Gutachten Sekundärnutzung Gesundheitsdaten

im Auftrag von
Interpharma – Verband der forschenden pharmazeutischen Firmen der Schweiz

Co-Autoren: Dr. Ursula Widmer (Dr. Widmer & Partner Rechtsanwälte)
Lukas Bühlmann (MLL Legal), Michael Schüepp (MLL Legal), Max Königseder (MLL Legal)

Datum 26. Juli 2022

Zitierweise: URSULA WIDMER/LUKAS BÜHLMANN ET.AL., Gutachten Sekundärnutzung Gesundheitsdaten, Zürich, 26. Juli 2022

Zusammenfassung

Die vorliegende Analyse veranschaulicht die Vielzahl von grundlegenden Hindernissen in der Schweizer Gesetzgebung, die der Ausschöpfung des grossen Potentials der Sekundärnutzung von Gesundheitsdaten im Wege steht. Ein grosser Teil der aufgezeigten Hindernisse lassen sich nicht mit der hohen Sensitivität von Gesundheitsdaten und einem damit verbundenen Regelungsbedarf begründen. Vielmehr sind sie als unnötig zu bezeichnen und sie werden auch mit der Totalrevision des Bundesdatenschutzgesetzes nicht beseitigt. Das Gutachten zeigt dabei insbesondere die vier folgenden Hindernisse auf und macht Vorschläge zur Verbesserung.

Erstens gleicht der **aktuelle Rechtsrahmen einem Flickenteppich**, der bereits bei der grundlegenden Frage, welchen Regelwerken eine Sekundärnutzung von Gesundheitsdaten überhaupt untersteht, zu unnötiger Unsicherheit führt. Dies ist umso gravierender, als die einzelnen Regelungen auf Bundes- und kantonaler Ebene inhaltlich nicht aufeinander abgestimmt sind und teilweise ohne ersichtlichen Grund abweichende Begrifflichkeiten und Regelungen enthalten. Für die Sekundärnutzung von Gesundheitsdaten, wo Akteure betroffen sind, die nicht nur unterschiedlichen kantonalen Datenschutzgesetzen, sondern auch den verschiedenen Regelungskomplexen für private Verantwortliche oder öffentliche Organe auf Bundesebene unterstellt sein können, ist der Rechtsrahmen im praktischen Alltag kaum mehr fassbar und unnötig komplex. Folglich gelangt das Gutachten zum Schluss, dass eine Vereinheitlichung der anwendbaren Vorschriften dringend angezeigt ist. Dies gilt selbstredend auch für neue gesetzgeberische Massnahmen zur Beseitigung der weiteren identifizierten Hindernisse.

Zweitens, die **Unsicherheiten rund um die Anforderungen an die Anonymisierung von Daten** stellen ein zweites zentrales Hindernis dar. In vielen Fällen wäre die Anonymisierung das geeignete und einzige Mittel, um die strengen datenschutzrechtlichen Vorgaben und die damit verbundenen Sanktionsrisiken zu vermeiden. Bedauerlicherweise sind die konkreten Anforderungen nach wie vor unklar oder zumindest umstritten. Für die Praxis der Sekundärnutzung von Gesundheitsdaten wären hierzu gesetzgeberische Klarstellungen angezeigt, namentlich durch Festlegung der massgeblichen Beurteilungs-Perspektive und durch Verankerung von Fällen hinreichender Anonymisierung.

Drittens verdeutlicht das Gutachten, dass die meisten der **gesetzlichen Erlaubnistatbestände, wie z.B. die sog. Forschungsausnahme, nicht die für die Praxis notwendige Absicherung bringen**. Vielmehr ist eine Datenbearbeitung selbst bei der Einhaltung der darin vorgesehenen Voraussetzungen noch nicht per se rechtmässig und es ist eine Prüfung sämtlicher Umstände im Einzelfall erforderlich. Dies gilt es zu vermeiden. Weiter sind auch die Anforderungen an eine gültige Einwilligung (insb. den Generalkonsent), als zentraler Erlaubnistatbestand, klarzustellen und es sind digitale Lösungen ausdrücklich für zulässig zu erklären. Förderlich für die Rechtssicherheit wäre in diesem Zusammenhang zudem die Schaffung einer institutionalisierten Möglichkeit, in bestimmten Fällen die datenschutzrechtliche Genehmigung einer zuständigen Behörde für geplante Sekundärnutzungen einholen zu können. Ein möglicher Ansatz könnte darin bestehen, die Bewilligung durch Ethikkommissionen auf die datenschutzrechtlichen Belange zu erstrecken.

Viertens ist die geltende **Regelung der Datenbekanntgabe ein grosses Hindernis für den Datenaustausch unter den involvierten Akteuren**. So besteht, auf der Basis der Unklarheiten zur Anonymisierung, auch eine erhebliche Unsicherheit darüber, wann von einer hinreichenden Pseudonymisierung auszugehen ist und inwiefern das Zugänglichmachen von pseudonymisierten Daten eine Bekanntgabe im datenschutzrechtlichen Sinne darstellt. Dies gilt es klarzustellen und es muss vordringlich auch Rechtssicherheit geschaffen werden in Bezug auf die Regelungen zur Datenbekanntgabe ins Ausland. Es ist namentlich zeitnah ein rechtssicherer Einsatz von Diensten von Anbietern mit US-Bezug zu ermöglichen. Schliesslich muss der künftige rechtliche Rahmen auch einheitliche technische Standards vorsehen und den sog. FAIR-Grundsatz sicherstellen. Für die Verwirklichung des Potentials der Sekundärnutzung von Gesundheitsdaten braucht es insbesondere auch eine deutliche Verbreiterung der Einsatzfähigkeit des elektronischen Patientendossiers und eine Interoperabilität zwischen den verschiedenen Infrastrukturen und IT-Systemen der Institutionen des Gesundheitswesens.

Inhaltsverzeichnis

1. Auftrag Gutachten

Gestützt auf unsere Vorgespräche und die von Ihnen zur Verfügung gestellten Vorarbeiten sowie unsere E-Mail-Korrespondenz finden Sie nachfolgend unser Gutachten zur rechtlichen Zulässigkeit der Sekundärnutzung von Gesundheitsdaten in der Schweiz.

Das Gutachten beinhaltet die vereinbarten Themen und Use Cases:

1. *Gesundheitsdaten als rechtlicher Spezialfall vor dem Hintergrund des grossen öffentlichen Interesses an der umfassenden Nutzung einerseits und dem erhöhten Schutzbedürfnis mit Fokus auf den Datenschutz andererseits.*

2. *Übersicht über die aktuellen Rahmenbedingungen der Sekundärnutzung von Gesundheitsdaten im Schweizer Recht. Wir untersuchen die zentralen bundesrechtlichen Erlasse sowie einige (max. 3) ausgewählte kantonale Datenschutzgesetze.*

3. *Die Analyse gesetzgeberischer Lücken, Unklarheiten oder Hindernisse, die der Sekundärnutzung von Gesundheitsdaten und der Verwirklichung des damit verbundenen gesellschaftlichen Nutzens im Wege stehen. Diese würden wir anhand von 2-3 ausgewählten Use Cases erarbeiten.*

4. *Vorschläge zur Anpassung des rechtlichen Rahmens unter Berücksichtigung einschlägiger Rechtsentwicklungen auf europäischer Ebene.*

Folgende Use Cases wurden bei der Analyse der Rechtsgrundlagen und der Vorschläge zur Anpassung des rechtlichen Rahmens berücksichtigt:

Use Case I: Sekundärnutzung im Behandlungs-, Vorsorge- und Früherkennungskontext

Ein Softwareunternehmen entwickelte gemeinsam mit einem Team aus Ärzten und Wissenschaftlern eine Anwendung zur frühzeitigen Erkennung von Autoimmunerkrankungen (z.B. Multiple Sklerose) und zur Bestimmung von Risikopatienten. Diese Anwendung wird von Ärzten im Rahmen der Behandlung eingesetzt und greift dabei zur Erkennung von Mustern auf pseudonymisierte (oder anonymisierte) Patientendaten verschiedener Spitäler zu. Darüber hinaus wird das Patientendossier der betroffenen Person in die Anwendung eingelesen, um Rückschlüsse auf etwaige Vorerkrankungen und Risikofaktoren zu erhalten. Der Patient hat zusätzlich die Möglichkeit, Daten, die über eine Smartwatch erhoben werden (Puls, Bewegungsmuster und weitere Daten zur körperlichen Verfassung) zur Verfügung zu stellen. Um Rückschlüsse auf familiäre Risikofaktoren zu erhalten, sollen Patientendossiers von verstorbenen und lebenden Angehörigen zur Verfügung gestellt werden. Die Anwendung errechnet das individuelle MS-Risiko des Patienten und gibt eine Handlungsempfehlung ab, wie oft sich die betroffene Person einer Kontrolluntersuchung unterziehen soll.

Use Case II: Sekundärnutzung im Forschungskontext

Im Rahmen eines Forschungsprojekts sollen mithilfe von künstlicher Intelligenz (KI) fortschrittliche Modelle entwickelt werden, um eine effektivere Behandlung einer bestimmten Krebsart (z.B. Prostatakrebs) zu ermöglichen. Insbesondere soll das Forschungsprojekt zu einer Verbesserung der Diagnose, der Erkennung von Metastasen und der Vorhersage des Ansprechens auf die Behandlung führen.

