Krankenhausentgeltdaten-Nutzung verstößt gegen Datenschutzrecht

Krankenhausdienstleister BinDoc vermarktet illegal sensitive Patientendaten

Stand 27.06.2024

Thilo Weichert
weichert@netzwerk-datenschutzexpertise.de
Waisenhofstraße 41, 24103 Kiel
Karin Schuler
schuler@netzwerk-datenschutzexpertise.de
Kronprinzenstraße 76, 53173 Bonn
www.netzwerk-datenschutzexpertise.de

Inhalt

1 Zusammenfassung 3
2 Geschäftstätigkeit von BinDoc 3
3 Vorgebliche Anonymisierung 5
3.1 Datengrundlage 5
3.2 Verfahren 6
3.3 Anonymisierungsversuch 7
3.3.1 Entfernen von Feldern 9
3.3.2 Ersetzen durch Hashwert 9
3.3.3 Ersetzen durch Wertegruppen 10
3.4 Konsequenzen 11
4 Datenschutzanforderungen 12
4.1 Verantwortlichkeit 12
4.2 Datenherkunft und Zwecke 13
4.3 Zulässigkeit der Verarbeitung von §-21-Daten 14
4.3.1 Keine Einwilligung 15
4.3.2 Sperrwirkung des § 21 KHEntgG für eine Weiterverarbeitung 15
4.3.3 Insbesondere Forschungsnutzung 16
4.3.4 Berufliche Schweigepflicht/Patientengeheimnis 18
4.4 Weitere rechtliche Anforderungen 18
4.4.1 Insbesondere Transparenz 19
4.4.2 Insbesondere Datenschutz-Folgenabschätzung 19
5 Ergebnis 20
Abkürzungen 21

Der Informationstechnik-Dienstleister BinDoc mit Sitz in Tübingen wertet für Krankenhäuser deren Patientendaten aus, um Wirtschaftlichkeits- und Marktanalysen zur Angebotsoptimierung zu erstellen. Er nutzt und vermarktet diese Daten zudem, nachdem sie angeblich anonymisiert wurden, für eigene kommerzielle Marketing- und Forschungszwecke.

1 Zusammenfassung

Das Unternehmen BinDoc bietet Krankenhäusern die Analyse ihrer eigenen Falldaten auf Grundlage von Vergleichen mit den Falldaten anderer deutscher Krankenhäuser an. Durch jede Nutzung dieser Dienstleistung gewinnt nicht nur der jeweilige Krankenhaus-Kunde Erkenntnisse, auch BinDoc gewinnt durch jeden Krankenhaus-Kunden weiteres Material zur Verbesserung seiner Datenbank. Diese Datenbank wird nicht nur für Krankenhaus-Kunden zur Durchführung vergleichender Analysen genutzt, sie wird von BinDoc auch zu Forschungszwecken verwendet sowie Dritten zur Verfügung gestellt.

Die vermutete Rechtmäßigkeit und Datenschutzkonformität des Geschäftsmodells basiert vollständig auf der Annahme des Dienstleisters, dass er lediglich anonymisierte Falldaten erhält und verarbeitet, die nicht dem Geltungsbereich der Datenschutzgesetzgebung unterfallen. Das vorliegende Gutachten zeigt auf, dass diese Grundannahme unzutreffend ist. Daraus ergeben sich datenschutzrechtliche Anforderungen, die nicht erfüllt werden (können), weshalb die Dienstleistung insgesamt unzulässig ist.

2 Geschäftstätigkeit von BinDoc

Der 2013 gegründete Tübinger IT-Dienstleister BinDoc[1] ist auf die **Analyse von Krankenhausdaten** für Kliniken und für andere medizinische Bedarfsträger spezialisiert. Er betreibt und ergänzt hierfür kontinuierlich eine umfangreiche Datenbank, deren Inhalte er über seine cloudbasierte Analyseplattform „BinDoc Meta“ verfügbar macht. Über diese Plattform kann mittels unterschiedlicher Dienstleistungen („Tools“) auf die Datenbank zugegriffen werden, um deren Daten unter verschiedenen Gesichtspunkten auszuwerten und zu präsentieren. Die Daten werden laut Eigenauskunft sowohl für kommerzielle als auch für so genannte Forschungszwecke bereitgestellt. Gemäß eigenen Angaben handelt es sich bei der Datenbank um „die größte Forschungsplattform im deutschsprachigen Raum“.[2]

Das Geschäftsmodell des Unternehmens basiert auf einer Art **Schneeballsystem**: Krankenhäuser, die sich mit anderen vergleichen möchten, Anknüpfungspunkte für örtlich günstige Angebote finden wollen oder eigene Optimierungsmöglichkeiten suchen, versorgen bei der Nutzung der Datenbank von BinDoc diese gleichzeitig mit ihren eigenen Daten. Man kennt dieses System aus dem Personalbereich, wo Anbieter wie z.B. Willis Towers Watson Vergleichszahlen zu Gehaltsstrukturen gegen die Überlassung eigener Gehaltsdatensätze anbieten, die vorgeblich anonymisiert werden.

[1] Karlstraße 3, 72072 Tübingen, info@bindoc.de, Geschäftsführung: Markus Heider, Manuel Heurich, Sven Seemann, Tel: +49 7071 7543170, Amtsgericht Stuttgart HRB 784987. Alle Internetlinks wurden letztmalig am 09.05.2024 verifiziert.
[2] https://www.bindoc.de/unternehmen.

BinDoc nutzt für seine Dienstleistung die Tatsache aus, dass alle in Krankenhäusern eingesetzten **Krankenhausinformationssysteme** die gesetzlichen Anforderungen des Krankenhausentgeltgesetzes (KHEntgG) erfüllen müssen, wonach Falldatensätze gewissermaßen „auf Knopfdruck“ in einer gesetzlich normierten Form für ebenfalls klar definierte Bedarfsträger bereitgestellt werden müssen. Bei diesen Fallakten handelt es sich um höchst sensible Datensätze, die wesentliche, patientenbezogene Angaben zu jedem Krankenhausaufenthalt, dessen Ursachen und seinem Verlauf enthalten.

Die Zusammenstellung dieser Datensätze muss das jeweilige Krankenhaus für eigene Zwecke auslösen (Export) und anschließend mittels des von BinDoc bereitgestellten „Anonymisierungstools“ in eine vorgeblich anonymisierte Form überführen. Erst dann können eigene Auswertungen zur Organisations- und Wirtschaftlichkeitsbetrachtungen mithilfe der auf der Plattform bereitgestellten Auswertungstools genutzt werden. Gleichzeitig werden die eigenen Datensätze durch Überführung in die BinDoc-Datenbank für alle zukünftigen Kunden nutzbar gemacht. Der Zweck der Datenverarbeitung ist aus Sicht des Krankenhaus-Kunden demnach die **Durchführung von Analysen** der eigenen Daten. Aus Sicht des Anbieters findet zur Verarbeitungszeit zudem eine Zweckänderung statt, die der **Verbesserung der Datenbasis** und damit des eigenen kommerziellen Angebots dient. Da die Dienstleistung gegenüber dem Krankenhaus-Kunden qualitativ von der Anzahl vorhandener Vergleichsdatensätze abhängt (nur eine große Anzahl von Vergleichswerten erzeugt brauchbare statistische Ergebnisse), ist die Überführung möglichst vieler Datensätze aus Sicht des Unternehmens essenziell und eine Löschung nicht erwünscht.

BinDoc argumentiert in Bezug auf die **Datenschutzkonformität** ganz ähnlich wie die oben erwähnten Anbieter von Gehaltsanalysediensten: die fraglichen Daten seien durch das bereitgestellte Programm anonymisiert worden, ließen also keinerlei Personenbezug zu und unterfielen damit nicht mehr dem Datenschutzrecht. Allein für die Überführung der Fallakten in die behauptete anonymisierte Form der Daten hält das Unternehmen vermutlich das Konstrukt einer Auftragsverarbeitung für erforderlich, da die Überführung mittels einer durch BinDoc bereitgestellten Software für die Nutzung über Webbrowser stattfindet.

