HAMMERMANN EHLERS ALBERT
RECHTSANWÄLTE IN PARTNERSCHAFT

HAMMERMANN EHLERS ALBERT · Karl-Liebknecht-Straße 25 · 03046 Cottbus

NAEMI-WILKE-STIFT
Dr.-Ayrer-Straße 1-4
03172 Guben

**Unser Az.: EH-211/23**

2. Juni 2023
mf128.docx

# Kurzgutachten über die datenschutzrechtliche Beurteilung

Gliederung



**PETER ALBERT** *
Rechtsanwalt
Fachanwalt für Arbeitsrecht
Fachanwalt für Miet- & WEG-Recht

**BENJAMIN EHLERS** *
Rechtsanwalt
Fachanwalt für Steuerrecht
Fachanwalt für Handels- & Gesellschaftsrecht

**FALK HAMMERMANN** **
Rechtsanwalt
Fachanwalt für Bau- & Architektenrecht
Fachanwalt für Miet- & WEG-Recht

**ANTJE GERDES** *
Rechtsanwältin
Mediatorin
Fachanwältin für Familienrecht

**CLAUDIA NAPIERALSKI** **
Rechtsanwältin
Fachanwältin für Strafrecht

**MARTA SZATARSKA LL.M** *
Rechtsanwältin
Fachanwältin für Transport- & Speditionsrecht
Radca Prawny

AG Cottbus PR 54 CB

**Deutsche Bank AG**
BIC: DEUTDEDB160

Geschäftskonto
IBAN: DE95 1207 0024 0304 3486 00

Anderkonto
IBAN: DE97 1207 0024 0015 6851 00

**VR Bank Lausitz eG**
BIC: GENODEF1FWA

Geschäftskonto
IBAN: DE67 1806 2678 0006 2318 29

**Abkürzungen**

| Abkürzung | Erläuterung |
|---|---|
| **Abs.** | Absatz |
| **AEUV** | Vertrag über die Arbeitsweise der Europäischen Union |
| **Art.** | Artikel |
| **BDSG** | Bundesdatenschutzgesetz |
| **DSGVO** | Datenschutz-Grundverordnung |
| **ErwGr** | Erwägungsgrund der DSGVO |
| **EU** | Europäische Union |
| **gem.** | gemäß |
| **GG** | Grundgesetz |
| **ggf.** | gegebenenfalls |
| **IfSG** | Infektionsschutzgesetzes |
| **i.V.m.** | in Verbindung mit |
| **lit.** | lateinisch littera - Buchstabe |
| **m.w.N.** | mit weiteren Nachweisen |
| **Rn.** | Randnummer |
| **S.** | Satz |
| **SGB** | Sozialgesetzbuch |
| **u.a.** | unter anderem |
| **v.a.** | vor allem |
| **vgl.** | vergleiche |
| **z.B.** | zum Beispiel |
| **Ziff.** | Ziffer |

**Literatur**

Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021
BeckOK Datenschutzrecht, Wolff/Brink, 43. Edition, Stand: 01.02.2023
Thüsing, Beschäftigtendatenschutz und Compliance, 3. Auflage 2021

**I. Hintergrund der Beauftragung**

Das Naemi Wilke Stift (nachfolgend Krankenhaus) hat uns beauftragt die geplante Entwicklung der medizinischen Infrastruktur im Hinblick auf eine Zusammenarbeit zwischen dem Krankenhaus in Guben, einem Medizinischen Versorgungszentrum ebenfalls in Guben (nachfolgend MVZ) und einem Rettungsdienst in Gubin/Polen (nachfolgend Rettungsdienst) rechtsberatend zu begleiten. Hierbei sollen insbesondere gesellschaftsrechtliche Fragestellungen hinsichtlich des neu zu gründenden MVZs sowie allgemeine datenschutzschutzrechtliche Fragestellungen bezüglich der Zusammenarbeit der drei Akteure geklärt werden.

Dieses Kurzgutachten soll allgemeine datenschutzrechtliche Aspekte des geplanten Vorhabens beleuchten.

**II. Sachliche Ausgangssituation**

Im Rahmen der Begutachtung gehen wir von der folgenden - abstrakt dargelegten - Ausgangssituation aus:
Geplant ist die Zusammenarbeit dreier rechtlich selbständiger Unternehmen, deren unternehmerischer Schwerpunkt ganz allgemein gesprochen in der medizinischen Versorgung von Patienten liegt. Besonders zu berücksichtigen sind hierbei die Rechtsform des Krankenhauses, welches als kirchliche Stiftung bürgerlichen Rechts agiert, und die Tatsache, dass zwei der Unternehmen ihren Sitz in Deutschland (Bundesland Brandenburg) haben, der dritte Akteur jedoch in Polen ansässig ist.

Die Zusammenarbeit soll dergestalt ablaufen, dass den Patienten - unabhängig davon bei welchem der drei Akteure sie erstmalig aufgenommen werden - das Leistungsportfolio aller Beteiligten zur Verfügung stehen soll. Zu diesem Zweck wird es erforderlich sein, dass Patientendaten, auf deren Definition die Begutachtung eingehen wird, zwischen den Unternehmen transferiert werden. Dieser Verarbeitungsvorgang soll im Fokus der datenschutzrechtlichen Begutachtung stehen, obschon es voraussichtlich vielerlei Verarbeitungssituationen geben wird, die einer gesonderten Betrachtung des Einzelfalls bedürfen.

**III. Datenschutzrechtliche Ausgangssituation**

Ausgehend von den Standorten der drei Akteure (Deutschland und Polen), ist vordergründig eine Datenverarbeitung innerhalb der EU zu erwarten.

Mit den Regelungen der DSGVO wird seit dem 25. Mai 2018 in der EU weitestgehend einheitlich geregelt, inwiefern personenbezogene Daten verarbeitet werden dürfen.

Als europäischer Rechtsakt in Form einer Verordnung nach Art. 288 Abs. 2 AEUV, entfaltet die DSGVO unmittelbare Wirkung in allen Mitgliedstaaten der EU und bedarf (z.B. anders als EU-Richtlinien) keiner Umsetzung in eine landesrechtliche

Rechtsgrundlage. Die DSGVO ist damit einheitliche Grundlage zur Verarbeitung personenbezogener Daten innerhalb der EU.

Lediglich über sog. Öffnungsklauseln in der DSGVO ergeben sich zumindest punktuell Spielräume für die nationalen Gesetzgeber zur Schaffung nationaler datenschutzrechtlicher Regelungen, welche die Anforderungen der DSGVO nicht unterschreiten dürfen. Auch solche nationalen Rechtsgrundlagen sollen daher vereinzelt in den Blick genommen werden.