Um diese Ziele zu erreichen, benötigt das Forschungsteam grosse Mengen an Gesundheitsdaten. Einerseits wollen die Forscher eine Datenbank, bestehend aus pseudonymisierten (oder anonymisierten) Prostata-

MRI-Scans und den dazugehörigen Patientendaten, welche im Rahmen der Krebstherapie angefertigt wurden, erstellen. Mithilfe dieser Scans soll eine KI-Anwendung trainiert werden, welche zu einer verbesserten Diagnose beiträgt. Zusätzlich soll genetisches Material und Blutproben gesammelt werden, um die Diagnosefähigkeiten der KI-Anwendung zu verbessern. Die Daten sollen aus verschiedenen Schweizer Spitälern und onkologischen Arztpraxen sowie aus anderen Forschungsprojekten stammen. Mit prospektiven Studien soll der Nutzen für den Patienten bestimmt werden, um die Wirksamkeit von verschiedenen (z.B. medikamentösen) Behandlungsmethoden mit Hilfe dieser Anwendung zu testen. Dafür ist ein Zugriff auf die Primärsysteme der Spitäler oder die elektronischen Patientendossiers der Probanden notwendig.

Use Case III: Sekundärnutzung für gesundheitspolitische Zwecke

In der Schweiz grassiert eine Pandemie, zu deren Bekämpfung politische Entscheidungsträger schnell über eine umfassende und aktuelle Faktenlage verfügen müssen. Die zuständigen Gesundheitsbehörden benötigen dazu einen Zugriff auf tagesaktuelle Gesundheitsdaten der Erkrankten. Die Verknüpfung dieser Daten mit der AHV-Nummer der Erkrankten ermöglicht die kontinuierliche Überwachung der Infektionen und des Expositionsrisikos gefährdeter Personen, sollte die Pandemie für eine bestimmte Altersgruppe ein erhöhtes Risiko darstellen. Hiervon versprechen sich die Entscheidungsträger der öffentlichen Hand unter anderem genaue Modellvorhersagen über den künftigen Bedarf an Spitalressourcen (ärztliches und nicht-ärztliches Gesundheitspersonal, Betten, medizinische Hilfsmittel).

2. Begriff der Sekundärnutzung

Das vorliegende Gutachten untersucht die Rahmenbedingungen der Sekundärnutzung von Gesundheitsdaten im Schweizer Recht.

In einem ersten Schritt ist deshalb zu klären, was unter Sekundärnutzung zu verstehen ist. Im Gesundheitssektor wird regelmässig die Nutzung von Gesundheitsdaten im Zusammenhang mit einer medizinischen Behandlung als Primärnutzung betrachtet. Ausgehend davon werden sodann jegliche anderen Bearbeitungen, namentlich die Nutzung im Rahmen der Gesundheitsforschung und Gesundheitspolitik, als Sekundärnutzung verstanden.[1]

Dies ist jedoch unpräzis und verleitet zu falschen Annahmen. Wie die Erläuterung der rechtlichen Rahmenbedingungen zeigen wird, muss datenschutzrechtlich von einem engen Verständnis des Zwecks ausgegangen werden. Bei der Erhebung von Gesundheitsdaten muss der Bearbeitungszweck bereits spezifiziert oder zumindest erkennbar sein. Es muss für eine Patientin oder einen Patienten somit bspw. klar sein, dass die Nutzung seiner Gesundheitsdaten zum Zweck der Behandlung der von ihm bezeichneten Symptome erfolgt. Eine Datenbearbeitung, die über diesen primären Zweck hinausgeht oder für andere Zwecke erfolgt, wird als Sekundärnutzung bezeichnet.[2] Deshalb kann auch die Verwendung von Gesundheitsdaten im Rahmen der Behandlung eine Sekundärnutzung darstellen und es ist bei der Verwendung der Begriffe Vorsicht geboten.

---

1 Vgl. z.B. die EU-Kommission, Study on health data, digital health and artificial intelligence in healthcare, 2022, S. 13; die Website der EU-Kommission zum European Health Data Space: https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_de?2nd-language=de (zuletzt aufgerufen am 16.05.2022); ferner auch ROITINGER/RACHAMIN/ANTONOV, Chancen und rechtliche Herausforderungen bei der Nutzung von Real World Data, LSR 2022, S. 4.

2 SPRECHER, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 154/2018, S. 482 (508); GORDON, Daten aus Selbstvermessung, digma 2016 S. 70 ff.

Wenn nachfolgend von Sekundärnutzung die Rede ist, sind deshalb aber auch diese Fälle gemeint. Das vorliegende Gutachten umfasst insofern Sekundärnutzungen im Bereich der Gesundheitsbehandlung, der Gesundheitsforschung und der Gesundheitspolitik, wie sie in den oben in Abschnitt 1 aufgeführten Use Cases zum Ausdruck kommen.

Für das Begriffsverständnis ist es wichtig, bereits hier zu betonen, dass die Datenbearbeiter es bis zu einem gewissen Grad selbst in der Hand haben, die Zwecke der Datenbearbeitungen bei der Erhebung der Daten festzulegen. So können unter Umständen bereits zu diesem Zeitpunkt mehrere unterschiedliche Bearbeitungszwecke festgelegt werden.[3] Einem Spital ist es deshalb bspw. unter Einhaltung gewisser Voraussetzungen gestattet, bei der Erhebung von Personendaten seiner Patientinnen und Patienten bereits festzulegen, dass die Daten nicht nur zur Behandlung, sondern auch zur Forschung verwendet werden. In diesem Fall ist auch die Bearbeitung der Patientendaten zur Forschung rein rechtlich betrachtet eine Primärnutzung, also eine Nutzung im Rahmen des originären, bei der Erhebung festgelegten Zwecks und es erfolgt keine Zweckänderung. Wir verwenden nachfolgend gleichwohl auch für diese Fälle die Bezeichnung Sekundärnutzung, da dies unserer Erfahrung nach besser dem Verständnis im geschäftlichen Alltag entspricht.

3. Gesundheitsdaten als rechtlicher Spezialfall

Für die Beantwortung der Frage, inwiefern Gesundheitsdaten einen rechtlichen Spezialfall darstellen, ist zunächst zu klären, was in den massgeblichen Rechtsvorschriften unter Gesundheitsdaten verstanden wird. Hierfür wird auf die zwei für das vorliegende Gutachten wesentlichen Regelwerke eingegangen: Das Datenschutzgesetz des Bundes (DSG)[4] und das Humanforschungsgesetz (HFG)[5]. Wie noch zu zeigen ist, haben diese Gesetze einen breiten Anwendungsbereich und die darin verankerten inhaltlichen Vorgaben sind entscheidend für die rechtliche Sonderbehandlung von Gesundheitsdaten.

3.1 Begriff der Gesundheitsdaten im Schweizer Datenschutzgesetz des Bundes

3.1.1 Vorbemerkungen

Das DSG gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane. Bereits dadurch veranschaulicht sich der breite Anwendungsbereich des Gesetzes. Für die Darstellung des Sonderfalls der Gesundheitsdaten erübrigt es sich, alle Aspekte des Anwendungsbereichs im Detail aufzuzeigen. Zentral ist das Verständnis von Daten bzw. von personenbezogenen Gesundheitsdaten, die bei der Sekundärnutzung einer datenschutzrechtlich relevanten Bearbeitung unterzogen werden. Ist im vorliegenden Gutachten von Daten die Rede, sind damit, ohne gegenteilige Hinweise, primär personenbezogene Daten gemeint.

Hervorzuheben ist bereits an dieser Stelle, dass von einem sehr breiten Verständnis des Bearbeitens von personenbezogenen Gesundheitsdaten auszugehen ist. Darunter versteht man jeden "Umgang mit Perso-

---

3 Siehe dazu die Ausführungen zum Zweckbindungsgebot, insb. Abschnitt 4.1.4a) ii.).

4 Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 19. Juni 1992, SR 235.1 (im Folgenden: DSG).

5 Bundesgesetz über die Forschung am Menschen (Humanforschungsgesetz, HFG) vom 30. September 2011, SR 810.30 (im Folgenden: HFG).

nendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten".[6] Hierbei handelt es sich lediglich um eine exemplarische Aufzählung. Das weite Begriffsverständnis der Bearbeitung umfasst jeglichen Umgang mit Personendaten.[7]

3.1.2 Definition Personendaten

a) Allgemeine Voraussetzungen

Das noch geltende DSG definiert Personendaten in Art. 3 lit. a DSG als "alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen". Eine Besonderheit des DSG ist, dass vom Begriff der "betroffenen Person", deren Daten bearbeitet werden, auch juristische Personen umfasst sind. Dieses Schweizer Unikum wird im Zuge der Totalrevision auf Bundesebene (nicht aber in allen Kantonen[8]) abgeschafft. Demzufolge sind ab dem Inkrafttreten des nDSG[9] – voraussichtlich am 1. September 2023[10] – nur noch natürliche Personen vom Schutzbereich des DSG umfasst[11]. Die Begriffsdefinition von Personendaten bleibt durch die Totalrevision – mit Ausnahme der erwähnten Einschränkung auf natürliche Personen – unverändert und entspricht weitgehend derjenigen der EU-DSGVO[12]. Die neue Definition in Art. 5 lit. a. nDSG lautet wie folgt: "Personendaten**:** alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen".