Das Unternehmen, das neben der Geschäftsführung ca. 13 Beschäftigte hat, ist gemäß eigenen Angaben **für ca. 300 Unternehmen** mit mehr als 2.000 Fachabteilungen tätig. Zu den Kunden und Geschäftspartnern gehören die deutschen Universitätskliniken von Heidelberg, Tübingen, Düsseldorf, Köln, Dresden und Schleswig-Holstein (Kiel, Lübeck), die Sana-, die Artemed- und die Agaplesion-Kliniken sowie viele weitere Krankenhäuser. In der „**Forschungs- und Benchmarking-Datenbank**“ des Unternehmens sind gemäß eigenen Angaben ca. 17 Millionen Behandlungsfälle gespeichert, wodurch „20 Prozent des gesamten deutschen stationären Patientenvolumens … über die Stichprobe in der Forschungsdatenbank repräsentiert“ würden. In die Analyse können, so die Selbstdarstellung, auch 130.000 ambulant tätige Ärzte einbezogen werden. Gespeichert seien Daten von insgesamt ca. 2.400 Krankenhäusern.

BinDoc führt **nicht nur für Krankenhäuser** Markt- und Wirtschaftlichkeitsanalysen durch, sondern auch für Medizintechnikunternehmen (Siemens Healthineers, Olympus, Abbott, Stryker, Intuitive Surgical, Boston Scientific), für Pharmaunternehmen sowie selbst für im Gesundheitsbereich tätige Banken (z.B. deutsche apotheker- und ärztebank). Analyseaufträge erfolgten zudem u.a. durch das

Bundesministerium für Gesundheit, das Ministerium für Justiz und Gesundheit Schleswig-Holstein und das Bayerische Staatsministerium für Gesundheit und Pflege.

Gemeinsam mit seiner Muttergesellschaft Oberender AG, dem Marktführer im Klinik- und Krankenhausmanagement in Deutschland, wurde BinDoc vom **Bundesministerium für Gesundheit** damit beauftragt, die Auswirkungsanalyse der Krankenhausreform auf die Versorgungsituation in Deutschland zu simulieren. Auf Basis dieser Simulation im Dezember 2022, so die Unternehmenswerbung, wurde von der auf Bundesebene eingesetzten Regierungskommission für eine moderne und bedarfsgerechte Krankenhausreform die Stellungnahme und Empfehlung „Grundlegende Reform der Krankenhausvergütung“ vorgelegt.[3]

Auch bei sonstigen Projekten kooperiert BinDoc mit seiner Muttergesellschaft.[4] Als weitere **Kooperationspartner** gibt BinDoc die ZEQ in Mannheim und Curacon mit Hauptsitz in Münster an, sowie die allgemeinen Unternehmensberatungsfirmen PD – Berater der öffentlichen Hand, Boston Consulting Group, Deloitte und KPMG. Als weitere Partner genannt werden der Bundesverband Medizintechnologie, der Verband der Krankenhausdirektoren Deutschlands e.V. und der Bundesverband Deutscher Privatkliniken e.V.

Mit seiner Forschungsdatenbank, so BinDoc, werden **Studien für die Pharmaindustrie** durchgeführt, um „das Marktvolumen und die Epidemiologie besser zu verstehen“. Dabei würden die klinischen Daten mit Informationen zur Bevölkerungsentwicklung und -struktur komplettiert. Hierfür betreibt BinDoc zusätzlich ein rechtlich nicht selbständiges „Institut für angewandte klinische Forschung“.[5]

Für 2022 weist das Unternehmen eine **Bilanzsumme** von über 1,2 Mio. Euro und einen Gewinn von über 240.000 Euro aus.[6]

Das Unternehmen BinDoc sowie dessen Datenschutzbeauftragter wurden vom Netzwerk Datenschutzexpertise mit Datum vom 24.03.2024 mit einem umfangreichen Fragenkatalog zur Datenverarbeitung und deren Rechtmäßigkeit angeschrieben. Mit Datum vom 12.04.2024 wurde noch einmal an diese Anfrage erinnert. Beide **Anfragen wurden nicht beantwortet**. Die folgende Bewertung beruht daher ausschließlich auf allgemein verfügbaren Informationen.

3 Vorgebliche Anonymisierung

3.1 Datengrundlage

Grundlage der von BinDoc vorgenommenen Verarbeitung sind Daten, die das Krankenhaus gemäß § 21 KHEntgG verarbeiten muss.

Zu jedem Krankenhausfall müssen nach § 21 Abs. 2 Nr. 2 KHEntgG von den Krankenhäusern dem Institut für das Entgeltsystem im Krankenhaus GmbH (InEK) neben den Angaben zur Einrichtung und

[3] https://www.bindoc.de/reformanalyse-bund.
[4] https://oberender.com/research/op-live-tool/.
[5] https://www.bindoc.de/klinische-forschung.
[6] https://www.northdata.de/BinDoc+GmbH,+T%C3%BCbingen/Amtsgericht+Stuttgart+HRB+784987.

zur Krankenkasse die Krankenversichertennummer (unveränderbarer Teil gem. § 290 Abs 1 S. 2 SGB V) detaillierte **Angaben zur Person und zur behandelten Krankheit** bereitgestellt werden und zwar

d) Geburtsjahr und Geschlecht des Patienten sowie die Postleitzahl und der Wohnort des Patienten, in den Stadtstaaten der Stadtteil, bei Kindern bis zur Vollendung des ersten Lebensjahres außerdem der Geburtsmonat,
e) Aufnahmedatum, Aufnahmegrund und -anlass, aufnehmende Fachabteilung, bei Verlegung die der weiter behandelnden Fachabteilungen, und der dazugehörigen Zeiträume, Zeiträume der Intensivbehandlung, Entlassungs- oder Verlegungsdatum, Entlassungs- oder Verlegungsgrund, bei Kindern bis zur Vollendung des ersten Lebensjahres außerdem das Aufnahmegewicht in Gramm,
f) Haupt- und Nebendiagnosen sowie Datum und Art der durchgeführten Operationen und Prozeduren nach den jeweils gültigen Fassungen der Schlüssel nach § 301 Abs. 2 Satz 1 und 2 des Fünften Buches Sozialgesetzbuch, einschließlich der Angabe der jeweiligen Versionen, bei Beatmungsfällen die Beatmungszeit in Stunden entsprechend der Kodierregeln nach § 17b Abs. 5 Nr. 1 des Krankenhausfinanzierungsgesetzes und Angabe, ob durch Belegoperateur, -anästhesist oder Beleghebamme erbracht,
g) Art aller im einzelnen Behandlungsfall abgerechneten Entgelte,
h) Höhe aller im einzelnen Behandlungsfall abgerechneten Entgelte.

In diesem Gutachten werden diese von den Krankenhäusern für Zwecke des § 21 KHEntgG erfassten und von den Krankenhäusern gespeicherten Daten kurz „**§-21-Daten**“ genannt.

3.2 Verfahren

BinDoc gibt an, dass die von den Krankenhäusern übermittelten Daten vor einer eigenverantwortlichen Weiterarbeitung durch das jeweilige Krankenhaus mithilfe eines von BinDoc bereitgestellten Programms hinreichend anonymisiert würden. Dies entspringt recht offensichtlich dem Wunsch, den **Anwendungsbereich des Datenschutzrechts zu verlassen** und die eingesammelten Daten so einfach für das eigene Dienstleistungsmodell nutzbar zu machen.

Von der tatsächlichen und fachgerechten Konzeptionierung und Durchführung der behaupteten Anonymisierung hängt demnach die **Rechtmäßigkeit des gesamten Dienstleistungsmodells** ab. Ein Angriffsszenario, das die Identifizierung einzelner Personen beinhaltet (gezielt oder zufällig) darf nicht existieren. Daher stellt die Anonymisierung großer Datenmengen mit umfangreichen, sehr sensiblen Einzeldatensätzen keine triviale Aufgabe dar. Sowohl die Wahl der Anonymisierungsmethoden als auch die Überprüfung der Sicherheit der Ergebnisse verlangen ein ausreichendes Verständnis der Datenstruktur und der inhärenten Personenbezüge.

BinDoc stellt dem Auftraggeber, also dem verantwortlichen Krankenhaus, im Rahmen seiner Dienstleistung ein **browserbasiertes Programm** bereit, mit dessen Hilfe das Krankenhaus die aus seinem Verwaltungsprogramm exportierten Falldaten in seinem eigenen Verantwortungsbereich anonymisieren soll. Der resultierende Datenbestand, nunmehr angeblich anonymisiert, wird vom Kunden über eine gesicherte Datenverbindung an BinDoc übertragen. Dort werden sie einerseits zur Durchführung der vom Kunden gewünschten Analysen verwendet als auch dauerhaft im Datenbestand der BinDoc abgelegt.