**IV. Begriffsklärungen**

Um für die gutachterlichen Ausführungen ein einheitliches Begriffsverständnis sicherzustellen, soll in gebotener Kürze auf einige wesentliche Begrifflichkeiten eingegangen werden.

- **Personenbezogene Daten (Art. 4 Ziff. 1 DSGVO)**

Unter personenbezogenen Daten sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person (nachfolgend: Betroffener) beziehen (vgl. Art. 4 Ziff. 1 DSGVO). Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

- **Gesundheitsdaten**

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (vgl. Art. 4 Ziff.15 DSGVO).

- **Verarbeitung**

Eine Verarbeitung im Sinne des Art. 4 Ziff. 2 DSGVO ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

- **Verantwortlicher**

Nach Art. 4 Ziff. 7 DSGVO ist Verantwortlicher im Sinne der DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

**Hinweis:** Die Verantwortung des Verantwortlichen umfasst nach Art. 24 DSGVO insbesondere
- die Einhaltung der DSGVO,
- Ergreifen geeigneter Schutzmaßnahmen und
- den Nachweis dafür.

- **Auftragsverarbeitung**

Ein Auftragsverarbeiter im Sinne von Art. 4 Ziff. 8 DSGVO ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Verantwortlich ist wiederum der Entscheider über Zweck und Mittel der Verarbeitung, also der Auftraggeber.

**V. Pflichten des Verantwortlichen**

Jeder der drei Akteure hat innerhalb seines eigenen Unternehmens und im Zusammenhang mit dem geplanten Vorhaben Pflichten als datenschutzrechtlich Verantwortlicher zu beachten. Diese sollen zunächst nur abstrakt beschrieben und im weiteren Verlauf mit Bezug auf die geplante Zusammenarbeit näher erwähnt werden.

Hervorzuheben sind die in Art. 5 DSGVO geregelten Rechtsgrundsätze der Datenverarbeitung, die in Art. 13 DSGVO verankerten Informationspflichten sowie die Pflicht zur Benennung eines Datenschutzbeauftragten (u.a. Art. 37 DSGVO).

**1. Grundsätze der Datenverarbeitung**

Für jedes der beteiligten Unternehmen gilt, dass die in Art. 5 DSGVO normierten Grundsätze der Datenverarbeitung zu beachten sind.

Das sind:
- Rechtmäßigkeit der Verarbeitung nach Treu und Glauben; Transparenz (Art. 5 Abs. 1 lit. a) DSGVO)
- Zweckbindung (Art. 5 Abs. 1 lit. b) DSGVO)
- Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO)
- Richtigkeit (Art. 5 Abs. 1 lit. d) DSGVO)
- Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO)
- Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO)
- Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)

Diese Grundsätze gelten bei sämtlichen Datenverarbeitungsvorgängen und sind unabhängig davon einzuhalten, welche Kategorien von Daten verarbeitet werden. Einen besonderen Stellenwert haben hierbei die Grundsätze nach Art. 5 Abs. 1 lit. a) und b) DSGVO, die bei dem geplanten Vorhaben, v.a. beim Datentransfer zwischen den einzelnen Akteuren, einzuhalten sein werden.

Dem Zweckbindungsgrundsatz kommt dabei eine signifikante Bedeutung zu, da dieser die Verarbeitung der Daten legitimiert (vgl. *Paal/Pauly/Frenzel DS-GVO Art. 5 Rn. 23*). Gem. Art. 5 Abs. 1 lit. b) DSGVO müssen personenbezogene Daten „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“. Der Zweck besagt also, aus welchem Grund bzw. Anlass personenbezogene Daten verarbeitet werden. Infolgedessen ist der Zweck der Datenverarbeitung der Fixpunkt, an dem sich z.B. die Erforderlichkeit der Verarbeitung, die Rechtsgrundlagen gem. Art. 6 Abs. 1 DSGVO und auch die Informationspflichten nach Art. 13 ff. DSGVO ausrichten. (vgl. *BeckOK DatenschutzR/Schantz DS-GVO Art. 5 Rn. 13*).

Der Zweckbindungsgrundsatz erstreckt sich ebenso auf die Weiterverarbeitung durch andere als diejenige Person, die die Daten erhoben hat, weshalb der Datenerheber verpflichtet ist, die vorgesehenen Zwecke auch an Folgenutzer zu übermitteln (vgl. *Paal/Pauly/Frenzel DS-GVO Art. 5 Rn. 29*).

Für die Beteiligten ist es somit ratsam ihren Fokus vorab auf die Festlegung der Verarbeitungszwecke zu legen, um davon ausgehend alle weiteren Schritte vorzubereiten.

**2. Informationspflichten**

Eine weitere - insbesondere im Hinblick auf das angedachte Vorhaben - bedeutende Pflicht, ist die Informationspflicht des Verantwortlichen gegenüber dem Betroffenen. Die DSGVO unterscheidet dabei zwei Fällen:

- Informationspflichten im Falle der Datenerhebung beim Betroffenen (Art. 13 DSGVO)
- Informationspflichten im Falle der Datenerhebung bei einem Dritten (Art. 14 DSGVO).

Werden personenbezogene Daten beim Betroffenen erhoben, so ist der Verantwortliche verpflichtet, der betroffenen Person zum Zeitpunkt der Erhebung die in Art. 13 und 14 DSGVO genannten Daten mitzuteilen (u.a. Name und Kontaktdaten des Verantwortlichen, ggf. seines Vertreters, Zwecke der Verarbeitung sowie Rechtsgrundlage).

**3. Dokumentationspflicht**

Der datenschutzrechtlich Verantwortliche ist gem. Art. 30 Abs. 1 DSGVO verpflichtet, sämtliche Verarbeitungsvorgänge in Verzeichnissen von Verarbeitungstätigkeiten zu dokumentieren. Dadurch soll u.a. einer Aufsichtsbehörde ein schneller Einblick in die Verarbeitungsprozesse des Unternehmens ermöglicht werden.

Da bei allen Akteuren die Verarbeitung von besonderen Datenkategorien (v.a. Gesundheitsdaten) zu erwarten ist, wird die Verpflichtung zum Führen von Verfahrensverzeichnissen für alle Beteiligten gelten und nicht nach Art. 30 Abs. 5 DSGVO entbehrlich sein.

**4. Datenschutz-Folgenabschätzung**

Darüber hinaus wird bei risikobehafteten Verarbeitungsvorgängen zusätzlich nach Art. 35 DSGVO eine sog. Datenschutz-Folgenabschätzung vorzunehmen sein. Hiernach muss eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge durchgeführt werden. Dies gilt, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

**5. Benennung eines Datenschutzbeauftragten**

Eine Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht nach Art. 37 Abs. 1 DSGVO auf jeden Fall, wenn

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln (vgl. Art. 37 Abs. 1 lit. a) DSGVO),
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (vgl. Art. 37 Abs. 1lit b) DSGVO), oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO besteht (vgl. Art. 37 Abs. 1 lit. c) DSGVO).