Der Begriff der Angabe ist weit zu verstehen; darunter ist jede Art von Information oder Aussage zu subsumieren, und zwar jeder Art, jeden Inhalts und in jeglicher Form.[13] Die erwähnte Angabe muss einen Bezug zu einer oder mehreren Personen aufweisen. Dies kann eindeutig bejaht werden, sofern sich die Angabe direkt auf die Person bezieht (z.B. Name, Ergebnisse einer medizinischen Untersuchung, Fingerabdruck). Neben diesen offensichtlichen Fällen sind auch Angaben umfasst, die sich indirekt auf eine Person beziehen lassen. Hierbei kann es sich beispielsweise um Information zu Vorgängen, Ereignissen oder Sachen handeln, die

---

6 Art. 3 lit. e DSG bzw. Art. 5 lit. d nDSG.

7 ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 63.

8 Vgl. nachfolgend Abschnitt 4.3.1.

9 Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020, Schlussabstimmungstext, BBl 2020 7639 ff. (im Folgenden: nDSG).

10 Vgl. Website des Bundesamtes für Justiz: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html (zuletzt aufgerufen am 21.04.2022).

11 Art. 5 Abs.1 nDSG; Website des Bundesamtes für Justiz: https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf.download.pdf/vorentw-d.pdf (zuletzt aufgerufen am 21.04.2022); hingegen gilt der Schutz des allgemeinen Persönlichkeitsrechts gem. Art. 28 ZGB nach wie vor auch für juristische Personen.

12 Vgl. Art. 4 Ziff. 1 DSGVO.

13 ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 8; Botschaft zum DSG, BBl 1988 S. 444.

aufgrund ihres Kontexts oder mithilfe von Zusatzinformation Schlüsse über Personen zulassen.[14] Beispielsweise könnte eine "Google Street View"-Aufnahme von einem Fahrzeug, das vor einer onkologischen Klinik parkiert ist, indirekt Rückschlüsse auf den Gesundheitszustand des Fahrzeughalters zulassen.[15]

b) "Bestimmbarkeit" im Besonderen

Vom Personenbezug bzw. der Personenbeziehbarkeit ist die Bestimmbarkeit der Person zu unterscheiden. Die Person oder die Personen, auf welche sich die Angaben beziehen oder auf welche sie beziehbar sind, muss bestimmt oder mindestens bestimmbar sein. Ist die Person nicht zumindest bestimmbar, liegen keine Personendaten vor und folglich ist das DSG nicht anwendbar. Eine Person ist bestimmt oder bestimmbar, wenn sich ihre Identität unmittelbar aus den Daten selbst oder aus dem Kontext der Daten oder durch Kombination mit anderen Daten ergibt, solange dies ohne unverhältnismässigen Aufwand möglich ist.[16] Der Aufwand gilt als unverhältnismässig, wenn nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird.[17]

Was genau unter diesen allgemeinen Kriterien verstanden werden muss, ist von grosser Bedeutung für den Umgang mit Gesundheitsdaten. Denn dies entscheidet darüber, inwieweit die gesetzlichen Vorgaben überhaupt zur Anwendung gelangen oder nicht. In seinem Leitentscheid zu dieser Frage qualifizierte das Bundesgericht z.B. sog. (dynamische) IP-Adressen, d.h. (vereinfacht) die von einem Internetzugangsanbieter einem Router zugewiesene technische Adresse, als Personendaten, wenn sie zwecks der Identifizierung des Internetnutzers in einem späteren Strafverfahrens gesammelt werden.[18] Dies gilt nach Ansicht des Bundesgerichts selbst dann, wenn die betroffene Person nicht in allen Fällen eindeutig bestimmbar ist, weil z.B. mehrere Personen Zugriff auf einen Computer oder ein Netzwerk mit derselben IP-Adresse haben.[19]

Nach einer im EU-Recht verbreiteten Auffassung ist der entsprechende Begriff der Identifizierbarkeit i.S.d. DSGVO dahingehend zu verstehen, dass nicht die konkrete Person identifiziert werden muss, sondern, dass auch schon die persönliche Zuordnung einer eindeutigen Kennnummer ausreiche, um in die Datenschutzrechte der betroffenen Person einzugreifen.[20] Nach diesem Ansatz des "Aussonderns" bzw. "Singling-out", welcher u.a. aus dem Erwägungsgrund 26 DSGVO abgeleitet wird, ist entscheidend, ob ein Individuum aus der Menge herausgesucht werden kann.[21] Inwieweit sich diese– sehr weite – Auslegung der Identifizierbarkeit in der EU durchsetzt und ob sie auch Eingang in die Rechtsprechung zum Schweizer Datenschutzrecht finden wird, kann noch nicht abschliessend beurteilt werden.

---

14 ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 14.

15 Vgl. BGE 138 II 346: Bei sensiblen Einrichtungen (Schulen, Spitälern, Altersheimen, Frauenhäusern, Gerichten und Gefängnissen etc.) ist vor der Aufschaltung im Internet die vollständige Anonymisierung von Personen und Kennzeichen vorzunehmen (E. 10.6.4 und 14.2).

16 RUDIN, in: BAERISWYL/PÄRLI (Hrsg.), SHK-DSG, 2015, Art. 3 N 10.

17 RUDIN, in: BAERISWYL/PÄRLI (Hrsg.), SHK-DSG, 2015, Art. 3 N 10.

18 BGer Urteil vom 08.09.2010, 1C_285/2009, E. 3.2 und 3.5.

19 BGer Urteil vom 08.09.2010, 1C_285/2009, E. 3.5.

20 DSB, Teilbescheid 22.12.2021, D155.027 2021-0.586.257; vgl. ferner KARG, in: SIMITIS/HORNUNG/SPIECKER GEN. DÖHMANN (Hrsg.), Datenschutzrecht, 2019, Art. 4 Nr. 1 N 48 ff.; Entscheid CNIL: https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf (zuletzt aufgerufen am 12.05.2022).

21 DSB, Teilbescheid 22.12.2021, D155.027 2021-0.586.257, S. 28.

Im Gegensatz zum Europäischen Datenschutzrecht,[22] wo der genannte Erwägungsgrund als Argument dient, wird das "Aussondern" weder in der Entstehungsgeschichte noch dem DSG selbst explizit erwähnt. Dementsprechend lässt das DSG mehr Spielraum für die Auslegung, dass eine eindeutige Kennnummer und die damit verbundene Möglichkeit des Aussonderns einer Person per se noch kein Personendatum darstellt, sofern dadurch keine natürliche Person namentlich identifiziert werden kann bzw. identifizierbar wird. Unabhängig davon ist der Streitpunkt und die damit verbundene Unsicherheit ein Hindernis, dass die Bearbeitung von vermeintlich bloss pseudonymisierten Daten erschweren kann.

c) Begriff der Anonymisierung

Grundsätzlich sind all die oben in Abschnitt 3.1.2 a) genannten Elemente weit auszulegen, folglich ist eine vollständige Entfernung des Personenbezugs bzw. der Bestimmbarkeit – im Zuge einer Anonymisierung – in der Praxis schwer umzusetzen.[23] Der Begriff der Anonymisierung ist im DSG nicht definiert. Anonymisierte Daten sind aber als Gegensatz zum Begriff der Personendaten zu sehen. Es ist deshalb nach den soeben erläuterten Kriterien zu beurteilen, ob von anonymisierten Daten oder Personendaten auszugehen ist. Handelt es sich um anonymisierte Daten, ist deren Bearbeitung nicht vom Anwendungsbereich des DSG erfasst.

Hierbei ist zu beachten, dass der Prozess der Anonymisierung selbst – also z.B. das Entfernen oder das Austauschen der personenbezogenen Elemente – eine Datenbearbeitung im Sinne des DSG darstellt. Im Gegensatz zur Pseudonymisierung muss die Anonymisierung irreversibel sein.[24] Bei der Beurteilung der Irreversibilität ist wiederum darauf abzustellen, ob der Personenbezug ohne unverhältnismässig grossen Aufwand wieder hergestellt werden kann. In diesem Zusammenhang kann keine pauschale Aussage gemacht werden, wann die Irreversibilität sichergestellt ist, diese Bewertung hat im Einzelfall unter Berücksichtigung der verfügbaren Technologien zu erfolgen.[25] Wie im nächsten Abschnitt beschrieben, ist diese Bewertung aus der relativen Perspektive des jeweiligen Verantwortlichen (und der ihm zuzurechnenden Personen) vorzunehmen.

Mit der Weiterentwicklung der zur Verfügung stehenden Technologien kann nicht davon ausgegangen werden, dass ein Datensatz, der im Zeitpunkt der Anonymisierung als irreversibel erachtet werden kann, dies auch dauerhaft bleibt. Vielmehr muss in regelmässigen Intervallen beurteilt werden, ob die Anonymisierung noch sichergestellt ist. Wie eine Studie von Forschern der Université Catholique de Louvain und dem Imperial College London zeigt, können selbst Daten in äusserst unvollständigen Datensätzen relativ einfach wieder re-identifiziert werden.[26] Das im vorstehenden Absatz beschriebene Erfordernis der Irreversibilität sorgt für Rechtsunsicherheit im Zusammenhang mit der Anonymisierung, umso mehr, wenn, wie in der nächsten

---

22 Erwägungsgrund 26 DSGVO: "*wie beispielsweise das Aussondern*".

23 Vgl. MARTANI/EGLI/WIDMER, Data protection and biomedical research in Switzerland: setting the record straight Swiss Med Wkly. 2020, S. 3; VOKINGER, Gesundheitsdaten im digitalen Zeitalter, in: Jusletter 27. Januar 2020, Rz. 21; EPINEY, Big Data und Datenschutzrecht, in: Jusletter 27. April 2020, Rz. 31; ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 2 und 38.