Hinsichtlich der **beauftragten Analysen** kann das Krankenhaus innerhalb der Software zwischen verschiedenen Fragestellungen und Detaillierungsgraden wählen. In der Software stehen unter

anderem Funktionalitäten zu Durchführung von Prognosen, Potenzialanalysen, Geo-Analysen, Einweiseranalysen, Benchmarking (zu Kennzahlen und DRGs) und Wettbewerbsanalysen zur Verfügung.[7] Durch diese Bestimmungsmacht der Auswertung der eigenen Daten ist eine Verantwortlichkeit des Krankenhauses gemäß Art. 4 Nr. 7 DSGVO für die Durchführung der gewünschten Analysen gegeben.

BinDoc beschreibt die **Datenverarbeitung**, wonach sowohl bei der Übertragung (data in transit) als auch in der Datenbank (data at rest) die Daten durch sachgerechte und sicher gestaltete Verschlüsselung geschützt würden. Die Schlüsselverwaltung für data at rest befände sich in den Händen des Unternehmens selbst. Die Speicherung erfolge auf „Servern in Deutschland (Frankfurt) bei Microsoft Ireland Operations Ltd, mit der vorsorglich (trotz Anonymisierung) ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO bzw. SCC - Standardvertragsklauseln geschlossen wurde“.[8]

Die nach diesem Programm **zu übertragenden Datensätze** werden von BinDoc eindeutig vorgegeben mit 56 Variablen (Merkmalen) zu jedem Behandlungsfall.

Die **Weiterverarbeitung** der angeblich anonymisierten Daten für sekundäre Zwecke, also zur Vornahme von Analysen für oder zur Weitergabe an Dritte liegt – auch nach Darstellung von BinDoc – in der ausschließlichen Verantwortlichkeit dieses Unternehmens.

3.3 Anonymisierungsversuch

Voraussetzung für eine rechtlich wirksame **Anonymisierung** ist, dass ein **Personenbezug beseitigt** wird. Die Anonymisierung hätte zur Folge, dass die Daten aus dem Geltungsbereich des Datenschutzrechts fallen und demnach keine datenschutzrechtlichen Restriktionen bei der Verarbeitung beachtet werden müssen.

Anonymisieren bedeutet das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder **bestimmbaren natürlichen Person zugeordnet** werden können.[9]

Der Begriff der Anonymisierung wird im Normtext der **DSGVO** nicht verwendet.[10] In ErwGr 26 S. 5, 6 DSGVO wird im Rahmen der Definition des Begriffs „personenbezogene Daten“ darauf hingewiesen, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten, also *„für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.“*

[7] https://help.bindoc.de/dokumentation.
[8] BinDoc, https://help.bindoc.de/dokumentation-analytics-anonymisierte-verarbeitung-von-datensaetzen (künftig zitiert als Verfahrensbeschreibung - Fn. 8), Kap. 3, 4.2.
[9] So § 3 Abs. 6 BDSGaF; Stiftung Datenschutz (Hrsg.), Anonymisierung und Pseudonymisierung von Daten, 2023, S. 6 f. (Kap. 2.4.2).
[10] Hansen in Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 4 Nr. 5 Rn. 11; Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 3. Aufl. 2024, Art. 4 Rn. 74.

Technisch wird Anonymität als ein Zustand definiert, bei dem ein einzelnes Subjekt innerhalb einer bestimmten Gesamtmenge von Subjekten (der so genannten Anonymitätsmenge) nicht identifizierbar ist.[11] In dieser Definition ist bereits erkennbar, dass die Anonymität eines Datensatzes nicht notwendig absolut ist, sondern von der betrachteten, verfügbaren Menge der Vergleichsdaten abhängt. Denkbare Angriffskategorien können aus dieser Definition ebenfalls erahnt werden: Die Identifizierbarkeit einer Person, deren Name oder andere Merkmale aus einem Datensatz entfernt wurden, und die Wirksamkeit der damit beabsichtigten Anonymisierung hängen nicht nur von der Art der Behandlung dieses einen Datensatzes ab, sondern auch von Struktur und Inhalt der zur Verfügung stehenden **Vergleichsmenge**. Da große Datensammlungen nicht in jedem Fall und quasi automatisch zu besseren Anonymisierungsergebnissen führen (etwa weil die Einzeldaten in der Masse „untergehen"), ist das Verständnis für die Veränderung von Anonymisierungsergebnissen bei der Veränderung der Datenbasis und der Anonymitätsmenge entscheidend für die wirksame Gestaltung eines Anonymisierungsvorgangs.

Ob eine Anonymisierung wirksam ist oder ob doch eine personenbezogene Zuordnung gelingen kann, hängt von den Erkenntnisquellen ab, die sowohl der verantwortlichen Stelle als auch jedem anderen Empfänger als **Zusatzwissen direkt oder indirekt zur Verfügung** stehen bzw. stehen können.[12] Dabei kann es sich beispielsweise um Zusatzwissen aus anderen Quellen, aus (zufälliger) eigener Kenntnis oder um aus der Anonymitätsmenge selbst ableitbares Zusatzwissen handeln.

Für die Annahme der **Verfügbarkeit des Zusatzwissens** genügt die theoretische Möglichkeit. Relevant ist, ob das Zusatzwissen vernünftigerweise bei einer Einheit der verarbeitenden Stelle verfügbar sein kann.[13] Nicht beachtlich ist, dass diese Möglichkeit nicht in Anspruch genommen werden soll oder will. Wenn identifizierende Kerndaten (Name, Vorname, Kennnummer etc.) eines Personen-Datensatzes gelöscht werden, kann es gleichwohl möglich sein, über die Kombination oder Struktur weiterer Merkmalsdaten eine Zuordnung zu einer bestimmten Person vorzunehmen. Eine absolute Anonymisierung ist bei hochkomplexen und umfangreichen Datensätzen zumeist praktisch nicht möglich. Umso wichtiger ist es, dass eine Anonymisierung unter Berücksichtigung vorhandener wissenschaftlicher Erkenntnisse und Methoden vorgenommen wird. Wenn das Zusatzwissen nur unter einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft beschafft werden kann, genügt dies für die Anonymisierung. Hierbei ist ein objektiver Maßstab anzulegen: es reicht nicht, wenn der Aufwand nur für die speichernde Stelle unverhältnismäßig ist; auch mögliche andere Empfänger und potenziell interessierte Angreifer sind bei der Aufwandsbetrachtung zu berücksichtigen.[14]

Identifizierbarkeit ist demnach nicht relativ oder subjektiv, sondern objektiv zu bestimmen. Verfügt eine verarbeitende Stelle nicht über eigene Zuordnungsmöglichkeiten, wohl aber eine **andere Stelle oder Person**, sind die Datensätze personenbezogen.[15]

---

[11] Vgl. Hansen, Pfitzmann, A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity and Identity Management, 2010, S. 9ff.
[12] Anders noch BFH, NJW 1994, 2247 = RDV 1995, 32, der meinte, dass Re-Identifizierung durch Branchenkenntnisse für eine Behandlung von Daten unschädlich ist.
[13] Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, S.10.
[14] Kühling/Klar in Kühling/Buchner, DS-GVO BDSG, 4 Aufl. 2024, Art. 4 Nr. 1 Rn. 32; Weichert in Däubler u.a. (Fn. 10), Art. 4 Rn. 75; Stiftung Datenschutz (Fn. 9), S. 28 ff.
[15] EuGH 19.10.2016 – C-582/14 (IP-Adressen) Rn. 43, 45, NJW 2016, 3579; Weichert in Däubler/Wedde/Weichert, Sommer (Fn. 10), Art. 4 Rn. 19.

BinDoc beschreibt sein Vorgehen bei der „Anonymisierung“ in seiner Verfahrensbeschreibung.[16]

Demnach werden im Wesentlichen drei sehr einfache Verfahren eingesetzt.

1. Einige Datenfelder werden ersatzlos aus dem Datensatz entfernt.
2. Einige Datenfelder werden durch einen Hashwert ersetzt.
3. Einige Datenfelder werden durch Kategorisierung in Wertegruppen (Kohorten) übertragen.

3.3.1 Entfernen von Feldern

Die **ersatzlose Entfernung** von Datenfeldern betrifft ausschließlich solche, die für die Dienstleistung nicht benötigt werden, wie z.B. so genannte Prozedurangaben zu Belegoperateur oder Beleganästhesist. Eine Motivation zur Anonymisierung aus persönlichkeitsschützenden Gründen ist bei diesen Feldern nicht zu erkennen. Die Entfernung der benannten Felder (die nicht gleichzeitig einer der beiden im Folgenden beschriebenen Verfahren unterfallen) leistet weder positiv noch negativ einen Beitrag zu einer beabsichtigten Anonymisierung.