In den beiden zuletzt genannten Fällen wird auf die Kerntätigkeit des Verantwortlichen abgestellt, welche - um nach diesen Regelungen eine Pflicht zu begründen - in der Durchführung von personenbezogenen Datenverarbeitungs-vorgängen bestehen muss.

In diesem Zusammenhang geht aus ErwGr 97 hervor, dass sich der Begriff der „Kerntätigkeit“ eines Verantwortlichen auf dessen Haupttätigkeiten bezieht und nicht auf Verarbeitungsvorgänge, die als bloße Nebentätigkeit anfallen.

Außerdem enthält Art. 37 Abs. 4 S. 1 DSGVO eine Öffnungsklausel für nationale Regelungen der Mitgliedstaaten. Der deutsche Gesetzgeber hat mit § 38 Abs. 1 BDSG von dieser Öffnungsklausel Gebrauch gemacht. Danach sollen der Verantwortliche und der Auftragsverarbeiter ergänzend zur Regelung der DSGVO einen Datenschutzbeauftragten benennen, wenn eine der folgenden Voraussetzungen vorliegt:

- sie beschäftigen in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten;
- sie nehmen Verarbeitungen vor, die einer Datenschutzfolgenabschätzung nach Art. 35 DSGVO unterliegen; oder
- sie verarbeiten personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung.

**VI. Rechte der Betroffenen**

Die Rechte der Betroffenen bilden keinen Schwerpunkt dieser Begutachtung und sollen daher lediglich für das Gesamtverständnis benannt werden.

Unter dem Begriff der Betroffenenrechte sind die Rechte der Personen zu verstehen, die von der Datenverarbeitung betroffenen sind. Die Art. 12 ff. DSGVO regeln die Betroffenenrechte im Einzelnen.

Betroffenen stehen folgende Rechte bezüglich der Datenverarbeitung zu:

- Recht auf Auskunft (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Recht auf Widerspruch (Art. 21 DSGVO)
- Recht auf Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO)
- Recht keiner automatisierten Entscheidung unterworfen zu werden (Art. 22 DSGVO)
- Beschwerderecht bei der Aufsichtsbehörde (Art. 77 DSGVO i.V.m. § 19 BDSG)

Ziel diese Rechte, aus denen sich zugleich Pflichten des Verantwortlichen ergeben, ist es, den Betroffenen in seiner informationellen Selbstbestimmung (vgl. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG)) zu schützen. Darüber hinaus dienen die Betroffenenrechte insbesondere der Gewährleistung eines Informationsflusses und der Transparenz.

**VII. Allgemeine Voraussetzungen der Verarbeitung personenbezogener Daten**

Jede Verarbeitung personenbezogener Daten stellt speziell einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) dar. Daher erfordert jede Verarbeitung personenbezogener Daten eine rechtliche Grundlage, welche in Form der Einwilligung des Betroffenen vorliegen oder sich aus einer Erlaubnisnorm ergeben kann. Datenverarbeitungen ohne rechtliche Grundlage sind folglich verboten oder anders ausgedrückt: Jede Verarbeitung personenbezogener Daten bedarf stets einer rechtlichen Erlaubnis.

**1. Rechtsgrundlagen nach DSGVO**

**a)** Eine rechtliche Grundlage (Erlaubnis) zur Verarbeitung personenbezogener Daten kann in unterschiedlichen Varianten gegeben sein, welche weitestgehend in Art. 6 DSGVO geregelt werden.

Danach kann eine Datenverarbeitung unter folgenden Umständen erlaubt sein:

- Vorliegen einer Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO)
- Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich (Art. 6 Abs. 1 S. 1 lit. b) DSGVO)
- Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (Art. 6 Abs. 1 S. 1 lit c) DSGVO)
- Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 S. 1 lit d) DSGVO)
- Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6 Abs. 1 S. 1 lit e) DSGVO)
- Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Art. 6 Abs. 1 S. 1 lit f) DSGVO)

Welche Erlaubnistatbestände einschlägig sein könnten, hängt von den jeweiligen Verarbeitungsvorgängen bzw. von den zu verarbeitenden Daten ab.

***Exkurs: Einwilligung***

Der Begriff der Einwilligung wird in Art. 4 Ziff. 11 DSGVO ebenfalls legal vom Gesetz definiert.
Danach ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Erforderlich für eine wirksame Einwilligung ist eine der Verarbeitung zeitlich vorgehende, freiwillige, informierte, bestimmte, formgemäße Einverständniserklärung einer einwilligungsfähigen betroffenen Person über die Verarbeitung personenbezogener Daten *(BeckOK DatenschutzR/Stemmer DS-GVO Art. 7 Rn. 34)*.

In Bezug auf das geplante Vorhaben werden speziell die Erfordernisse der Informiertheit der Einwilligung, die Form und - im Einzelfall - der Einwilligungsfähigkeit von besonderer Relevanz sein.

- Informiertheit

Die Informiertheit bezieht sich dabei auf die Pflicht des Verantwortlichen den Betroffenen über die in Art. 13 DSGVO genannten Punkte in Kenntnis zu setzen, um den Einwilligenden in die Lage zu versetzen, die Tragweite seiner Erklärung abschätzen zu können. Die Anforderung der Informiertheit trägt somit dem in Art. 5 Abs. 1 lit. a) DSGVO verankerten Grundsatz der Transparenz Rechnung.

**Hinweis:** Eine der wesentlichen Herausforderungen der beteiligten Unternehmen wird bezüglich der Einholung von Patienten-Einwilligungserklärungen, in der vorgelagerten Erarbeitung von Formularen zur Erfüllung der gesetzlichen Informationspflichten bestehen. Hierbei wird speziell der Datentransfer zwischen den drei Akteuren einer der anzugebenden Verarbeitungszwecke sein.

Jedenfalls aus dem Klinikalltag ist die Wichtigkeit einer korrekten und vollständigen Information des Patienten bereits bekannt.

- Form

Aus der gesetzlichen Definition der Einwilligung ist zu entnehmen, dass die Willensbekundung „unmissverständlich […] in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“ abgegeben werden muss. Hiervon sind mündliche, schriftliche oder durch schlüssiges Handeln geäußerte Willensbekundungen erfasst (vgl. ErwGr 32 S. 2). Bloßes Stillschweigen genügt beispielweise nicht (vgl. ErwGr 32 S.3).

Essentiell für jeden der Akteure ist der Nachweis, dass eine Willensbekundung tatsächlich vorgelegen hat. Denn der Verantwortliche trägt die Beweislast für das Vorhandensein einer Einwilligung (vgl. Art. 7 Abs. 1 DSGVO, ErwGr 42 S. 1).