24 BLECHTA, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 3 DSG Rz.12 und 13.

25 BLECHTA, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 3 DSG Rz.13.

26 ROCHER/HENDRICKX/DE MONTJOYE, Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069 (2019); vgl. Artikel auf nature.com: https://doi.org/10.1038/s41467-019-10933-3.

Ziffer erläutert wird, dabei unterschiedliche Perspektiven einbezogen werden. In den USA sorgt ein pragmatischer Ansatz für klare Rahmenbedingungen: Gesundheitsdaten gelten als endgültig de-identifiziert (d.h. anonymisiert), sobald eine genaue und erschöpfende Liste von 18 persönlichen Identifikatoren entfernt wurde.[27]

Es entwickeln sich jedoch nicht nur die Re-Identifizierungstechnologien weiter, sondern auch die Verschlüsselungstechnologien, welche eine Anonymisierung ermöglichen und gegebenenfalls aufrechterhalten können. In diesem Zusammenhang sind insbesondere die Fortschritte im Confidential Computing zu nennen. Hierbei handelt es sich um eine Technologie, welche die Bearbeitung von Daten in einem Trusted Execution Environment (TEE) – ein verschlüsselter Datenraum – ermöglicht.[28] Hierbei werden die Daten nicht nur verschlüsselt abgelegt ("data at rest"), sondern können auch verschlüsselt bearbeitet werden ("data in use").[29] Die Daten werden somit bei der Bearbeitung nicht unverschlüsselt in den Arbeitsspeicher kopiert und selbst der Provider des TEE hat keine technische Möglichkeit, auf die Daten zuzugreifen. Im Ergebnis bedeutet dies, dass innerhalb des TEE Datenbearbeitungen vorgenommen werden können, jedoch niemand, der nicht hierzu berechtigt wird, Zugriff auf die unverschlüsselten Personendaten hat.

d) Absoluter oder relativer Ansatz der Bestimmbarkeit?

Zentral für die Qualifikation von Gesundheitsdaten als Personendaten ist die Frage, ob es auf die relative oder absolute Bestimmbarkeit der betroffenen Person ankommt. In der Schweiz ist dies zumindest im Grundsatz höchstrichterlich geklärt,[30] während in der EU nach wie vor unterschiedliche Auffassungen vertreten werden.

Es gilt seit dem Logistep-Leiturteil des Bundesgerichts der relative Ansatz, welchen auch die mittlerweile wohl überwiegende Meinung in der EU befürwortet.[31] Nach der bundesgerichtlichen Umschreibung beurteilt sich die Bestimmbarkeit deshalb "*aus der Sicht des jeweiligen Inhabers der Information*".[32] Bei der Beurteilung ist ferner auf objektive (ist die natürliche Person für den Inhaber der Information bestimmbar) und subjektive Kriterien (ist der Inhaber der Information bereit, den für die Identifizierung notwendigen Aufwand zu betreiben) abzustellen.[33]

Nach dem nicht einschlägigen absoluten Ansatz könnte es demgegenüber schon genügen, dass die theoretische Möglichkeit der Identifizierung einer betroffenen Person durch einen beliebigen Dritten besteht.[34]

---

27 MARTANI/EGLI/WIDMER, Data protection and biomedical research in Switzerland: setting the record straight Swiss Med Wkly. 2020; VOKINGER/STEKHOVEN/KRAUTHAMMER, Lost in Anonymization - A Data Anonymization Reference Classification Merging Legal and Technical Considerations. J Law Med Ethics. 2020, S. 228– 231.

28 GORBET, SC Magazine, Vol. 31, Iss. 1, (Feb 2020): 8-9.

29 GORBET, SC Magazine, Vol. 31, Iss. 1, (Feb 2020): 8-9.

30 ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, S. 8; BGE 136 II 508, E. 3.2.

31 Vgl. zum Meinungsstand in der EU: KARG, in: SIMITIS/HORNUNG/SPIECKER GEN. DÖHMANN (Hrsg.), Datenschutzrecht, 2019, Art. 4 Nr. 1 N 57 ff.

32 BGE 136 II 508, E. 3.4.

33 ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, S. 8.

34 Bei diesem Ansatz wäre jedenfalls aber auch zu klären, welche Anforderungen an die theoretische Identifizierungsmöglichkeit gelten sollen, also, ob auch unrechtmässige Handlungen hierzu zählen würden; vgl. zum Ganzen unter der EU-DSGVO KARG, in: SIMITIS/HORNUNG/SPIECKER GEN. DÖHMANN (Hrsg.), Datenschutzrecht, 2019, Art. 4 Nr. 1 N 58.

Die praktischen Auswirkungen des relativen Ansatzes werden in einem Urteil des Handelsgerichts Zürich verdeutlicht.[35] Diesem Entscheid lag die Bekanntgabe eines pseudonymisierten Datensatzes durch eine Schweizer Bank an eine US-Behörde zu Grunde.[36] Das Gericht hatte sich in diesem Verfahren mit der Frage zu beschäftigten, ob eine Bekanntgabe von Personendaten ins Ausland vorliegt, wenn der Empfänger eines pseudonymisierten (oder anonymisierten) Datensatzes nicht über den Schlüssel verfügt, der die Identifizierung der betroffenen Personen erlaubt bzw. der Empfänger mit verhältnismässigem Aufwand keinen Personenbezug herstellen kann.[37] Das Handelsgericht vertrat hierbei grundsätzlich die Auffassung, dass "*für Personen, die keinen Zugang zum Schlüssel haben und auch nicht über andere Kenntnisse verfügen, um die Daten wieder einer bestimmten Person zuordnen zu können, stellen pseudonymisierte Personendaten hingegen keine Personendaten mehr dar*".[38] Demzufolge liegt keine grenzüberschreitende Bekanntgabe von Personendaten i.S.d. DSG vor, "*wenn Personendaten vor der Bekanntgabe ins Ausland so anonymisiert oder pseudonymisiert werden, dass deren Empfänger im Ausland keinen Personenbezug mehr herstellen kann*".[39] Obwohl es der Bank im Zuge dieses Verfahrens nicht gelang, den Beweis zu erbringen,[40] dass vom Empfänger kein Personenbezug mehr hergestellt werden kann, sind die Aussagen dieses Entscheids von wichtiger praktischer Bedeutung für die (grenzüberschreitende) Daten-Bekanntgabe.

Der zitiere Entscheid sorgte für Diskussionen und es wurde vorgebracht, dass damit eine Abkehr vom Logistep-Urteil des Bundesgerichts vollzogen werde. Denn darin führte das Bundesgericht aus, dass es für den Fall einer Weitergabe ausreiche, wenn der Empfänger die betroffene Person zu identifizieren vermag.[41] Es sei deshalb nicht vorausgesetzt, dass die betroffenen Personen (auch) bereits für den Übermittler bestimmbar sind, hingegen sei es ausreichend, wenn sie es nach Übergabe der Daten für den Empfänger werden. In diesem Fall gelange das DSG auch auf den Absender selbst zur Anwendung. Somit rechnete das Gericht die Mittel des Empfängers, welche einer Identifizierung dienen können, auch dem Absender der Daten zu.[42] Diesen vermeintlichen Widerspruch zum Relativitätsgrundsatz löst das Bundesgericht nicht auf. Bereits deshalb kann zumindest die Begründung dieses Ergebnisses nicht überzeugen.[43] Kritikern ist dahingehend zuzustimmen, dass die Entscheidung mangels hinreichender Begründung ergebnisorientiert erscheint.[44] Namentlich wären Erläuterungen zum Verhältnis zwischen Logistep und ihren Auftraggebern und deren datenschutzrechtlichen Rollen erforderlich gewesen.

---

35 HGer ZH, Urteil vom 04.05.2021, HG190107-O; ähnlich: AppGer BS: ZB.2019.3 E. 4.2.2.

36 HGer ZH, Urteil vom 04.05.2021, HG190107-O.

37 HGer ZH, Urteil vom 04.05.2021, HG190107-O.

38 HGer ZH, Urteil vom 04.05.2021, HG190107-O, S. 12 m.H.a. ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 36; RUDIN, in: BAERISWYL/PÄRLI (Hrsg.), SHK-DSG, 2015, Art. 3 N 14.

39 HGer ZH, Urteil vom 04.05.2021, HG190107-O, S. 12; ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 36 und Art. 6 Rz.8.

40 JACOT-GUILLARMOD/HIRSCH, Pseudonymisierung von Bankkundendaten, digma 2020, S. 216 ff.

41 BGer Urteil vom 08.09.2010, 1C_285/2009, E. 3.4.

42 BGer Urteil vom 08.09.2010, 1C_285/2009, E. 3.4.

43 Das BGer nennt das Beispiel einer Zeitungsmeldung über den Unfall eines nicht namentlich genannten Lokalpolitikers, der von der Leserschaft anhand von Zusatzinformationen oder weiterer Recherche identifiziert werden könne. Dieses Beispiel ist untauglich, weil auch die Zeitung – allenfalls durch eine zusätzliche Recherche – die betroffene Person identifizieren kann, somit handelt es sich ohnehin sowohl aus der Perspektive des Senders (der Zeitung) und der Empfänger (die Leserschaft) um Personendaten.

