellung einer einheitlichen und bundeslandübergreifend nutzbaren Vertragsvorlage für eine externe Datenverarbeitung erschweren, wenn nicht gar unmöglich machen. Es sollte jedoch zumindest versucht werden, die Kernpflichten der jeweils anwendbaren Vor-

827 Dies ist beispielsweise bei der Datenschutzkontrolle der Auftragnehmer von Krankenkassen bereits vielfach geübte und von den Aufsichtsbehörden akzeptierte Praxis.

schriften annähernd auf einen gemeinsamen Nenner bringen, um diesen dann in Form einer Checkliste oder auch Vertragsvorlage für die Forschungsgemeinschaft als Unterstützungsangebot zur Verfügung zu stellen.⁸²⁸

828 Wobei eine bundeseinheitliche Basis-Checkliste bzw. -Vertragsvorlage durch bundeslandspezifische Dokumente ergänzt werden könnte.