3.3.2 Ersetzen durch Hashwert

Einige, sehr eindeutig identifizierende Felder werden durch einen **Hashwert ersetzt**. Dies betrifft vor allem die Krankenversichertennummer (Versicherten-ID) sowie eine krankenhausinterne, patientenbezogene Fallnummer. Hierüber werden jeweils Hashwerte erstellt und zur Übermittlung in den Falldatensatz übernommen, um eine „eindeutige Zuordnung zwischen Datensätzen (z.B. Löschen von alten Datensätzen bei erneutem Upload)“ vornehmen zu können.[17]

Durch das Anwenden einer Hashfunktion auf ein Datenfeld wird dessen Eintrag in eine (für natürliche Personen kryptisch scheinende) Zeichenkette überführt. Ein direkter Rückschluss aus dieser Zeichenkette auf den ursprünglichen Inhalt des Datenfeldes ist nicht möglich. Zur Anonymisierung sind Hashfunktionen dennoch nicht geeignet, weil sie für eine bestimmte Eingabe (z.B. eine Krankenversicherten-Nr.) **immer den gleichen Hashwert** erzeugen. Vereinfacht dargestellt kann man in einer großen Datenbank mit gehashten KV-Nummern nach einem Datensatz der Nachbarin suchen, deren Krankenversichertennummer man kennt. Man muss nur seinerseits deren KV-Nummer hashen und nach dem Resultat in der Datenbank suchen. Der Datensatz, bei dem man fündig wird, gehört zur Nachbarin.

Jeder Einzeldatensatz enthält zudem eine Vielzahl weiterer **Diagnose- und Behandlungsdaten**. Liegt nur ein weiteres Merkmal vor, kann von einer sicheren Zuordnung ausgegangen werden. Die Verfügbarkeit solcher Daten beschränkt sich eben nicht auf das Krankenhaus, sondern geht darüber hinaus und erstreckt sich z.B. auf Familienangehörige, Freunde und Bekannte, vor- und nachbehandelnde Gesundheitseinrichtungen. Das Zusatzwissen kann in Selbsthilfegruppen ausgetauscht worden sein oder auch durch einen geleakten Arztbrief. Hierüber lässt sich dann nicht nur ein konkreter Behandlungsfall zuordnen, sondern lassen sich sämtliche in der Datenbank über die gehashte Patienten-ID diesen betreffende Behandlungsfälle zuordnen. Patientenbezogen kann somit

[16] https://help.bindoc.de/dokumentation-analytics-anonymisierte-verarbeitung-von-datensaetzen.
[17] BinDoc, Verfahrensbeschreibung (Fn. 8), Kap. 4.3, 4.4, 5.

bei der von BinDoc geführten Datenbank nicht von einer ausreichenden Anonymisierung gesprochen werden.

Bei der BinDoc GmbH könnten Patientendaten inklusive der Hashwerte durch **eine Datenpanne** unbeabsichtigt öffentlich bekanntwerden. Wie oben bereits exemplarisch beschrieben, können Dritte allein durch „Ausprobieren“ bekannter Versicherten-IDs oder krankenhausinterner Kennzeichen auf Patienten rückschließen und so deren Falldaten eindeutig zuordnen. Rückschlüsse sind je nach Angriffsszenario – beispielsweise unter Verwendung von Rainbow-Tables – auch im großem Umfang möglich.

Angriffsszenarien, bei denen ein möglicher Angreifer **Insiderwissen** über den genauen Einsatz des Hash-Algorithmus hat (z.B. Verwendung eines Salts), würden noch schneller zum Ziel führen, wenn die Falldaten einer gegebenen Person gesucht werden sollen.

Im Ergebnis ist festzustellen, dass eine wirksame Anonymisierung durch die Verwendung von Hashwerten für stark identifizierende Feldinhalte nicht stattfindet, weil die Möglichkeiten zur eindeutigen Zuordnung von Daten zu einer Person nicht wirksam ausgeschlossen werden und in zahlreichen Angriffsszenarien das Risiko der Zuordnung gehashter Daten zu Personen besteht. Bestenfalls kann die Ersetzung durch gehashte Werte als **Verschleierung durch Pseudonymisierung** bezeichnet werden. Man hat es dann jedoch nach wie vor mit personenbezogenen Daten zu tun, die unter den Geltungsbereich der DSGVO und anderer Datenschutzbestimmungen fallen.

3.3.3 Ersetzen durch Wertegruppen

Einige Datenfelder werden durch verallgemeinerte Daten einer so genannten Merkmalsgruppe ersetzt. Dies betrifft insbesondere die Datenfelder „Geburtsjahr“ und „Geburtsmonat“. Diese beiden werden selbst nicht übertragen, sondern zunächst einer **Kohortenzuordnung** unterzogen und so in einem Feld „Altersgruppe“ abgelegt. Diese Kohorten sind allerdings derart engmaschig gestaltet (5-Jahres-Intervalle), dass keine besonders starke Verschleierung stattfindet. In technisch gleicher Weise wird scheinbar (unklare Darstellung in der Verfahrensbeschreibung) ein Feld zur Kennzeichnung der versichernden Krankenkasse durch ein Kennzeichen ersetzt, das nur die Werte „gesetzlich“ oder „privat“ annimmt.

Auch nach diesen Ersetzungen lässt sich eine Zuordnung zu einer Person **mit geringem Zusatzwissen** vornehmen. Zu einer Person sind im Einzeldatensatz folgende Identifizierungsangaben verfügbar: Geschlecht, Krankenkassenart, Postleitzahl/Landkreis, Altersgruppe (5-Jahres-Cluster), Diagnoseangaben. Allein diese Angaben genügen in einigen Fällen, um eine eindeutige Zuordnung vorzunehmen, ohne dass ein weiteres Zusatzwissen nötig ist. Kommt als weiteres Zusatzwissen das Krankenhaus oder gar der konkrete Standort bzw. die Fachabteilung hinzu, so ist in sehr vielen Fällen eine eindeutige Zuordenbarkeit gegeben. Und auch die durch Wertegruppen ersetzten Daten „Alterskohorte“ und „Versicherungsart“ erleichtern in derartigen Kombinationen die personenbezogene Zuordnung fast so gut wie die Originaldaten.

3.4 Konsequenzen

BinDoc behauptet, dass die Verarbeitung in eigener Verantwortung ausschließlich **mit anonymisierten Daten** erfolgen würde. Diese Aussage ist falsch.

Schon die für jedermann ohne Authentifizierung auf der öffentlichen Website des Unternehmens angebotenen Auswertungen, z.B. nach der kleinzelligen lokalen Verteilung jedes beliebigen ICD-Schlüssels mit Aufschlüsselung von Geschlecht, Klinik etc. lassen eine fachgerechte, echte Anonymisierung sehr unwahrscheinlich erscheinen. Wie oben beschrieben, sind die gewählten Methoden ungeeignet, eine wirksame Anonymisierung durchzuführen. Neben den beschriebenen Möglichkeiten der Identifizierung von Personen, auch auf Grundlage des durch BinDoc transferierten Datensatzes werden weitere Formen von Zusatzwissen offensichtlich gar nicht bedacht, die zur Identifikation von Personen führen. So werden beispielsweise **OPS-Daten** (zu Operationen und sonstigen ärztlichen Prozeduren) weder verschleiert noch gelöscht. Und so kann aus dem Datum geburtshilflicher Prozeduren (OPS-Datum) auf den genauen Geburtstag von Neugeborenen geschlossen werden. Diese Informationen ermöglichen verbunden mit der Angabe zur Einrichtung schon allein eine präzise Datensatzzuordnung zu den beteiligten Personen (Mutter und Kind).

Von einer Möglichkeit zur Identifizierung durch Zusatzwissen ist nicht nur auszugehen, wenn dieses Wissen bei BinDoc selbst vorliegt. Es reicht, wenn die für Zuordnungen nötigen Kenntnisse bei Empfängern der vermeintlich anonymisierten Daten vorliegen. Sind diese **Dritten** nach allgemeinem Ermessen in der Lage, einen Personenbezug herzustellen, so ist dieser anzunehmen.[18] Da Empfänger von BinDoc-Daten offenbar auch Forschende sind, die Zugriff auf weitere behandlungsrelevante Gesundheitsdaten haben können, muss man die Möglichkeit einer Identifizierung aufgrund der unzureichenden technischen Schutzmaßnahmen annehmen.

Da die gewählten Methoden und Prozesse keine wirksame Anonymisierung sicherstellen, stellt die Übergabe der (nicht wirksam anonymisierten) Daten durch den Krankenhaus-Kunden an BinDoc eine **Übermittlung im Sinne des Datenschutzrechts** dar. Mit dieser Übermittlung geht eine – gegenüber der ursprünglichen Krankenhaus-Auswertung – Zweckänderung einher. Das Datenschutzrecht ist demnach anzuwenden und für alle durch BinDoc vorgenommenen Verarbeitungen und Übermittlungen sind die üblichen datenschutzrechtlichen Sachverhalte zu prüfen.