44 In diese Richtung deutet auch folgende Erwägung: "*Anders zu entscheiden würde bedeuten, das Datenschutzgesetz nur auf die einzelnen Empfänger anzuwenden, nicht aber auf die Person, welche die betreffenden Daten beschafft und sie verbreitet*".

Die Kritiker des Logistep-Entscheids vernachlässigen aber genau die Relevanz der datenschutzrechtlichen Rollenverteilung, auf welche an späterer Stelle[45] näher einzugehen ist. Der sogenannte Verantwortliche, der über die Zwecke und Mittel einer Datenbearbeitung bestimmt, bleibt jedenfalls auch dann für die (gesamte) Datenbearbeitung verantwortlich, wenn er diese nicht selbst ausführt, sondern einen Dienstleister in Form eines Auftragsbearbeiters zu Hilfe nimmt.[46] Bei der Beurteilung, ob die Bestimmbarkeit nach dem relativen Ansatz gegeben ist, muss deshalb primär auf die Perspektive des Verantwortlichen abgestellt werden.[47] Es ist deshalb auch in arbeitsteiligen Sachverhalten aus seiner Sicht zu bestimmen, inwiefern eine Datenbearbeitung überhaupt Personendaten zum Gegenstand hat oder nicht. Im Falle des Logistep-Urteils spricht Einiges dafür, dass die Empfänger der Daten als Verantwortliche zu qualifizieren und Logistep als blosser Auftragsbearbeiter der Verantwortlichen.[48] Da für Letztere die Bestimmbarkeit gegeben war, nahm Logistep somit eine Datenbearbeitung (für die Verantwortlichen) vor[49] und das Urteil wäre im Ergebnis richtig[50] und bloss die Begründung, welche die jeweiligen Rollen ausser Acht liess, unzureichend. Ein Widerspruch zum (korrekt umschriebenen) relativen Ansatz ist deshalb auch nicht ersichtlich. Wie aber Fälle generell zu beurteilen sind, in welchen Verantwortliche mit Dritten zusammenwirken, insbesondere, wenn eine Co-Verantwortlichkeit oder eine andere Konstellation der Auftragsbearbeitung vorliegt, ist unklar.

Aus den Leiturteilen des Europäischen Gerichtshofs zum Verhältnis zwischen Co-Verantwortlichen lässt sich aber jedenfalls ableiten, dass eine gegenseitige Zurechnung der Möglichkeiten zur Bestimmung einer Person zu erfolgen hat. So entschied der EuGH in zwei Urteilen, dass eine gemeinsame Verantwortlichkeit nicht voraussetzt, dass jeder Verantwortliche Zugang zu den betreffenden Daten im Klartext hat.[51] Daraus folgt zugleich, dass aus der Sicht eines (Co-)Verantwortlichen auch dann von Personendaten auszugehen ist und damit eine relevante Datenbearbeitung vorliegen kann, wenn er keinen Zugriff auf die Daten hat und diese auch nicht einer bestimmbaren Person zuordnen kann. Es kann demnach genügen, wenn die Bestimmbarkeit für einen der Co-Verantwortlichen gegeben ist. Die Mittel desselben werden insofern dem oder den anderen Co-Verantwortlichen zugerechnet und es liegt auch aus ihrer Sicht – im Umfang der gemeinsamen Verantwortlichkeit – eine Bearbeitung von Personendaten vor.

Diese Rechtsprechung ist auch für die Schweiz relevant, wurden doch die Begriffsdefinitionen in Bezug auf die datenschutzrechtlichen Rollen bewusst aus der EU-DSGVO übernommen. Ausgehend davon verbleibt die Frage, inwieweit dem Verantwortlichen auch die Mittel des Auftragsbearbeiters zuzurechnen sind. Anders

---

45 Vgl. insb. Abschnitt 4.1.3.

46 Dies ergibt sich neben den Begriffsdefinitionen des Auftragsbearbeiters ("im Auftrag des Verantwortlichen") bereits aus Art. 9 Abs. 1 lit. a nDSG/Art. 10a Abs. 1 lit. a DSG; vgl. ferner z.B. zur EU-DSGVO die Leitlinien des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, 2021, Rz. 80, wonach sich Rechtmässigkeit der Verarbeitung sich von der Tätigkeit des Verantwortlichen ableite.

47 Vgl. auch Erwägungsgrund Nr. 26 DSGVO, nach welchem ebenfalls primär die Perspektive des Verantwortlichen ("oder einer anderen Person") massgeblich ist; im Ansatz ferner wie hier zum alten deutschen Datenschutzgesetz: Schneider, Sekundärnutzung klinischer Daten Rechtliche Rahmenbedingungen, 2015, S. 14 f.

48 Vgl. hierzu z.B. das (vorinstanzliche) Urteil des Bundesverwaltungsgerichts vom 27.5.2009, A-3144/2008, E. 8.2. ("Die Beklagte bestreitet, systematisch und proaktiv Verbindungsdaten im Internet zu sammeln. Sie sammle lediglich auf konkreten Auftrag eines Urheberrechtsinhabers hin…").

49 A.M. womöglich ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 98, im Widerspruch dazu aber dann Rz. 99 lit. c, wo richtigerweise auf die Perspektive des Verantwortlichen abgestellt und von einer Bekanntgabe ausgegangen wird.

50 Auch wenn sich das Verbot somit zwar primär an die Verantwortlichen hätte richten sollen, ist ein Vorgehen gegen den Auftragsverarbeiter als an der Datenbearbeitung Mitwirkender gleichwohl denkbar.

51 EuGH Urteil vom 05.06.2018, C-210/16, Rz. 38; EuGH Urteil vom 10.07.2018, Rz. 69.

als im oben erläuterten Fall im Zusammenhang mit dem Logistep-Urteil ist diese umgekehrte Konstellation weniger klar. Auch hier scheint eine Zurechnung jedoch naheliegend, soweit in solchen Fällen, wo nur der Auftragsbearbeiter über eine Möglichkeit zur Zuordnung der Daten zu einer bestimmbaren Person verfügt, überhaupt von einer Auftragsbearbeitungskonstellation ausgegangen werden kann.

Die vorangehenden Ausführungen verdeutlichen, dass alle genannten Urteile (Logistep, EuGH und HGer ZH) miteinander in Einklang gebracht werden können und insoweit auch nicht im Widerspruch zum relativen Ansatz stehen. Voraussetzung dafür ist jedoch, dass die datenschutzrechtlichen Rollen in die Umschreibung des Ansatzes einbezogen werden[52] und nicht bloss auf unklare Begriffe wie den "Inhaber" des Datums oder denjenigen, "der Zugang zu einer Information hat", abgestellt wird.[53] Es ist somit zwar davon auszugehen, dass bei der Beurteilung der Bestimmbarkeit aus der Sicht des Verantwortlichen auch die Mittel anderer Rechtseinheiten, insbesondere der Co-Verantwortlichen, einzubeziehen sind. Mitunter können sogar auch die Mittel eigentlicher unabhängiger "Dritter" einzubeziehen sein, allerdings in jedem Fall nur insoweit, als diese vom Verantwortlichen vernünftigerweise bzw. mit verhältnismässigem Aufwand auch genutzt werden können.[54] Dies ist im Einzelfall zu beurteilen.

In einer Konstellation wie im Entscheid des Handelsgerichts Zürich, in welcher der Übermittler als (Allein-)Verantwortlicher die Personendaten pseudonymisiert und diese an einen unabhängigen Dritten weitergibt, der selbst über die Zwecke und Mittel der Weiter-Bearbeitung bestimmt, könnten die Daten aus relativer Perspektive für den Dritten tatsächlich als anonymisiert betrachtet werden, selbst wenn sie für den Übermittler Personendaten darstellen. Entscheidend ist, inwieweit der Empfänger selbst über Mittel zur Zuordnung der Daten zu einer Person verfügt. Eine Zurechnung der Mittel zur Identifizierung des Absenders hat in diesem Fall aber, gleichermassen wie bei Mitteln anderer Dritter und anders als bei Co-Verantwortlichen und u.U. Auftragsbearbeitern, nicht von vornherein zu erfolgen, sondern nur, sofern diese vom Empfänger vernünftigerweise auch genutzt werden könnten. Während dabei im Schweizer Recht auch das subjektive Element miteinzubeziehen sein dürfte, inwieweit der konkrete Verantwortliche auch bereit ist, den erforderlichen Aufwand zur Identifizierung vorzunehmen, dürfte unter der EU-DSGVO[55] rein auf objektive Kriterien abgestellt werden.

Es lässt sich somit festhalten, dass in der Schweiz zwar der relative Ansatz gilt, Details dazu aber nach wie vor ungeklärt sind. Auch wenn die einschlägigen Schweizer Urteile, wie soeben erläutert, miteinander in Einklang gebracht werden können, ist dies nicht höchstrichterlich bestätigt und es verbleibt in diesem für die Praxis äusserst zentralen Punkt Rechtsunsicherheit. Darüber hinaus existieren, wie noch zu zeigen ist,[56] in

---

52 Ähnlich, aber gleichwohl anders JACOT-GUILLARMOD/HIRSCH, Pseudonymisierung von Bankkundendaten, digma 2020 S. 216 ff., 217 ("aus der Sicht des für die Pseudonymisierung Verantwortlichen (und anderer, die den Pseudonymisierungsvorgang rückgängig machen können"); differenzierend, aber ohne direkte Bezugnahme auf die datenschutzrechtlichen Rollen, PROBST, Die unbestimmte "Bestimmbarkeit" der von Daten betroffenen Person im Datenschutzrecht, AJP 2013 S. 1423 ff., 1433.