**Hinweis:** Grundsätzlich sollte somit stets eine schriftliche Einwilligungserklärung eingeholt werden, soweit diese erlangt werden kann. Erfolgt eine Einwilligungserklärung im Ausnahmefall nicht schriftlich, sollte zu Beweiszwecken zumindest die Abgabe der Erklärung (mit Ort, Datum, Zeugen) dokumentiert werden. Pauschal- oder Blankoerklärungen genügen in keinem Fall.

Schließlich ist zu beachten, dass eine Einwilligungserklärung - jedenfalls mit Wirkung für die Zukunft - widerrufen werden kann. Eine solche Widerrufsmöglichkeit darf dem Betroffenen nicht unnötig erschwert werden (Maßstab sind dabei die Anforderungen, die an die Erteilung der Einwilligung gestellt wurden).

---

**b)** Bereits an dieser Stelle soll auf die Besonderheiten im Rahmen der Verarbeitung von besonderen Kategorien von Daten eingegangen werden, die von Art. 9 DSGVO erfasst werden.

Einer der zentralen Datenverarbeitungsprozesse wird bei dem geplanten Vorhaben in der Verarbeitung von Gesundheitsdaten liegen, welche von Art. 9 DSGVO als „besondere Kategorie“ personenbezogener Daten genannt wird.

Im Zusammenhang mit der Frage, inwiefern die Verarbeitung von besonderen Kategorien von Daten datenschutzrechtlich zulässig ist, stößt man auf einen theoretischen und bis dato nicht abschließend geklärten Streit hinsichtlich des Verhältnisses von Art. 9 DSGVO zu Art. 6 DSGVO. Ungeachtet der juristischen Einzelheiten steht fest, dass Art. 9 DSGVO gegenüber Art. 6 DSGVO strengere Voraussetzungen an die Rechtmäßigkeit einer Verarbeitung stellt, da die von dieser Norm erfassten Daten besonders sensibel (vgl. ErwGr 51 S. 1) und somit besonders schutzwürdig sind. Im Ergebnis der theoretischen Auseinandersetzung wird man sagen müssen, dass die Verarbeitung besonderer Kategorien personenbezogener Daten ausschließlich nach Art. 9 DSGVO zu rechtfertigen ist.

Art. 9 DSGVO ist dabei anders angelegt als die Regelung zur Verarbeitung einfacher personenbezogener Daten (meint: Art. 6 DSGVO): Während bei diesem die Verarbeitung nur unter bestimmten Voraussetzungen - insbesondere der Einwilligung - zulässig und rechtmäßig ist, ist die Verarbeitung besonderer personenbezogener Daten verboten (vgl. *Paal/Pauly/Fenzel DS-GVO Art. 9 Rn.1*). Von diesem Grundsatz des Verbots der Verarbeitung besonders sensibler Daten, sieht Art. 9 Abs. 2 DSGVO wiederum Ausnahmen vor.

Hintergrund dieser gesetzlichen Struktur liegt in der besonderen Schutzbedürftigkeit, personenbezogener Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind und bei deren Verarbeitung erhebliche Risiken für eben besagte Grundrechte und Grundfreiheiten auftreten können (vgl. ErwGr 51 S. 1).

Art. 9 Abs. 2 DSGVO nennt folgende Tatbestände:

- Einwilligung (Art. 9 Abs. 2 lit a) DSGVO)
- Recht der sozialen Sicherheit und Sozialschutz (Art. 9 Abs. 2 lit b) DSGVO)
- Verarbeitung zum Schutz lebenswichtiger Interessen (Art. 9 Abs. 2 lit c) DSGVO)
- Zweckgebunden interne Verarbeitung durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht (Art. 9 Abs. 2 lit d) DSGVO)
- Betroffene Person hat Daten offensichtlich öffentlich gemacht (Art. 9 Abs. 2 lit e) DSGVO)
- Verfolgung rechtlicher Ansprüche (Art. 9 Abs. 2 lit f) DSGVO)
- erhebliches öffentliches Interesse (Art. 9 Abs. 2 lit g) DSGVO)
- Verarbeitung zum Zwecke der individuellen medizinischen Versorgung (Art. 9 Abs. 2 lit h) DSGVO)
- Verarbeitung von Gesundheitsdaten im öffentlichen Interesse (Art. 9 Abs. 2 lit i) DSGVO)
- Archivzwecke, Forschungszwecke, statistische Zwecke (Art. 9 Abs. 2 lit j) DSGVO)

Aus denen in Art. 9 Abs. 2 DSGVO geregelten Ausnahmen von Absatz 1 (also von dem Verbot der Verarbeitung), kann jedoch keine grundsätzliche Erlaubnis allein beim Vorliegen einzelner Tatbestände abgeleitet werden (vgl. *Paal/Pauly/Fenzel DS-GVO Art. 9 Rn.18*). Das heißt, selbst wenn die in Art. 9 Abs. 2 DSGVO genannten Fälle vorliegen, kann hieraus nicht ausnahmslos auf eine Rechtmäßigkeit der Datenverarbeitung geschlossen werden.

Vielmehr sind die in Art. 9 Abs. 2 DSGVO geregelten Tatbestände insoweit unterschiedlich strukturiert, dass nur einige die Geltung des Verbots nach Art. 9 Abs.1 DSGVO ausschließen (vgl. *Paal/Pauly/Fenzel DS-GVO Art. 9 Rn.18*) und demzufolge eine Datenverarbeitung gestatten. Dies gilt für die Tatbestände in Art. 9 Abs. 2 lit a), c), e) und f) DSGVO.

Andere in Art. 9 Abs. 2 DSGVO genannte Tatbestände, bedürfen darüber hinaus der Ergänzung durch Rechtsnormen, sei es um die Zulässigkeit der Verarbeitung zu begründen (lit. b, g, h, i und j), und/oder um die Garantien oder angemessenen und spezifischen Maßnahmen zu definieren (lit. b, d, g, h, i, j), vgl. *Paal/Pauly/Fenzel DS-GVO Art. 9 Rn.19*.

Für das geplante Vorhaben bedeutet dies, dass u.a. die Einholung wirksamer Einwilligungserklärungen der betroffenen Patienten maßgeblich für die Rechtmäßigkeit der Datenverarbeitungen sein wird.

Eine Datenverarbeitung wird durch die drei beteiligten Akteure voraussichtlich ebenfalls (unmittelbar) erlaubt sein, wenn die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben (vgl. Art. 9 Abs. 2 lit. c) DSGVO).