Dazu gehören insbesondere:

- die datenschutzrechtliche Rolle von BinDoc,
- die Rechtsgrundlagen für die Verarbeitungen und die Zweckänderungen,
- die Notwendigkeit einer Datenschutzfolgeabschätzung wegen des hohen Risikos für die Betroffenen,
- die Umsetzung des Transparenzgebots, insbesondere die Information der Betroffenen nach Art. 13 DSGVO.

Diese Fragen werden im Folgenden erörtert.

[18] Klar/Kühling in Bühling/Buchner (Fn. 14), Art. 4 Nr. 1 Rn. 27, vgl. ErwGr 26 S. 3 DSGVO.

4 Datenschutzanforderungen

4.1 Verantwortlichkeit

Zwecks Zuweisung **datenschutzrechtlicher Pflichten** muss die Rolle des Verantwortlichen eindeutig bestimmt sein. Es ist daher zu klären, in welcher datenschutzrechtlichen Rolle BinDoc erstens die Daten seiner Kunden für deren Zwecke bearbeitet und zweitens seinem eigenen Datenbestand für eigene Zwecke hinzufügt.

Zu prüfen ist, zumindest für die Analysen im Auftrag des Kunden, das Vorliegen einer **Auftragsverarbeitung** gemäß Art. 28 DSGVO.

Gemäß Art. 28 DSGVO ist die **Datenweitergabe eines Verantwortlichen an einen Auftragsverarbeiter** (Art. 4 Nr. 8 DSGVO) zulässig, soweit der Auftragsverarbeiter „geeignete technische und organisatorische Maßnahmen“ ergreift, um den Schutz der Betroffenenrechte zu gewährleisten (Art. 28 Abs. 1 DSGVO) und dies auf der Grundlage eines Vertrags erfolgt, „in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind“ (Art. 28 Abs. 3 S. 1 DSGVO). Der Vertrag muss insbesondere Weisungsrechte des Verantwortlichen festlegen (Art. 28 Abs. 3 S. 2 lit. a u. h DSGVO).

Nicht als Auftragsverarbeiter, sondern als **Verantwortlicher** gilt, der „die Zwecke und Mittel der Verarbeitung bestimmt“ (Art. 28 Abs. 10 DSGVO). Art. 4 Nr. 7 DSGVO definiert den „Verantwortlichen“ damit, dass er „über die Zwecke und Mittel“ der Datenverarbeitung entscheidet. Erfolgt diese Entscheidung in Bezug auf einen konkreten Verarbeitungsschritt nicht durch eine Stelle allein, sondern durch zwei oder mehrere Stellen, so besteht eine in Art. 26 DSGVO geregelte „gemeinsame Verantwortlichkeit“.[19]

Bei der Erstellung des Gutachtens lag dem Netzwerk Datenschutzexpertise kein Auftragsvertrag i.S.v. Art. 28 Abs. 3 DSGVO vor. Auf der **Webseite von BinDoc** werden in der Verfahrensbeschreibung Angaben gemacht, die so interpretiert werden können, dass für die Dienstleistung der Analyse eigener Daten der datenschutzrechtlich verantwortliche Krankenhaus-Kunde eine Auftragsverarbeitung durch die Firma BinDoc als Auftragnehmer begründet.[20] Es wird allerdings auf der Website nicht explizit dokumentiert, dass die Dienstleistung im Rahmen einer Auftragsverarbeitung erfolgen soll und ein entsprechender Vertrag geschlossen wid. Dies irritiert insofern, als auf den Vertragsschluss mit Microsoft als Auftragsverarbeiter durchaus und ausdrücklich hingewiesen wird.

Da die Angaben bezüglich **technisch-organisatorischer Schutzmaßnahmen** in der Verfahrensbeschreibung von BinDoc lediglich Einzelaspekte erfassen, muss bezweifelt werden, dass

[19] EuGH 05.06.2018 – C-210/16 (Wirtschaftsakademie) Rn. 28, 43, NJW 2018, 2537; EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas) Rn. 68, NJW 2019, 285; EuGH 29.07.2019 – C-40/17 (Fashion-ID), NJW 2019, 2755; EuGH 05.12.2023 – C-683/21 (Gesundheitsministerium Litauen) Rn. 40, NJW 2024, 348; EuGH 07.03.2024 – C-604/22 (IAB Europe), Rn. 59; vgl. EuGH 05.12.2023 – C-683/21 Rn. 45 f.
[20] BinDoc, Verfahrensbeschreibung (Fn. 8).

diese den Anforderungen des Art. 28 Abs. 1 DSGVO genügen. Dies gilt insbesondere für den dort geforderten Schutz der Betroffenenrechte.

Weisungs- und Kontrollrechte in Bezug auf die konkrete Realisierung der Zwecke gegenüber BinDoc sind aus der Verfahrensbeschreibung nicht erkennbar und werden von BinDoc offenbar auch nicht eingeräumt. So liegen sämtliche technischen Gestaltungen, wie beispielsweise die Verschlüsselung der Daten bei der Übermittlung ausschließlich in der Verantwortung von BinDoc.

Spätestens mit dieser Übermittlung bestimmt demnach BinDoc die „Zwecke und Mittel dieser Datenverarbeitung" (Art. 4 Nr. 7 DSGVO), so dass ab da **BinDoc ebenfalls als Verantwortlicher** zu behandeln ist (Art. 28 Abs. 10 DSGVO).[21] Durch die Kenntnis des Krankenhauses und dessen Billigung der Datenweitergabe an BinDoc teilt das Krankenhaus die Verantwortung mit BinDoc.

Es liegt insofern für die eigentliche Dienstleistung (Durchführung von Analysen für den Kunden) weder eine ausschließliche Verantwortung des Krankenhauses noch eine Auftragsverarbeitung durch BinDoc vor, sondern eine **gemeinsame Verantwortlichkeit gemäß Art 26 DSGVO.** Dass den Anforderungen des Art. 26 DSGVO entsprochen würde (Vereinbarung u.a. zu Informationspflichten, Betroffenenrechten), ist nicht erkennbar.

Für die Überführung der Daten durch BinDoc in den eigenen Bestand und deren Verwendung für eigene kommerzielle Zwecke kann wegen der alleinigen Bestimmung über die Art und Weise der Verarbeitung nur das Vorliegen einer **eigenen Verantwortlichkeit** angenommen werden, was den Kunden als Datenlieferanten allerdings nicht davon entbindet, für die Übermittlung der Daten an BinDoc zur Weiternutzung eine Rechtsgrundlage zu identifizieren.

4.2 Datenherkunft und Zwecke

Angesichts des Umstands, dass der Ursprung der Falldatensätze rechtlich in **§ 21 KHEntgG** begründet und geregelt ist, stellt sich die Frage nach der Rechtmäßigkeit von deren Nutzung durch BinDoc.

Die Quellen für die BinDoc Datenbank mit den stationären Falldaten sind Krankenhäuser. Diese müssen gemäß § 21 KHEntgG detailliert Daten zu allen Behandlungsfällen erheben und für die Auswertung jährlich einer Datenstelle, nämlich dem „**Institut für das Entgeltsystem im Krankenhaus GmbH**" (InEK), bereitstellen. Das InEK bereitet die Daten auf und stellt ihre Ergebnisse dem Bundesministerium für Gesundheit (BMG) sowie den für die Krankenhausplanung zuständigen Landesbehörden zur Verfügung (§ 21 Abs. 3 S. 4, 5 KHEntgG). Das InEK analysiert zum Zweck der Weiterentwicklung der Entgeltsysteme im Vierteljahresrhythmus von den Krankenhäusern übermittelte Daten (§ 21 Abs. 3b KHEntgG). Es veröffentlicht selbst anonymisiert Ergebnisse auf seiner Webseite (§ 21 Abs. 3 S. 6 KHEntgG).

Das **Bundeskartellamt** erhält im Bedarfsfall bestimmte Daten aus dem §-21-Datenbestand für konkrete Fusionskontrollverfahren (§ 21 Abs. 3 S. 8 KHEntgG). Dem „**Institut für Qualitätssicherung und Transparenz im Gesundheitswesen**" (IQTiG) werden Daten aus diesem Bestand für Zwecke der Qualitätssicherung bereitgestellt (§ 21 Abs. 3a KHEntgG).

[21] Stiftung Datenschutz (Fn. 9), S. 41.