53 So aber ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 19; vgl. hierzu bereits die Kritik bei PROBST, Die unbestimmte "Bestimmbarkeit" der von Daten betroffenen Person im Datenschutzrecht, AJP 2013 S. 1423 ff., 1432.

54 So ist auch das Leiturteil des EuGH zu verstehen, Urteil vom 19.1.2016; C-582/14; vgl. dazu Karg, in: SIMITIS/HORNUNG/SPIECKER GEN. DÖHMANN (Hrsg.), Datenschutzrecht, 2019, Art. 4 Nr. 1 N 61: ("Es ist gerade nicht erforderlich […], dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden. Anders formuliert muss sich die verantwortliche Stelle das abstrakt verfügbare Drittwissen und die für Dritte zur Verfügung stehenden Mittel zurechnen lassen. Allerdings gilt dies nur, soweit das Wissen und die Mittel durch die verantwortliche Stelle vernünftigerweise eingesetzt werden (können)."

55 Vgl. Erwägungsgrund Nr. 26.

56 Siehe unten Abschnitt 4.3.3a).

den Kantonen teilweise komplett anders definierte datenschutzrechtliche Rollen, sodass im Falle von mehreren anwendbaren schweizerischen Datenschutzgesetzen kaum mehr jemand zuverlässig wird einschätzen können, welche Kriterien für die Bestimmbarkeit konkret gelten sollen und was das Ergebnis der Beurteilung sein wird.

3.1.3 Daten über die Gesundheit

Bei Gesundheitsdaten, die einer bestimmbaren Person im soeben erläuterten Sinne zugeordnet werden können, handelt es sich somit um Personendaten. Für die Bearbeitung solcher Gesundheitsdaten gelten daher grundsätzlich ebenfalls die allgemeinen Datenschutzbestimmungen. Gemäss Art. 3 lit. c Ziff. 2 DSG werden Personendaten über die Gesundheit als besonders schützenswert erachtet. Ähnlich wie im EU-Datenschutzrecht stellt auch das DSG in zahlreichen Punkten höhere Anforderungen an die Bearbeitung dieser sensitiven Datenkategorien, so dürfen z.B. besonders schützenswerte Daten nicht ohne Rechtfertigungsgrund an Dritte bekanntgegeben werden.[57]

Eine Legaldefinition von Gesundheitsdaten fehlt im DSG. Ginge es nach dem allgemeinen Sprachgebrauch, könnte der Begriff der Gesundheitsdaten alle Informationen erfassen, welche – direkt oder indirekt – Rückschlüsse auf den physischen oder psychischen Gesundheitszustand einer Person zulassen. Bereits nach der Botschaft zum geltenden DSG werden hingegen nicht sämtliche Angaben über den körperlichen Zustand (z.B. Haar- und Augenfrage, Körpergrösse) als besonders schützenswert erachtet, sondern nur "medizinische Befunde, welche sich für die Betroffenen negativ auswirken können".[58] Als medizinscher Befund wird das Ergebnis einer medizinischen Untersuchung, wie z.B. einer körperliche Untersuchung, einer psychischen Exploration oder einer labor- und gerätemedizinischen Untersuchung bezeichnet.[59]

Es ist hingegen nicht erforderlich, dass es sich bei dem Befund um eine den medizinischen Standards entsprechende Diagnose handelt, welche spezifische Merkmale einer bestimmten gesundheitlichen Störung bzw. Krankheit erfasst[60] Neben einer eigentlichen medizinischen Diagnose können deshalb auch simple Verordnungen oder Rechnungen für Medikamente Gesundheitsdaten darstellen.[61] Darüber hinaus müssen der medizinische Befund auch nicht richtig sein, um als Gesundheitsdaten zu gelten.[62] Das Begriffsverständnis von "Daten über die Gesundheit" – als besonders schützenswerte Daten – bleibt durch die Totalrevision des DSG unberührt und ist nun in Art. 5 lit. c Z. 2 nDSG normiert.

Aus dem Gesagten folgt, dass auch hier kein absolutes Verständnis zugrunde liegt. Vielmehr ist der Kontext relevant, in welchem eine bestimmte Information verarbeitet wird, und aus wessen Sicht die Beurteilung vorzunehmen ist. Folgt man dem Begriffsverständnis der Botschaft DSG 1988 wird man auch nicht ohne wertende Beurteilung auskommen und einzubeziehen haben, inwieweit der Umgang mit dem Inhalt des Befunds

---

57 Art. 12 Abs. 2 lit. c DSG.

58 Botschaft zum DSG, BBl 1988 S. 446.

59 BLECHTA, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 3 Rz. 33.

60 ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 48; BLECHTA, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 3 Rz.33.

61 MEIER, Protection des données, 2010, Rz. 486.

62 BLECHTA, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 3 Rz.33.

der betroffenen Person schaden könnte, wobei die Lehre neben den Umständen des Einzelfalls auch auf die Sozialadäquanz abstellt.[63]

Ausgehend davon stellt sich deshalb bspw. die Frage, ob aus der Aggregation einer Vielzahl von Daten, die für sich genommen keine Gesundheitsdaten darstellen, Gesundheitsdaten im vorgenannten Sinne entstehen können. Werden z.B. über eine App oder ein Wearable Informationen zu den Essgewohnheiten, der Häufigkeit der sportlichen Aktivitäten etc., über einen längeren Zeitraum gesammelt, kann dies letztlich Rückschlüsse im Sinne eines Befunds erlauben. Es wird deshalb in solchen Fällen im Einzelfall zu beurteilen sein, ob diese Sammlung als solche bereits ausreicht oder ob es hierzu zusätzlich auch einer gewissen Bewertung bedarf, damit von besonders schützenswerten Gesundheitsdaten ausgegangen werden muss. In jedem Fall besteht auch hier in der Praxis eine Unsicherheit, inwieweit für die Bearbeitung entsprechender Daten bereits die höheren datenschutzrechtlichen Anforderungen zu berücksichtigen sind. Im Zweifelsfall werden die Verantwortlichen zur Vermeidung von Risiken hiervon ausgehen, auch wenn dies nach einer korrekten Auslegung der Vorschriften im Einzelfall nicht zutreffend wäre.

3.1.4 Genetische und biometrische Daten

Einen engen Zusammenhang zu Gesundheitsdaten weisen sodann auch genetische und biometrische Daten auf, welche ab dem Inkrafttreten des DSG nun auch ausdrücklich als besonders schützenswert i.S.v. Art. 5 lit. c Z. 3 und 4 nDSG gelten. Da die Totalrevision des nDSG eine – teilweise – Angleichung an die europäische Rechtslage bezweckte, erscheint es nicht überraschend, dass die DSGVO – genau wie das nDSG – zwischen Gesundheitsdaten (nDSG: "Daten über die Gesundheit"), biometrischen und genetischen Daten unterscheidet und diesen als "besonders schützenswerte Kategorien personenbezogener Daten" ein höheres Schutzniveau zuerkennt. Das Begriffsverständnis von genetischen und biometrischen Daten des nDSG stimmt auch weitgehend mit jenem der DSGVO überein.

Gemäss Botschaft zum nDSG sind genetische Daten alle Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden; darin enthalten sind auch DNA-Profile i.S.v. Art. 3 lit. k GUMG.[64] Diese Bestimmung definiert das DNA-Profil wie folgt: "die für ein Individuum spezifische Information, die mit Hilfe molekulargenetischer Techniken aus den nicht-codierenden Abschnitten der DNA gewonnen wird".

Im Zusammenhang mit genetischen Daten fällt auf, dass der Gesetzgeber auf den bei der Begriffsdefinition von biometrischen Daten enthaltenen Zusatz "die eine natürliche Person eindeutig identifizieren" verzichtete. Demnach ist fraglich, ob damit beabsichtigt wurde, dass sämtliche genetischen Daten als besonders schützenswert erachtet werden sollen, unabhängig davon, ob ein Personenbezug hergestellt werden kann. Die Lehre gelangt teilweise aufgrund einer teleologischen und systematischen Auslegung[65] zum Ergebnis, dass nur genetische Daten erfasst sein können, die auch den Anforderungen von Personendaten gerecht werden und will den Zusatz in die Definition hineinlesen.[66] Ob der bewusst weggelassene Zusatz – immerhin wurde

---

63 MEIER, Protection des données, 2010, Rz. 489.

64 Botschaft zum nDSG, BBl 2017 S. 108; Bundesgesetz vom 8. Oktober 2004108 über genetische Untersuchungen beim Menschen (GUMG), SR 810.12 (im Folgenden GUMG).

65 Bei der teleologischen bzw. systematischen Auslegung handelt es sich um juristische Interpretationsmethoden, die dabei helfen sollen, den Inhalt einer Norm zu bestimmen. Die telelogische Auslegung stellt auf den angestrebten Zweck ("Telos") der Norm ab. Dementsprechend ist die Norm so zu verstehen, dass diese mit dem angestrebten Sinn und Zweck vereinbar ist. Bei der systematischen Auslegung legt man die Norm so aus, dass sie mit der Systematik der (Teil-)Rechtsordnung im Einklang steht.