Eine Bezugnahme auf die Ausnahmetatbestände in Art. 9 Abs. 2 lit b, g, h, i und j) DSGVO muss demgegenüber noch durch Rechtsnormen (nationalen Rechts) ergänzt werden, damit eine Datenverarbeitung rechtmäßig sein kann.

Zusammenfassend lässt sich sagen, dass die Verarbeitung von Gesundheitsdaten beispielsweise beim Vorliegen einer wirksamen und ausdrücklichen Einwilligung des Betroffenen nicht verboten, sondern unmittelbar erlaubt ist. Außerhalb dieses Tatbestandes muss die Struktur des Art. 9 DSGVO berücksichtigt und ggf. eine nationale Rechtsgrundlage hinzugezogen werden, um eine Datenverarbeitung zu legalisieren.

Ohne konkrete Kenntnisse der einzelnen Verarbeitungsvorgänge kann hier nicht auf weitere Details eingegangen werden. Dies wird sodann für die konkreten Sachverhalte zu prüfen sein.

**2. Gesetzliche Erlaubnistatbestände nach nationalem Recht**

Im Hinblick auf das geplante Vorhaben werden möglicherweise über die eingangs erwähnten Öffnungsklauseln der DSGVO auch gesetzliche Erlaubnistatbestände nach nationalen Rechtsgrundlagen die Zulässigkeit einzelner Verarbeitungsvorgänge begründen.

Mangels detaillierter Kenntnisse der denkbaren Verarbeitungsprozesse, sollen nationale Rechtsgrundlagen lediglich beispielhaft benannt werden.

**a) nationale Vorschriften in Deutschland**

Neben den allgemeinen Regelungen der DSGVO existieren nationale bereichsspezifische Datenschutzregelungen, die möglicherweise auch im Rahmen des geplanten Vorhabens Anwendung finden könnten.

- Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze

Zu diesen nationalen Regelungen gehört das mit Einführung der DSGVO reformierte BDSG (n.F.) als Auffanggesetz, welches nach § 1 Abs. 1 BDSG sowohl für nicht-öffentliche Stellen als auch für öffentliche Stellen des Bundes und teilweise für öffentliche Stellen der Länder gilt.

Ebenfalls als Auffanggesetze bestehen Landesdatenschutzgesetze, deren Existenz aus Überschneidungen der Kompetenzen von Bund und Ländern herrührt. Das Datenschutzrecht unterfällt demzufolge je nach inhaltlichem Bezug der Gesetzgebungskompetenz des Bundes bzw. der Länder.

Die Landesdatenschutzgesetze regeln dabei die Datenverarbeitung durch Landes- und Kommunalbehörden.

Heißt *(vgl. JuS 2006, 213 (214))*:

- Für öffentliche Stellen des Bundes gelten gem. § 1 Abs. 2 Nr. 1 BDSG die ersten beiden Abschnitte des Bundesdatenschutzgesetzes.
- Landesbehörden sind, auch soweit sie Bundesrecht vollziehen, den Datenschutzgesetzen der Länder unterworfen.
- Die automatisierte Datenverarbeitung durch natürliche oder juristische Personen des Privatrechts unterliegt schließlich nach § 1 Abs. 2 Nr. 3 BDSG grundsätzlich dem ersten und dritten Abschnitt des Bundesdatenschutzgesetzes.

Rein von der Gesetzessystematik kommt im Hinblick auf das geplante Vorhaben allenfalls das BDSG zum Zuge. Das Brandenburgische Datenschutzgesetz wird demgegenüber nicht relevant sein, da die Akteure voraussichtlich nicht in den Anwendungsbereich dies Landesdatenschutzgesetzes fallen werden.

- Kirchliches Datenschutzrecht

Als relevante nationale Regelung ist allerdings das kirchliche Datenschutzrecht nach dem Gesetz über den kirchlichen Datenschutz (KDG) zu nennen.

In den organisatorischen Anwendungsbereich dieser Regelungen fallen kirchliche Stellen, zu denen u.a. die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform gezählt werden (vgl. § 3 Abs. 1 lit.) c KDG). Nach § 3 Abs. 2 KDG findet das Gesetz auf die Verarbeitung personenbezogener Daten Anwendung, soweit diese im Rahmen der Tätigkeiten eines Verantwortlichen oder eines Auftragsverarbeiters erfolgt, unabhängig davon, wo die Verarbeitung stattfindet, wenn diese im Rahmen oder im Auftrag einer kirchlichen Stelle erfolgt.

Da jedenfalls das Krankenhaus in der Rechtsform einer kirchlichen Stiftung bürgerlichen Rechts organisiert ist, wird bei der Verarbeitung personenbezogener Daten der datenschutzrechtlich Verantwortliche bzw. deren Erfüllungsgehilfen das KDG zu beachten sein.

Die Regelungen des KDG gleichen denen der DSGVO in vielen Bereichen. So wurden die Kapitel 1 (Allgemeine Bestimmungen), 2 (Grundsätze) oder 3 (Rechte der betroffenen Personen) des KDG fast unverändert aus den Regelungen der DSGVO übernommen.
Insbesondere sind Voraussetzungen, die das KDG an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten stellt (vgl. § 6 Abs. 1 KDG), weitestgehend mit denen der DSGVO vergleichbar, diese enthalten lediglich Konkretisierungen hinsichtlich des kirchlichen Kontextes.

Entscheidende Unterschiede sind bei möglichen Bußgeldern zu verzeichnen, denn kirchliche Stellen sind von Geldbußen ausgenommen. Zudem finden sich weitere Unterschiede beispielsweise bezüglich der Anforderungen an eine Einwilligung (§ 8 KDG), welche im KDG strenger gefasst sind als die der DSGVO. Soweit also eine Einwilligung die rechtliche Grundlage für eine Verarbeitung personenbezogener Daten sein soll (vgl. § 6 Abs. 1 lit. b) KDG), sind grundsätzlich § 4 Ziff. 13 KDG und § 8 KDG zu beachten. Danach erfordert eine wirksame Einwilligungserklärung u.a. die Schriftform, die nur in Ausnahmefällen entbehrlich ist. Bei der Verarbeitung besonderer Kategorien von personenbezogener Daten, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen (vgl. § 8 Abs. 4 KDG).

Das sog. Datengeheimnis wird in § 5 KDG ausdrücklich geregelt, in der DSGVO dagegen nicht. Das Datengeheimnis besagt, dass es den bei der Verarbeitung personenbezogener Daten tätigen Personen untersagt ist, diese unbefugt zu verarbeiten, wobei dies aus nach Beendigung der Tätigkeit gilt. Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten.
Zu beachten ist darüber hinaus, dass nach § 36 KDG alle kirchlichen Stellen im Sinne des § 3 Abs. 1 lit. a) KDG schriftlich einen betrieblichen Datenschutzbeauftragten benennen müssen. Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. b) und c) KDG benennen schriftlich einen betrieblichen Datenschutzbeauftragten, wenn
a) sich bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen,
b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 besteht.