Außerdem können der Spitzenverband Bund der Krankenkassen, der Verband der privaten Krankenversicherung und die Deutsche Krankenhausgesellschaft **Begleitforschung** zu den Auswirkungen des neuen Vergütungssystems ausschreiben und durchführen lassen, wobei die Auswertung der §-21-Daten vom InEK durchzuführen ist (§ 21 Abs. 3 S. 9 KHEntgG i. V. m. § 17b Abs. 8 Krankenhausfinanzierungsgesetz – KHG).

Für die oben genannten Zwecke müssen die Krankenhäuser zusätzlich zu den unter 3.1 genannten personenbezogenen Falldaten umfangreich **Strukturdaten der jeweiligen Einrichtung** zur Verfügung stellen, u.a. zu Art, Trägerschaft, (Intensiv-)Betten, Ausbildungsplätze und weitere Angaben zur Ausbildung, DRG-Fälle, Pflegepersonal (§ 21 Abs. 2 Nr. 1 KHEntgG).

Im Interesse des Datenschutzes gelten hinsichtlich der Personenbeziehbarkeit und der **Zweckbindung** der Daten nach § 21 KHEntgG strenge Regelungen: „Nach Abschluss der Plausibilitätsprüfung darf die Herstellung eines Personenbezugs nicht mehr möglich sein“ (§ 21 Abs. 3 S. 2 u. Abs. 3b S. 4 KHEntgG). Andere als die „genannten Verarbeitungen sind unzulässig“ (§ 21 Abs. 3 S. 9 u. Abs. 3b S. 10 KHEntgG). Auch die Nutzung der vom InEK zusammengefassten „veröffentlichten Daten durch Dritte ist ausschließlich zu nicht-kommerziellen Zwecken zulässig“ (§ 21 Abs. 3 S.3 u. Abs. 3b S. 6 KHEntgG).

Gemäß § 21 Abs. 4 KHEntgG vereinbaren der Spitzenverband Bund der Krankenkassen, der Verband der privaten Krankenversicherung und die Deutschen Krankenhausgesellschaft im Benehmen mit dem Bundesbeauftragten für den Datenschutz und dem Bundesamt für die Sicherheit in der Informationstechnik die weiteren Einzelheiten der Datenübermittlung. In dieser „**Vereinbarung über die Übermittlung von DRG-Daten** nach § 21 Abs. 4 und Abs. 5 KHEntgG“ vom 01.01.2007[22] wird in § 2 Abs. 2 nochmals betont: „Die Datenschutzanforderungen des § 21 KHEntgG sind einzuhalten.“ Ausführungen über die Nutzung der §-21-Daten durch die Krankenhäuser finden sich in der Vereinbarung nicht. In einer Anlage findet sich eine detaillierte Darstellung des Datensatzes.[23] Die Übermittlung der Datensätze muss verschlüsselt erfolgen.[24]

4.3 Zulässigkeit der Verarbeitung von §-21-Daten

Die Regelung des § 21 KHEntgG hat für die Sekundärnutzung durch BinDoc Relevanz. § 21 KHEntgG regelt gemäß seinem Wortlaut ausschließlich die **Übermittlung der erfassten Daten an das InEK** sowie die weitere Nutzung dieser Daten durch das InEK und weitere, im Gesetz explizit aufgeführte Datenempfänger, **nicht aber die Nutzung dieser Daten durch das Krankenhaus selbst oder durch Dritte**. Wohl aber enthält § 21 KHEntgG detaillierte Vorgaben zur Anonymisierung und zur Zweckbindung. Damit bringt der Gesetzgeber nicht nur die hohe Sensitivität der Daten zum Ausdruck, sondern macht präzise Vorgaben, wie mit diesen Daten umzugehen ist.

[22] https://www.g-drg.de/content/download/245/file/Vereinbarung_Par_21_KHEntgGG.pdf.
[23] Anlage zur Vereinbarung über die Übermittlung von Daten nach § 21 Abs. 4 und Abs. 5 KHEntgG, Daten nach § 21 KHEntgG – Version 2024 für das Datenjahr 2023 v. 03.01.2024, https://www.g-drg.de/content/download/13512/file/v21-KHEntgGG_A-2024_2023_Endfassung.pdf.
[24] https://www.g-drg.de/datenlieferung-gem.-21-KHEntgGg/datenlieferung-gem.-21-abs.1-KHEntgGg/dokumente-zur-datenlieferung/verschluesselung.

Bei den §-21-Daten des Krankenhauses handelt es sich ausnahmslos um **sensitive Gesundheitsdaten** i.S.v. Art. 9 Abs. 1 DSGVO. Für diese gilt ein allgemeines Verarbeitungsverbot, für das es begrenzte Ausnahmetatbestände gibt, die in Art. 9 Abs. 2 DSGVO geregelt sind.

Normadressat datenschutzrechtlicher Zulässigkeitsvorgaben ist einerseits der Krankenhaus-Kunde, der sowohl für die Verarbeitung im eigenen Interesse eine Rechtsgrundlage benötigt als auch für die Übermittlung an BinDoc zu dessen eigenverantwortlicher Weiterverwendung; andererseits jedoch auch BinDoc als Verantwortlicher für eben diese eigenverantwortliche Weiternutzung der im Rahmen von Analyseaufträgen gewonnenen Daten.

4.3.1 Keine Einwilligung

Eine Nutzungsbefugnis dieser Daten durch BinDoc wegen **ausdrücklichen Einwilligungen** der in den Krankenhäusern behandelten Patienten (Art. 9 Abs. 2 lit. a DSGVO) liegt nicht vor. Diese müssten umfassend über geplante Datenverarbeitung durch BinDoc (sowohl im Auftrag des Krankenhauses als auch für eigene kommerzielle Zwecke) informiert werden und dem ausdrücklich zustimmen. Nicht ausreichend wäre eine Einwilligung im Kleingedruckten (Allgemeine Geschäftsbedingungen – AGB) des Krankenhauses. Soweit bekannt, wird die Datennutzung der Behandlungsdaten durch BinDoc in den Krankenhaus-AGB auch nicht aufgeführt.

4.3.2 Sperrwirkung des § 21 KHEntgG für eine Weiterverarbeitung

Eine Verarbeitung kommt daher nur in Frage, soweit diese für „*die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die **Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich** auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich*“ ist (Art. 9 Abs. 2 lit. h DSGVO, vgl. § 22 Abs. 1 Nr. 1 b BDSG).

Da die §-21-Daten umfassend auch dem Patientengeheimnis (§ 203 Abs. 1 Nr. 1 StGB, § 9 MBOÄ) unterliegen, sind zusätzlich gemäß Art. 9 Abs. 3 DSGVO die nationalgesetzlichen Anforderungen hinsichtlich der **Verarbeitung durch „Fachpersonal“** zu beachten. § 21 KHEntgG enthält eine nationale gesetzliche Regelung, die den Anforderungen des Art. 9 DSGVO entspricht, indem sie mit davon abgedeckten Zwecken und unter Benennung enger Umstände die Datenverarbeitung und zugleich eine Offenbarung von Patientengeheimnissen erlaubt.

Fraglich ist, ob die **vom ursprünglichen Gesetzeszweck abweichende Datenverarbeitung** durch BinDoc erlaubt ist. Insofern könnte sich das Krankenhaus darauf berufen, diese erfolge durch seinen „Auftragsverarbeiter“ BinDoc, wobei sich das Krankenhaus auf die Ausnahmeregelung des Art. 9 Abs. 2 lit. h DSGVO beruft. Außerdem müssten die allgemeinen Rechtmäßigkeitsanforderungen des Art. 6 DSGVO beachtet werden.[25]

Möglicherweise hat ein Krankenhaus ein **berechtigtes Interesse** an der Vornahme von softwaregestützten Analysen ihrer Patientenfalldaten, um Prozesse und Behandlungen zu optimieren und die Leistungserbringung qualitativ und wirtschaftlich zu verbessern. Hinsichtlich der

[25] EuGH 21.12.2023 – C-667/21 Rn. 78 f.

zweckändernden Nutzung der §-21-Daten durch das Krankenhaus (unter Hinzuziehung eines Auftragsverarbeiters) kommt hier nur Art. 6 Abs. 1 lit. f DSGVO in Betracht.

Nach dieser Bestimmung ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, überwiegen. Voraussetzung ist also, dass die Interessen oder Grundfreiheiten und Grundrechte der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen. Dies ist regelmäßig dann der Fall, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer solchen Verarbeitung rechnet.[26] Es ist davon auszugehen, dass in einem Krankenhaus behandelte Patienten nicht damit rechnen, dass ihre sensitiven Daten ohne ihre Kenntnis und ihre Zustimmung von einem externen Verarbeiter für dessen eigene kommerzielle Zwecke weiterverarbeitet werden.