66 ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, S. 9.

darüber im Nationalrat diskutiert – einfach so dazu interpretiert werden kann, ist fraglich, da dies offensichtlich dem gesetzgeberischen Willen widerspricht. Dennoch sprechen einige gute Gründe für die genannte Lehrmeinung, da die genetischen Daten unter die Gruppe der "besonders schützenswerten Personendaten" fallen und auch die DSGVO, welche als gesetzgeberisches Vorbild diente, diese Einschränkung vornimmt.[67] Gegen die genannte Auffassung – und somit dafür, dass genetische Daten per se Personendaten sind – spricht die bewusste gesetzgeberische Entscheidung, den Zusatz, anders als bei der Definition der biometrischen Daten, wegzulassen. Selbst wenn diese Entscheidung der Lehrmeinung[68] zufolge auf mangelnde Sachkenntnis der Parlamentarier zurückzuführen wäre, ist letztlich der gesetzgeberische Wille ausschlaggebend und danach sollen genetische Daten, unabhängig von einem Personenbezug, zu besonders schützenswerten Personendaten erklärt werden. Eine abschliessende – gerichtliche – Klärung des Begriffsverständnisses gilt es noch abzuwarten.

Wie bereits angesprochen, sind auch biometrische Daten, die eine natürliche Person eindeutig identifizieren, als besonders schützenswerte Personendaten zu qualifizieren.[69] In der Botschaft zum nDSG wird ausgeführt, dass darunter Personendaten zu verstehen sind, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen.[70] Es handelt sich dabei z.B. um einen digitalen Fingerabdruck, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme.[71] Diese Daten müssen zwingend auf einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt. Laut der Botschaft zur Totalrevision des DSG fallen grundsätzlich gewöhnliche Fotografien nicht unter das Begriffsverständnis von biometrischen Daten.[72] Dies entspricht auch dem Verständnis der EU-DSGVO.[73] Hingegen ist es wahrscheinlich, dass "Face-Scans", welche ein dreidimensionales Bild des Gesichts abbilden und die Proportionen der Gesichtsmerkmale (Nase, Augenabstand etc.) vermessen, als biometrische Daten gelten. Diese Face-Scans werden regelmässig als Identifikation bei Smartphones, wie z.B. bei den neueren iPhone-Modellen, verwendet.

3.1.5 Zwischenfazit: Hindernisse in den Begriffsdefinitionen des DSG

Wie aus Abschnitt 3.1 ersichtlich wird, ergeben sich bereits auf Ebene der Begriffsbestimmungen des DSG zahlreiche Unschärfen. Die daraus resultierende Rechtsunsicherheit erschwert den Umgang mit Personendaten und insbesondere Gesundheitsdaten und stellt ein erhebliches praktisches Hindernis für die Innovation im Gesundheitssektor dar. Insbesondere die korrekte Pseudonymisierung bzw. Anonymisierung, durch welche man sich einen fairen Interessenausgleich zwischen den Rechten der betroffenen Personen und den Bearbeitern von Gesundheitsdaten erwartet, ist faktisch schwer umzusetzen und mit einer erheblichen Unsi-

---

67 Art. 4 Z. 13 DSGVO definiert genetische Daten als "*personenbezogene Daten zu den ererbten oder erworbenen Eigenschaften einer natürlichen Person (...)*".

68 ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, S. 9.

69 Art. 5 lit. c Z. 4 nDSG.

70 Botschaft zum nDSG, BBl 2017 S 108.

71 Botschaft zum nDSG, BBl 2017 S. 108.

72 Botschaft zum DSG, BBl 2017 S. 7020.

73 Vgl. Erwägungsgrund Nr. 51 EU-DSGVO.

cherheit verbunden. Dies gilt umso mehr vor dem Hintergrund, dass die Beweislast für die wirksame Vereitelung der Re-Identifizierbarkeit von den Gerichten den Datenübermittlern auferlegt wird.[74] Im Zuge der Totalrevision des DSG wurde die Gelegenheit nicht genutzt, in dieser Hinsicht klare datenschutzrechtliche Rahmenbedingungen zu schaffen.

3.2 Begriff der Gesundheitsdaten im Humanforschungsgesetz

3.2.1 Vorbemerkungen

Das zweite grundlegende Gesetz im Zusammenhang mit der Bearbeitung von Gesundheitsdaten ist das Humanforschungsgesetz (HFG). Gewisse der genannten Hindernisse im Zusammenhang mit der Nutzung von Gesundheitsdaten im Anwendungsbereich des DSG werden durch das HFG abgebaut, welches u.a. als Sonderdatenschutzrecht für die Forschung am Menschen konzipiert ist. Das HFG verfolgt im Wesentlichen zwei zentrale Ziele: einerseits soll die "Würde, Persönlichkeit und Gesundheit des Menschen in der Forschung" geschützt werden und andererseits soll es günstige Rahmenbedingungen für die Forschung am Menschen schaffen und für Qualität und Transparenz in der Humanforschung sorgen.[75] Im Folgenden soll nur auf die Punkte eingegangen werden, die für die Darstellung des Sonderfalls der Gesundheitsdaten relevant sind.

Obwohl weiter unten[76] genauer auf das Verhältnis der relevanten Gesetze eingegangen wird, ist hier kurz zu erwähnen, dass das HFG in jenen Bereichen, in denen es – in seinem Geltungsbereich – datenschutzrechtliche Regelungen trifft, als sog. lex specialis, d.h. als spezielles Gesetz Anwendungsvorrang gegenüber den allgemeineren Bestimmungen des DSG hat.[77] Insofern jedoch das HFG gewisse datenschutzrechtlich relevanten Bereiche offen lässt bzw. keine abschliessende Regelung trifft, kommt das DSG zur Anwendung.[78]

3.2.2 Geltungsbereich

Um beurteilen zu können, welchen Vorschriften ein Forschungsvorhaben untersteht, muss daher zunächst geprüft werden, ob es vom Anwendungsbereich der Datenschutzbestimmungen des HFG erfasst ist.

Dieses gilt für die Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers, die durchgeführt wird:

- mit Personen
- an verstorbenen Personen;
- an Embryonen und Föten;
- mit biologischem Material;

---

74 Vgl. dazu kritisch JACOT-GUILLARMOD/HIRSCH, Pseudonymisierung von Bankkundendaten, digma 2020 S. 216 ff., 219 f.

75 Art. 1 HFG.

76 Vgl. insb. Abschnitte 4.1.2, 4.2.2, 4.3.2.

77 MARTANI,/EGLI,/WIDMER, Data protection and biomedical research in Switzerland: setting the record straight Swiss Med Wkly. 2020, S. 5.

78 MARTANI,/EGLI,/WIDMER, Data protection and biomedical research in Switzerland: setting the record straight Swiss Med Wkly. 2020, S. 5.

- mit gesundheitsbezogenen Personendaten.[79]

Auf die Einzelheiten wird an späterer Stelle[80] zurückgekommen. Festzuhalten ist in diesem Kapitel nur, was für die Darstellung des Sonderfalls der Gesundheitsdaten erforderlich ist. Hierzu zählt das Verständnis der relevanten Daten, von dem das HFG ausgeht und damit auch, inwiefern sich dieses von demjenigen des DSG unterscheidet. Ferner wird in einem nächsten Schritt[81] kurz erläutert, wie diese Daten unter dem HFG behandelt werden.

Im Kontext dieses Gutachtens sind insbesondere Daten bzw. biologische Materialien relevant, die im Zuge der Sekundärnutzung in einem Forschungsprojekt verarbeitet werden können. Das HFG definiert drei zentrale Begriffe von geschützten Datenkategorien bzw. Materialien: biologisches Material, gesundheitsbezogene Personendaten und genetische Daten.

Von Bedeutung sind sodann die Begriffe der anonymisierten und pseudonymisierten sowie verschlüsselten Daten. Denn vom Geltungsbereich ausgenommen ist namentlich die Forschung an anonymisiertem biologischem Material und mit anonym erhobenen und anonymisierten gesundheitsbezogenen Daten[82] und die Vorgaben für die Sekundärnutzung stellen massgeblich auf die Anonymisierung und Verschlüsselung ab.

3.2.3 Biologisches Material

Unter biologischem Material sind laut Legaldefinition jegliche "Körpersubstanzen, die von lebenden Personen stammen" zu verstehen.[83] Unter die Begriffsdefinition fallen insbesondere Organe, Gewebe, Zellen (einschliesslich Ei- und Samenzellen) und Köperflüssigkeiten, wie z.B. Blut und Urin.[84] Mit Körpersubstanzen sind nicht nur Flüssigkeiten gemeint, sondern verschiedenste Formen, z.B. ganze Organe, fixierte Gewebeproben, aus weissen Blutkörperchen isolierte und als chemische Substanz tiefgefrorene DNA oder als in permanente Zellkulturen transformierte (i.d.R. Blut-) Zellen.[85] Biologisches Material beinhaltet gesundheitsbezogene Personendaten bzw. genetische Daten, dennoch wird es im HFG von den beiden genannten Datenarten abgegrenzt.[86] Ferner zählen nur Körpersubstanzen, die von lebenden Personen stammen, als biologisches Material i.S.d. HFG.

---

79 Art. 2 Abs. 1 HFG.

80 Siehe dazu nachfolgend Abschnitt 4.2.1.

81 Siehe dazu nachfolgend Abschnitt 3.3.2.

82 Art. 2 Abs. 2 HFG.

83 Art. 3 lit. e HFG.

84 VAN SPYK/RUDIN/SPRECHER/POLEDNA, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 3 Rz. 41; Botschaft zum HFG, BBl 2009 S. 8045.