Die Besonderheiten des kirchlichen Datenschutzrechts werden folglich im Rahmen des geplanten Vorhabens zu berücksichtigen sein, wobei je nach Verarbeitungsvorgang, Kategorie der zu verarbeitenden Daten oder der betroffenen Personen unterschiedliche Voraussetzungen für die Rechtmäßigkeit der Verarbeitung erfüllt sein müssen.

- Krankenhausgesetze

Die in Art. 9 Abs. 2 DSGVO enthält in Bezug auf die Verarbeitung von sensiblen Daten im Gesundheitsbereich verschiedene Öffnungsklauseln, von denen der nationale Gesetzgeber in Deutschlands u.a. über die Krankenhausgesetze einiger Bundesländer Gebrauch gemacht hat.

- §§ 27 ff. Brandenburgisches Krankenhausentwicklungsgesetz (BbgKHEG)

Nach § 27 Abs. 1 BbgKHEG gilt ergänzend zu der DSGVO das Brandenburgische Datenschutzgesetz, soweit in diesem Gesetz oder anderen Spezialgesetzen, die Regelungen über die Datenverarbeitung von Patientendaten durch Krankenhäuser treffen, nichts anderes bestimmt ist.

§ 28 BbgKHEG enthält eine Erlaubnisnorm zur Verarbeitung von Patientendaten u.a. zum Zwecke der Behandlung von Patienten einschließlich der notwendigen Dokumentation.

---

***Exkurs: Patientendaten***

Zwar enthält die DSGVO eine Definition für Gesundheitsdaten als besonders schutzbedürftige Daten, der Begriff der Patientendaten ist jedoch nicht näher definiert.

Nach § 27 Abs. 2 BbgKHEG sind Patientendaten „alle Einzelangaben über persönliche oder sachliche Verhältnisse

1. bestimmter oder bestimmbarer Patientinnen oder Patienten aus dem Bereich der Krankenhäuser
2. von deren Angehörigen und anderen Bezugspersonen und
3. sonstiger Dritter,

die dem Krankenhause im Zusammenhang mit einer stationären, teilstationären oder ambulanten Behandlung bekannt werden.

---

- Weitere bereichsspezifische Rechtsgrundlagen

Weitere nationale bereichsspezifische Regelungen könnten sich für den Gesundheitsbereich aus den Regelungen der SGBs und des IfSG ergeben.

**b) nationale Vorschriften in Polen**

Der nationale Gesetzgeber in Polen hat von den in der DSGVO enthaltenen Öffnungsklauseln lediglich in begrenztem Umfang Gebrauch gemacht.

Zwar wurden einige polnische Gesetze nach Geltung der DSGVO teils reformiert und ergänzen die Regelungen an einigen Stellen, jedoch betreffen die geänderten Regelungen nicht die hier zu betrachtende Materie der Verarbeitung von Gesundheitsdaten, weshalb aus dem nationalen Recht Polens keine strengeren Vorschriften zu befürchten sind.

**VIII. Konkrete Problematiken in Bezug auf das geplante Vorhanden**

**1. Wer ist der datenschutzrechtlich Verantwortlicher?**

Innerhalb des eigenen Geschäftsbetriebes wird jeder der beteiligten Akteure datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Ziff. 7 DSGVO sein.

Im Hinblick auf das geplante Vorhaben erscheint jedoch auch eine gemeinsame Verantwortlichkeit (vgl. Art. 4 Ziff. 7 i.V.m. Art. 26 Abs. 1 S.1 DSGVO) denkbar.

Entscheidendes Merkmal der gemeinsamen Verantwortlichkeit ist, dass die Beteiligten gemeinsam sowohl Zweck als auch Mittel der Datenverarbeitung festlegen.

Da die Anforderungen einer gemeinsamen Verantwortlichkeit relativ gering sind, braucht es keine gleichberechtigte Entscheidungskompetenz und kein gleichrangiges Interesse aller Beteiligten oder gar eine gleichwertige Verantwortung hinsichtlich der Datenverarbeitung. Ausreichend ist im Wesentlichen, dass von jedem Beteiligten ein Beitrag zur Entscheidung über die Zwecke und Mittel einer Verarbeitung erbracht wird. Demzufolge kann sogar jeder der Beteiligten unterschiedliche Zwecke mit der beabsichtigten Datenverarbeitung verfolgen.

Wichtig für das geplante Vorhaben ist, dass im Falle einer gemeinsamen Verantwortlichkeit nach Art. 26 Abs. 1 S. 2 DSGVO eine Vereinbarung zwischen den Beteiligten erforderlich ist. Zwar schreibt die Vorschrift keine bestimmte Form für eine solche Vereinbarung vor, jedoch ist hier jedenfalls die Textform (im Sinne § 126b BGB) anzuraten. Außerdem empfiehlt sich zumindest die Textform, da das „wesentliche der Vereinbarung“ dem Betroffenen zur Verfügung gestellt werden muss (vgl. Art. 26 Abs. 2 S.2 DSGVO).

Bezüglich des Inhalts der Vereinbarung gilt, dass das tatsächlich gelebte und nicht das vereinbarte Vertragsverhältnis entscheidend ist.

Die gemeinsam Verantwortlichen haften gem. Art. 82 Abs. 2 S. 1, Abs. 4 DSGVO gesamtschuldnerisch, weshalb ein Betroffener einen ihm entstandenen Schaden von jedem der Verantwortlichen voll ersetzt verlangen kann. Der in Anspruch genommene Verantwortliche muss sich sodann im Innenverhältnis an die weiteren Verantwortlichen wenden, um diese anteilig am ausgeglichenen Schaden zu beteiligen.

---

***Exkurs: Abgrenzung gemeinsame Verantwortlichkeit – Auftragsverarbeitung***

In dem Merkmal der gemeinsamen Festlegung von Zweck und Mittel der Datenverarbeitung, unterscheidet sich die gemeinsame Verantwortlichkeit von der Auftragsverarbeitung. Bei Letzterer bestimmt der Verantwortliche Zweck und (in der Regel auch) die Mittel, die ein anderer weisungsabhängig ausführt.

**Hinweis:** Hält sich ein Auftragsverarbeiter nicht an die Vorgaben/Weisungen des Verantwortlichen und bestimmt unter Verstoß gegen die Maßgaben der DSGVO die Zwecke und Mittel der Verarbeitung, gilt er in Bezug auf diese Verarbeitung als Verantwortlicher (vgl. Art. 28 Abs. 10 DSGVO).