Bei der Abwägung von schutzwürdigen Betroffeneninteressen mit berechtigten Verarbeitungsinteressen sind **gesetzgeberische Erwägungen** in besonderem Maße zu berücksichtigen. Angesichts der hohen Sensitivität der Krankenhaus-Falldaten nach § 21 KHEntgG hat der Gesetzgeber eine strenge Zweckbindung und eine konkrete Benennung möglicher Empfänger festgelegt. Eine Weitergabe der Daten an BinDoc wird davon nicht erfasst. Unter diesen Umständen können die Interessen des Krankenhauses, über die zweckbegrenzt erfassten Informationen allgemein zu verfügen, nicht gegenüber den Schutzinteressen der Patienten überwiegen. Jedenfalls kann keine Verarbeitung und Nutzung dieser personenbezogenen Daten – selbst nach weiterer Pseudonymisierung – durch einen Dienstleister wie BinDoc auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden.[27]

4.3.3 Insbesondere Forschungsnutzung

BinDoc gibt an, die §-21-Daten auch für Forschungszwecke zu nutzen. Insofern enthalten die DSGVO und das nationale Recht Sondervorschriften: Gemäß Art. 5 Abs. 1 S. 1 lit. b i. V. m. Art. 89 DSGVO ist eine Nutzung für im öffentlichen Interesse liegende wissenschaftliche Forschungszwecke nicht mit den ursprünglichen Zwecken unvereinbar, wenn geeignete „**Garantien für die Rechte und Freiheiten der betroffenen Person**“ bestehen. Damit sind insbesondere technische und organisatorische Maßnahmen, etwa zur Umsetzung des Grundsatzes der Datenminimierung durch Pseudonymisierung, gemeint. In Bezug auf Gesundheitsdaten wird diese Zweckprivilegierung dadurch konkretisiert, dass die Verarbeitung gemäß einer gesetzlichen Grundlage in einem „angemessenen Verhältnis zu dem verfolgten Ziel steht“ und der „Wesensgehalt der Grundrechte und Interessen der betroffenen Person gewahrt wird“ (Art. 9 Abs. 2 lit. j DSGVO).

Als **gesetzliche Grundlage** kommen hier die für die jeweiligen Krankenhäuser geltenden Gesetze in Betracht oder die allgemeine Regelung des § 27 BDSG. Hinsichtlich der zu treffenden angemessenen und spezifischen Maßnahmen wird auf § 22 Abs. 2 verwiesen (§ 27 Abs. 1 S. 2 BDSG). Ergänzend regelt § 27 Abs. 3 S. 1 BDSG, dass bei wissenschaftlicher Forschung die Daten zu anonymisieren sind, sobald

[26] EuGH 07.12.2023 – C-26/22 u. C-64/22 Rn. 80, 87.
[27] Vgl. EuGH 07.12.2023 – C-26/22 u. C-64/22 Rn. 99.

dies nach dem Forschungszweck möglich ist. Es gilt ein strenges Datenminimierungsgebot (vgl. Art. 5 Abs. 1 lit. c DSGVO).

Diese Privilegierung der Forschungsnutzung ist nur anwendbar, wenn die konkreten Forschungsprojekte den grundrechtlichen **Schutz der Forschungsfreiheit** nach Art. 5 Abs. 3 S. 1 GG bzw. Art. 13 S. 1 GRCh in Anspruch nehmen können. Dies ist der Fall, wenn das Projekt ein auf wissenschaftlicher Eigengesetzlichkeit (Methodik, Systematik, Beweisbedürftigkeit, Nachprüfbarkeit, Kritikoffenheit, Revisionbereitschaft) beruhender Prozess zum Auffinden von Erkenntnissen, ihrer Deutung und ihrer Weitergabe ist.[28] Diesen Anforderungen genügt nur unabhängig durchgeführte Forschung.[29]

Steht die Erkenntnisgetriebenheit im Vordergrund, so ist eine kommerzielle Intention nicht schädlich. Rein oder **vorrangig kommerziell motivierte Forschung** kommt dagegen nicht in den Genuss der Privilegierung nach den datenschutzrechtlichen Forschungsregelungen.[30] Die Angebote von BinDoc zu Wirtschaftlichkeits- und Marktanalysen für Krankenhäuser oder sonstige Einrichtungen können nicht auf Art. 9 Abs. 2 lit. j DSGVO gestützt werden.

Eine weitere zwingende Anforderung für die Forschungsprivilegierung besteht in der Sicherstellung einer transparenten Projektdurchführung.[31] Inwieweit BinDoc diesen Anforderungen genügt, kann aus den allgemein verfügbaren Informationen nicht abgeleitet werden. BinDoc betreibt ein „**Institut für angewandte klinische Forschung**“, mit dem „Real World Evidenz in der Praxis“ nutzbar gemacht werden soll.[32] Dieses Institut ist nicht mit eigener Rechtspersönlichkeit ausgestattet, sondern es handelt sich um eine „Marke“ der BinDoc GmbH. Bzgl. der eigenen „Forschungsdatenbank“ behauptet BinDoc 17 Mio. „anonymisierte Patientendaten“ auszuwerten, was 18% des gesamten deutschen stationären Patientenvolumens ausmache und „1 Trillion Variablenkombinationen für multidimensionale Analyse“ von Variablen in beliebiger Art und Weise ermögliche.[33]

Mit dem Format der BinDoc „Research Notes“ veröffentlicht das Unternehmen seine „internen Research Projekte“. Dabei gehe es um eine Art „Klinische Fast Track Forschungsplattform“, „die wir in der Forschungs-Community teilen und die dazu animieren soll, interessante Forschungsthemen zu identifizieren, zu analysieren und daraus wichtige Erkenntnisse zu ziehen“.[34] Bisher (Mai 2024) hat BinDoc 4 Research Notes veröffentlicht. Aus diesen „Notes“ können allenfalls indirekt Schlüsse hinsichtlich der Wissenschaftlichkeit der Datenauswertungen gezogen werden. Inwieweit und unter welchen Voraussetzungen **externe Stellen** die „anonymisierten“ §-21-Daten für Forschungszwecke erhalten können, ist nicht bekannt.

[28] Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, S. 18 m.w.N.; kann im Internet kostenlos abgerufen werden unter https://library.oapen.org/bitstream/id/671ad747-59fe-48a6-adac-6a2a9c585e1b/external_content.pdf.
[29] Weichert, Rahmenbedingungen (Fn. 28), S. 20 f. m.w.N.
[30] Weichert, Rahmenbedingungen (Fn. 28), S. 20.
[31] Weichert, Rahmenbedingungen (Fn. 28), S. 21 ff.
[32] https://www.bindoc.de/klinische-forschung.
[33] https://www.bindoc.de/research-notes.
[34] https://www.bindoc.de/research-notes.

4.3.4 Berufliche Schweigepflicht/Patientengeheimnis

Bei den §-21-Daten handelt es sich durchgängig um Patientengeheimnisse, deren unbefugte Offenbarung nach Standesrecht (vgl. § 9 MBOÄ) verboten ist und nach § 203 Abs. 1 StGB strafrechtlich sanktioniert werden kann. Gegenüber den Mitarbeitern von BinDoc können nach § 203 Abs. 3 S. 2 StGB diese Patientendaten offenbart werden, „soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist“. Bei der Entscheidung über die **Erforderlichkeit der Zuziehung externer Mitwirkender** hat das Krankenhaus – konkret dessen ärztliche Leitung – einen weiten Beurteilungsspielraum.[35] Die Zulässigkeit der Einschaltung externer Dritter als Mitwirkende ist weitgehend kongruent mit der datenschutzrechtlichen Zulässigkeit der Beauftragung von Auftragsverarbeitern nach Art. 28 DSGVO.[36] Die reine Beauftragung von externen mit Datenauswertungen zu Zwecken von Markt- und Wirtschaftlichkeitsanalysen kann aber schwerlich noch als für die ärztliche Behandlung erforderlich angesehen werden.