In die grundlegenden Überlegungen und Vereinbarungen wird also auch eine Festlegung von Kompetenzen bezüglich der Bestimmung von Zweck und Mittel von Datenverarbeitungsvorgängen aufzunehmen sein.

---

**2. Zweckbindungsgrundsatz**

Nach Festlegung der Verarbeitungszwecke im Sinne des Art. 5 Abs. 1 lit b) DSGVO ist es in der Praxis nicht unüblich, dass sich nachträglich weitere Zwecke ergeben, zu denen die Daten verarbeitet werden sollen. Solche Zweckänderungen sind unter gewissen Voraussetzungen grundsätzlich möglich, können jedoch im Einzelfall problematisch sein. Umso wichtiger ist es, dass die Verarbeitungszwecke zuvor dezidiert zusammengetragen werden.

Ungeachtet der Voraussetzungen für eine Zulässigkeit von Zweckänderungen, ziehen diese Folgen für die Informationspflichten des Verantwortlichen mit sich sowie ggf. eine Anpassung der Verzeichnisse über Verarbeitungstätigkeiten.

**3. Informationspflichten**

In der ordnungsgemäßen Erfüllung der Informationspflichten wird für das geplante Vorhaben ein entscheidender Baustein liegen, um die Verarbeitung personenbezogener Daten insgesamt rechtmäßig zu gestalten. Demzufolge sollte ein besonderes Augenmerk auf die Erarbeitung entsprechender Entwürfe für Patienteninformationen gelegt werden, welche das angedachte Vorhaben des Datentransfers zwischen den beteiligten Akteuren beinhalten müssen.

**4. Datenschutzfolgenabschätzung**

Insbesondere bei einer umfangreichen Verarbeitung von besonderen Kategorien von personenbezogenen Daten gem. Art. 9 Abs. 1 DSGVO ist eine Datenschutz-Folgenabschätzung durchzuführen (vgl. Art. 35 Abs. 3 lit. b) DSGVO. Folglich wird könnte diese Verpflichtung auch für das geplante Vorhaben zum Tragen kommen.

Denn insbesondere der Verarbeitung von Gesundheits- und Patientendaten als sensible Daten ist ein hohes Datenschutzrisiko immanent.

**5. Datenschutzbeauftragter**

Für jeden der drei Akteure wird zu prüfen sein, ob nach den Regelungen der DSGVO oder des BDSG eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht.

Eine aus Art. 37 Abs. 1 lit. c) DSGVO resultierende Benennungspflicht käme in Betracht, wenn die Kerntätigkeit der Verantwortlichen u.a. in der umfangreichen Verarbeitung besonderer Kategorien von Daten im Sinne des Art. 9 Abs. 1 DSGVO (wie z.B. Gesundheitsdaten) besteht. Dies dürfte insbesondere für Krankenhäuser, für Labors oder für Arztpraxen, die genetische Daten verarbeiten zutreffen, nicht dagegen für einzelne Arztpraxen (vgl. ErwGr. 91 S. 4).

Für das Krankenhaus als kirchliche Stiftung wird sich die Verpflichtung zur Benennung eines Datenschutzbeauftragten aus der nationalen und bereichsspezifischen Regelung des § 36 KDG ergaben. Es ist davon auszugehen, dass das Krankenhaus bereits über einen Datenschutzbeauftragten verfügt.

**6. Rechtsgrundlagen der Datenverarbeitung**

In Bezug auf das geplante Vorhaben wird insbesondere die Verarbeitung von Patientendaten als Gesundheitsdaten den Dreh- und Angelpunkt der Beurteilung einer datenschutzrechtlichen Zulässigkeit von Datenverarbeitungsvorgängen bilden.

Hinsichtlich der anwendbaren Rechtgrundlagen für die jeweiligen Verarbeitungsvorgänge zu prüfen sein, welche rechtlichen Grundlagen zum Tragen kommen können.

Nach dem unter Punkt VII. Gesagten wird eine maßgebliche Rechtsgrundlage die Einwilligung des Patienten darstellen, soweit es um die Verarbeitung von Gesundheitsdaten geht. Diesbezüglich werden bei Akteuren in kirchlichen Rechtsformen die Regelungen des KDG ergänzend bzw. konkretisierend zur DSGVO herangezogen und beachtet werden müssen.

Der Alltag im Gesundheitswesen lässt Fälle erwarten, in denen es dem Patienten nicht möglich sein wird, eine den Anforderungen an eine wirksame Einwilligung genügende Willensbekundung abzugeben (z. B. Bewusstlosigkeit des Patienten). Für diese Fälle kommt u.a. der Tatbestand nach Art. 9 Abs. 2 lit c) DSGVO in Betracht. Dieser erfordert, dass die Person einwilligen würde, wenn sie denn könnte. Die Voraussetzung für die Verarbeitung der Daten des Abs. 1 ist dementsprechend die mutmaßliche Einwilligung (vgl. *Paal/Pauly/Frenzel DS-GVO Art. 9 Rn. 29*, m.w.N.). Die Person muss dabei aus körperlichen oder rechtlichen Gründen verhindert sein, die Einwilligung zu erteilen (vgl. *Paal/Pauly/Frenzel DS-GVO Art. 9 Rn. 30*).

Ein weiterer in Betracht kommender Erlaubnistatbestand ist Art. 9 Abs. 2 lit. h) DSGVO. Die Verarbeitung sensibler Daten ist danach zulässig, wenn sie für die Zwecke der Gesundheitsvorsorge oder Arbeitsmedizin, zur Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheitsbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich ist.

**7. Übermittlung von personenbezogenen Daten**

Da die Datenübermittlung eine Form der Datenverarbeitung darstellt, gelten für Erstere dieselben bereits genannten Datenverarbeitungsgrundsätze (Art. 5 DSGVO) sowie das Erfordernis einer Rechtsgrundlage, welche die Verarbeitung erlaubt (Art. 6 DSGVO u.a.).

Die Übermittlung von personenbezogenen Daten zwischen Unternehmen kann im Wesentlichen in drei Kategorien eingeordnet werden:

- Übermittlung innerhalb eines Unternehmens bzw. zwischen Unternehmen eines Konzerns
- Übermittlung an Dritte
- Übermittlung an einen weisungsgebundenen Dienstleister (Auftragsverarbeiter)

Mangels konkreter Kenntnisse über die gesellschaftsrechtlich aufzubauenden Strukturen, soll hier nur allgemein auf vereinzelte Aspekte des Datentransfers eingegangen werden.