Aber selbst, wenn derartige Aktivitäten noch als Mitwirkung in einem weiteren Sinne akzeptiert werden, so muss hinsichtlich der **Erforderlichkeit der jeweiligen konkreten Offenbarung** ein enger Maßstab angelegt werden.[37] Anderenfalls wäre es über die Mitwirkung möglich, die Vertraulichkeitsbeziehung zwischen Arzt und Patient uferlos zu beeinträchtigen. Dies bedeutet, dass für Analysen, die BinDoc für Krankenhäuser mit deren Daten durchführen, eine Erforderlichkeit der jeweiligen Daten für die konkrete Analyse gegeben sein muss. Die pauschale Bereitstellung der §-21-Daten geht hierüber – je nach Fragestellung – hinaus. Insofern ist die Bereitstellung der Daten gegenüber BinDoc allgemein ein strafbarer Verstoß gegen § 203 Abs. 1 Nr. 1 StGB durch die ärztliche Leitung des Krankenhauses.

Unabhängig von der Zulässigkeit der Mitwirkung (bzw. vom Umfang der Mitwirkung) sind die mitwirkenden Personen gemäß § 203 Abs. 4 S. 2 Nr. 1 StGB zur Geheimhaltung zu verpflichten. Offenbaren die verpflichteten Personen unberechtigt die ihnen anvertrauten Berufsgeheimnisse, so machen auch diese sich strafbar. Die Beschäftigten von BinDoc, die die vom Krankenhaus erlangten §-21-Daten an Dritte weitergeben, haben hierfür keine Befugnis und machen sich daher **als Mitwirkende strafbar** nach § 203 StGB. In Betracht kommt darüber hinaus auch eine Anstiftung oder eine Beihilfe zur strafbaren Offenbarung durch die ärztliche Leitung des Krankenhauses.[38]

4.4 Weitere rechtliche Anforderungen

Aus dem oben Dargestellten ergibt sich, dass für die Verarbeitung der §-21-Daten durch BinDoc als verantwortliche Stelle **keine Rechtsgrundlage** besteht. Soweit sich deren Datenverarbeitung als Auftragsverarbeiter konkret auf einen bestimmten Auftrag bezieht, kann dies bei Beachtung des Datenminimierungsgebots zulässig sein. Es ist allerdings zu bedenken, dass auch das Angebot der Auftragsverarbeitung (Vergleich eigener Krankenhaus-Daten mit denen anderer Krankenhäuser) ohne die eigenverantwortliche Verarbeitung durch BinDoc (Zweitverwertung und Aufbau Vergleichsdatenbank) nicht sinnvoll genutzt werden könnte.

[35] Weichert, Rahmenbedingungen (Fn. 28), S. 84 m.w.N.
[36] Weichert, Rahmenbedingungen (Fn. 28), S. 86 ff. m.w.N.
[37] Weichert, Rahmenbedingungen (Fn. 28), S. 84 m.w.N.
[38] Weichert MedR 2024, 88 f.

Die DSGVO definiert **weitere Voraussetzungen** für eine zulässige Datenverarbeitung.

4.4.1 Insbesondere Transparenz

Voraussetzung für die Übermittlung der personenbeziehbaren §-21-Daten von den Krankenhäusern an BinDoc wäre es, dass hierüber die Krankenhäuser oder BinDoc die betroffenen **Patienten informieren**. Art. 13 und Art. 14 DSGVO verlangen eine frühestmögliche Information „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ (Art. 12 Abs. 1 S. 1 DSGVO) u.a. über die Zwecke, die Rechtsgrundlage, die Empfänger und die Betroffenenrechte (Art. 13/14, jeweils Abs. 1 u. 2 DSGVO). Eine solche Information ist bei den bekannten Krankenhaus-Verträgen bzw. -Hinweisblättern nicht erkennbar.

4.4.2 Insbesondere Datenschutz-Folgenabschätzung

Gemäß Art. 35 Abs. 1 S. 1 DSGVO hat eine verantwortliche Stelle eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Verarbeitung „aufgrund der Art, des Umfangs und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge hat. Dies ist gemäß Art. 35 Abs. 3 DSGVO insbesondere der Fall, wenn eine „umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten“ erfolgt.

Die Aufsichtsbehörden haben eine **Liste** von Auslösern gemäß Art. 35 Abs. 4 DSGVO erstellt, die die Verarbeitung der §-21-Daten durch Krankenhäuser und durch BinDoc erfassen.[39] Folgende Aspekte sind hierfür relevant:

- Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen (1.),
- Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern 1. die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, 2. für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, und die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind (3. u. 8.).

Bei einer Datenschutz-Folgenabschätzung sind nicht nur die kurzfristigen Risiken zu bewerten und zu minimieren. Vielmehr muss langfristig die Wahrung des Datenschutzes gewährleistet werden. BinDoc nimmt offenbar für sich in Anspruch, die nur vorgeblich anonymisierten §-21-Daten unbefristet weiter zu speichern und für sich zu nutzen. Dies begründet die Befürchtung, dass ohne jegliche Vorkehrungen und Schutzmaßnahmen zu Einzelpersonen (**pseudonyme) Gesundheits-Lebensprofile** erstellt werden.

Ob durch die Krankenhäuser und BinDoc in Bezug auf die betrachtete Datenverarbeitung Folgenabschätzungen durchgeführt wurden und zu welchen Ergebnissen diese ggf. kommen, ist nicht bekannt.

[39] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf.

5 Ergebnis

Bei den Angeboten von BinDoc zur Durchführung von Datenanalysen sowie von Forschungsprojekten werden keinen anonymen, sondern personenbeziehbare sensitive und dem Patientengeheimnis unterliegende Daten verarbeitet. Die durch BinDoc erfolgende eigene Sekundärnutzung der von Krankenhäusern im Rahmen einer „Auftragsverarbeitung“ erlangten Daten ist **datenschutzrechtlich unzulässig und erfüllt den Straftatbestand des § 203 StGB**.

Auch wenn sich direkt für die Krankenhauspatienten durch die BinDoc-Datenverarbeitung keine spürbaren nachteiligen Folgen ergeben mögen, weil bisher keine missbräuchliche Identifizierung von Personen aus den pseudonymisierten Datensätzen bekannt wurde, muss der Rechtsverstoß von BinDoc sehr ernst genommen werden: Die **Sekundärnutzung von hochsensitiven Gesundheitsdaten** erfreut sich nicht nur bei diesem privaten Dienstleister großer Beliebtheit. Durch nationale (Gesundheitsdatennutzungsgesetz – GNDG) und europäische Initiativen (European Health Data Space – EHDS) werden für solche Sekundärnutzungen Rechtsgrundlagen geschaffen. Der damit verbundene Paradigmenwechsel beim Patientengeheimnis erfolgt bei der Schaffung neuer Gesetzesgrundlagen ohne hinreichende Reflektion der Konsequenzen für das heilberufliche Vertraulichkeitsversprechen und insbesondere ohne Schutzmaßnahmen für die betroffenen Patienten. Doch selbst den Anforderungen des GDNG und des EHDS genügt die Bereitstellung die Bereitstellung der §-21-Daten an BinDoc durch die Krankenhäuser und die dortige Datennutzung nicht im Ansatz.

Die betroffenen Krankenhauspatienten werden mit dieser Datenverarbeitung rechtlos gestellt; Ihnen wird jegliche Information darüber vorenthalten, was mit ihren Daten passiert. Einher geht damit eine **Kommerzialisierung der medizinischen Datenverarbeitung**, bei der ethische und grundrechtliche Vorbehalte stillschweigend übergangen werden. Diese von BinDoc – in marktverzerrender Weise – vorexerzierte Praxis schädigt letztlich das Vertrauen in ein vorrangig gemeinwohlorientiertes Gesundheitssystem.

Abkürzungen

Abs.	Absatz
Art.	Artikel
Aufl.	Auflage
BDSG/aF	Bundesdatenschutzgesetz/alte Fassung
BFH	Bundesfinanzhof
bzw.	beziehungsweise
ca.	circa
DSGVO	Europäische Datenschutz-Grundverordnung
ErwGr	Erwägungsgrund
etc.	und so weiter
EuGH	Europäischer Gerichtshof
f/f.	fort-/folgende
Fn.	Fußnote
GG	Grundgesetz
GRCh	Europäische Grundrechte-Charta
ID-	Identifizierung/s-
InEK	Institut für das Entgeltsystem im Krankenhaus GmbH
insbes.	insbesondere
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
Kap.	Kapitel
KHEntgG	Krankenhausentgeltgesetz
lit.	Buchstabe
Mio.	Millionen
Mrd.	Milliarden
m.w.N.	mit weiteren Nachweisen
MBOÄ	Musterberufsordnung der Ärztekammern
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
RDV	Recht der Datenverarbeitung (Zeitschrift)
Rn.	Randnummer
S.	Satz/Seite
s.o.	siehe oben
StGB	Strafgesetzbuch
s.u.	siehe unten
u.a.	unter anderem/und andere
v.	von
vgl.	vergleiche
z.B.	zum Beispiel