**a) Übermittlung innerhalb der Akteure**

- Datenübermittlung innerhalb eines Akteurs

Unkritisch im Zusammenhang mit dem geplanten Vorhaben erscheint die Weiterleitung von Patientendaten innerhalb eines Akteurs (z.B. zwischen verschiedenen Abteilungen des Krankenhauses), soweit diese unter Beachtung der Verarbeitungsgrundsätze nach Art. 5 DSGVO und mit einer erforderlichen Erlaubnis im Sinne des Art. 9 Abs. 2 DSGVO erhoben wurden. In diesem Zusammenhang ist insbesondere auf ein strenges Berechtigungskonzept zu achten. Innerhalb eines Akteurs, der in einer kirchlicher Rechtsform organisiert ist, ist zudem § 5 KDG zu beachten, der die Verpflichtung auf das Datengeheimnis regelt.

- Datenübermittlung innerhalb von Unternehmen eines Konzerns

Riskobehafteter gestaltet sich beispielsweise der Datentransfer innerhalb von Unternehmen eines Konzerns. Da der Fall der Datenübermittlung nicht gesondert in der DSGVO geregelt wird, lässt sich insoweit aus den Bestimmungen der DSGVO kein sog. Konzernprivileg ableiten, aus welchem sich die generelle Zulässigkeit der Datenübermittlung im Konzern ergeben würde (vgl. *Thüsing, § 16, Rn. 3*).

Aus dem ErwGr 48 ergibt sich lediglich eine Besonderheit hinsichtlich eines berechtigten Interesses des Verantwortlichen, der Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen ist. Diese Verantwortlichen können ein berechtigtes Interesse daran haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.

Im Zusammenhang mit den Datenübermittlungen kann wiederum die Frage der gemeinsamen Verantwortlichkeit relevant werden.

Eine tiefgreifende Auseinandersetzung ist nicht Gegenstand dieses Gutachtens, denn diese bedarf des Vorliegens von Detailkenntnissen in Bezug auf die zukünftige Zusammenarbeit.

**b) Übermittlung an Dritte**

Die grundlegende Frage ist zunächst, wer datenschutzrechtlich als „Dritter“ zu betrachten ist.

Die gesetzliche Definition des Art. 4 Ziff. 10 DSGVO beschreibt als Dritte eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Ein Datentransfer zwischen dem Verantwortlichen und dem Dritten ist stets eine erlaubnispflichtige Übermittlung im datenschutzrechtlichen Sinne (vgl. *Thüsing, § 16, Rn. 13*).

Speziell zu betrachten und zu prüfen sind Datenweitergaben an Dritte mit Sitz außerhalb der EU.

**c) Form der Übermittlung**

Bei der Wahl der Übermittlungsform ist insbesondere an das Haftungsrisiko zu denken, welche bei Datenverlust grundsätzlich beim Übermittler/Versender der Daten liegt.

Bezüglich der verschiedenen Übermittlungsformen werden vordergründig digitale Wege in Betracht kommen und der postalische Weg wird voraussichtlich eine untergeordnete Rolle spielen.

Bei sämtlichen digitalen Übertragungswegen ist dem besonderen Schutzbedürfnis von Gesundheitsdaten Rechnung zu tragen und eine geeignete Verschlüsselung (nach dem aktuellen Stand der Technik) einzusetzen.

Bei einem E-Mail-Versand wird es nicht genügen, die versendeten Anhänge zu verschlüsseln, wenn sich aus der Betreffzeile oder dem E-Mail-Text ein Personenbezug herstellen lässt. Hier müsste also der E-Mail-Text mit seiner Betreffzeile soweit pseudonymisiert werden, dass keine Bestimmung der Betroffenen in Verbindung mit dem Anhang erfolgen kann.

Probleme können v.a. bei Übermittlungen per Telefax auftreten, da hierbei das größte Risiko beim Empfänger liegt. Regelmäßig wird ungewiss sein, welche Technologie beim Empfänger zum Einsatz kommt. Folglich sollte von einer Übermittlung von Patientendaten per Telefax grundsätzlich abgesehen werden.

Beim Einsatz von Clouddiensten oder anderen Dienstleistern wird darauf zu achten sein, dass DSGVO-konforme Anbieter eingesetzt werden, bestenfalls mit Sitz und Serverstandort in Deutschland oder jedenfalls innerhalb der EU.

**8. Datenschutzkonzepte**

Jedes der beteiligten Unternehmen sollte ein Datenschutzkonzept vorhalten, welches sich nicht nur mit der eigenen unternehmerischen Situation auseinandersetzt, sondern vielmehr auch die besondere Verarbeitungssituation zwischen den drei Akteuren erfasst.

Dabei ist insbesondere ein streng zu beurteilendes Berechtigungskonzept einzubeziehen und es sind technische und organisatorische Maßnahmen (TOMs) festzuhalten, welche die Sicherheit der Datenverarbeitung gewährleisten sollen. Diese TOMs sind in den Verarbeitungsverzeichnissen zu erfassen.

## IX. Zu klärende Fragen und Punkte

Wesentlich wäre die Klärung folgender Fragen:
Wie werden die Verantwortlichkeiten zwischen den Akteuren gestaltet (Stichwort: gemeinsame - datenschutzrechtliche – Verantwortlichkeit)? Wie werden die rechtlichen Strukturen zwischen den Beteiligten gestaltet.
Welche konkreten Prozesse zur Verarbeitung personenbezogener Daten werden im Einzelnen geplant?
Welche Verarbeitungszwecke kommen im Rahmen der Verarbeitungsprozesse in Betracht?
Festlegung der Verarbeitungszwecke (Wichtig: Allein aus der Existenz einer rechtlichen Grundlage für die Datenverarbeitung ist keine Zweckfestlegung abzuleiten. Die Zweckfestlegung ist sozusagen ein „Mehr“ zum Erfordernis der Verarbeitungsgrundlage.)
In welcher Form soll der angedachte Datentransfer hauptsächlich erfolgen? Werden bereits Verschlüsselungstechniken genutzt? Welche Software soll bzw. wird bereits eingesetzt? Sind in diesem Zusammenhang Cloudlösungen geplant?
Müssen die Beteiligten einen Datenschutzbeauftragten benennen? Wenn ja, kommt ein gemeinsamer Datenschutzbeauftragter in Betracht, um das gesamte Vorhaben zu betreuen?

**X. Fazit**

Alles in allem sind eine Vielzahl datenschützender Rechtsgrundlagen zu beachten, wobei jedoch keine Hürden zu erwarten sind, die die Datenverarbeitungsprozesse im Hinblick auf das geplante Vorhaben gänzlich verhindern.
Ratsam wird es in dieser Gemengelage sein, die strengsten gesetzlichen Grundlagen in Bezug auf die Verarbeitung von personenbezogenen Daten, speziell im Falle der Gesundheits-/Patientendaten, als Maßstab der Rechtmäßigkeit der Verarbeitungsprozesse anzusetzen.

Benjamin Ehlers
Rechtsanwalt