85 VAN SPYK/RUDIN/SPRECHER/POLEDNA, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 3 Rz. 41.

86 VAN SPYK/RUDIN/SPRECHER/POLEDNA, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 3 Rz. 39.

3.2.4 Gesundheitsbezogene Personendaten

Art. 3 lit. f HFG definiert gesundheitsbezogene Personendaten als "Informationen über eine bestimmte oder bestimmbare Person, die sich auf deren Gesundheit oder Krankheit beziehen, einschliesslich ihrer genetischen Daten". Laut der Botschaft zum HFG entspricht der Begriff der Definition von "Daten über die Gesundheit" i.S.d. DSG.[87]

Ob sich die Begriffe tatsächlich gänzlich entsprechen, ist zweifelhaft. So werden in der Botschaft zum HFG gesundheitsbezogene Daten wie folgt näher definiert: "diejenigen Informationen über eine Person zu verstehen, die einen Bezug zu einer physischen oder psychischen Krankheit aufweisen oder über Aufbau und Funktion des Körpers der betreffenden Person".[88] Wie bereits erläutert, sind aber "Informationen über den Aufbau und Funktion des Körpers der betreffenden Person" nicht zwangsläufig vom Begriffsverständnis von "Daten über die Gesundheit" i.S.d. DSG umfasst, da sich diese nicht unbedingt "für die Betroffenen negativ auswirken können"[89] und auch nicht in allen Fällen eine Aussage über den Gesundheitszustand der betroffenen Person im Sinne eines Befunds zulassen. Wäre tatsächlich ein einheitliches Begriffsverständnis beabsichtigt gewesen, hätte man im Gesetzgebungsprozess die Definition des DSG übernehmen können und nicht in der Botschaft zusätzlich "Informationen über den Aufbau und Funktion des Körpers der betreffenden Person" erwähnen müssen. Gestützt darauf müsste von einem im Vergleich zum DSG weiteren Begriffsverständnis des HFG ausgegangen werden.

Grundsätzlich ist jedoch eine einheitliche Auslegung der Begriffe zu befürworten, wie dies auch der Gesetzgeber laut Botschaft eigentlich vorgehabt hatte.[90] Diese Auslegung ist auch näher am Wortlaut der Begriffsdefinition im HFG. Hierbei kann die Rechtsprechung und Literatur zu den entsprechenden Begriffen des DSG als Auslegungshilfe für das HFG dienen. Warum der Gesetzgeber nicht den Begriff der "Daten über die Gesundheit" des DSG übernahm, obwohl er offensichtlich inhaltlich das Gleiche regeln wollte, ist unverständlich und führt zu unnötiger Rechtsunsicherheit.

3.2.5 Genetische Daten

Genetische Daten sind eine Unterkategorie der gesundheitsbezogenen Daten und umfassen nach der Legaldefinition jegliche "Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden".[91] Dementsprechend ist die Definition wortgleich mit dem bereits erläuterten Verständnis gemäss nDSG. Im Unterschied zum Verständnis gemäss nDSG im Vergleich zum Art. 3 lit. l Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG) ist die Bezugnahme auf DNA-Profile für die genetischen Daten i.S.d. HFG nicht relevant, da diesen im Forschungskontext des HFG gemäss Botschaft zum

87 Botschaft zum HFG, BBl.2009 S. 8095.

88 Botschaft zum HFG, BBl.2009 S. 8095.

89 Botschaft zum DSG, BBl 1988 S. 446.

90 Botschaft zum HFG, BBl 2009 S. 8095.

91 Art. 3 lit. g HFG.

HFG keine Bedeutung zukomme.[92] Genetische Daten können grundsätzlich aus nahezu jeder Art biologischen Materials im Rahmen einer genetischen Untersuchung gewonnen werden.[93] In der Lehre wird von einem weiten Begriffsverständnis ausgegangen.[94] Demzufolge sind nicht nur die Sequenzierungen spezifischer Genome vom Begriffsverständnis umfasst, sondern auch die Informationen, die gewonnen werden, wenn z.B. bei einer onkologischen Untersuchungsmethode mit Genmarkern gearbeitet wird.[95]

Die Unterscheidung zwischen gesundheitsbezogenen Personendaten und einer ihrer Unterkategorien, den genetischen Daten, ist deshalb relevant, weil das HFG strengere Anforderungen an die Bearbeitung von genetischen Daten im Forschungskontext stellt. Die Differenzierung dieser beiden Datenkategorien hat mittels einer negativen Abgrenzung zu erfolgen; folglich sind sämtliche gesundheitsbezogenen Personendaten, welche nicht als genetische Daten zu qualifizieren sind, gesundheitsbezogene Personendaten i.S.d. HFG.

3.2.6 Anonymisierung im HFG

Im Gegensatz zum DSG ist die Anonymisierung im HFG gesetzlich definiert. Gemäss Art. 3 lit. i gelten biologisches Material und gesundheitsbezogene Daten als anonym, wenn sie nicht oder nur mit unverhältnismässigem Aufwand auf eine bestimmte Person zurückgeführt werden können. Laut der Botschaft zum HFG entspricht diese Definition dem Begriffsverständnis des DSG.[96] Die terminologischen Abweichungen und die fehlende Erwähnung der bestimmbaren Person sind im Ergebnis nicht relevant, kann doch die Bestimmbarkeit einer Person mit der Zurückführbarkeit auf eine Person gleichgesetzt werden. Für diese Auslegung spricht, dass der Gesetzgeber das Begriffsverständnis des Datenschutzrechts – wie aus der Botschaft ersichtlich wird – übernehmen wollte und dass auch in der Definition von gesundheitsbezogenen Personendaten und des biologischen Materials von einer bestimmten oder bestimmbaren Person die Rede ist.

Die Anforderungen an die Verhältnismässigkeit der Identifizierungs- oder Zurückführbarkeits-Möglichkeit werden in der Botschaft durch folgendes Beispiel veranschaulicht: Es ist theoretisch denkbar, dass genetische Daten, die aus biologischem Material gewonnen werden, mit Referenzdaten verglichen und somit ein Personenbezug hergestellt werden könnte. Diese theoretische Identifizierungsmöglichkeit erscheint jedoch in der Praxis unverhältnismässig, da die dafür notwendigen Referenzdaten bzw. Vergleichsproben in der Regel nicht bzw. nicht rechtmässig zugänglich sind.[97]

In der Literatur wird kritisch angemerkt, dass die Anonymisierung von genetischem Material kaum möglich ist, da es praktisch unvorstellbar sei, die in Körperzellen vorhandene Information irreversibel zu entfernen.[98] Dieser Auffassung wäre vorbehaltlos zuzustimmen, wenn man von einem absoluten Ansatz der Bestimmbarkeit ausginge. Das genannte Beispiel bekräftigt jedoch, dass der Gesetzgeber auch im HFG von einem relativen Verständnis der Bestimmbarkeit der betroffenen Person ausgeht, wie es bereits im Zusammenhang mit dem DSG erläutert wurde. Denn er stellt implizit darauf ab, ob es einem konkreten Verantwortlichen für eine

---

92 Botschaft zum HFG, BBl 2009 S. 8095.

93 Botschaft zum HFG, BBl 2009, S. 8095.

94 VAN SPYK/RUDIN/SPRECHER/POLEDNA, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 3 Rz. 50.

95 VAN SPYK/RUDIN/SPRECHER/POLEDNA, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 3 Rz. 50.

96 Botschaft zum HFG, BBl. 2009 S. 8096.

97 Botschaft zum HFG, BBl 2009 S. 8096.

98 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 35 Rz. 10 ff.

Datenbearbeitung möglich ist, mit verhältnismässigen Mittel die genetischen Daten zu identifizieren und nicht, ob dies irgendeiner beliebigen Person möglich wäre. Die Identifizierung ist anhand der Referenzdaten zwar theoretisch möglich, jedoch ist es für den konkreten Verantwortlichen unmöglich oder zumindest unverhältnismässig schwer, die Referenzdaten zu beschaffen. Folglich ist jeweils auch hier die Perspektive des oder der Verantwortlichen für die Datenbearbeitung, also vielfach des Inhabers der Daten bzw. des biologischen Materials, einzunehmen, um zu beurteilen ob für diese eine natürliche Person mit verhältnismässigem Aufwand zumindest bestimmbar ist. Neben dem objektiv erforderlichen Aufwand der Identifizierung ist auch das (subjektive) Interesse des Datenbearbeiters an der Identifizierung zu berücksichtigen.[99] Für eine relative Perspektive spricht des Weiteren, dass in der Botschaft zum HFG auf die Begriffe des DSG (z.B. "Daten über die Gesundheit") bzw. auf das Verständnis der Anonymisierung verwiesen wird und deswegen eine einheitliche Auslegung der beiden Gesetze systematisch erforderlich ist.[100]

Trotz des genannten Beispiels in der Botschaft und der Tatsache, dass das HFG die Anonymisierung von biologischem Material vorsieht, ist dabei Vorsicht geboten.[101] Denn die Beurteilung, ob tatsächlich eine Anonymisierung vorliegt, ist jeweils vom konkreten Einzelfall abhängig.[102] Desto mehr biologisches Material erhoben wird und desto effizienter die verfügbaren IT-Anwendungen werden, umso weniger aufwändig wird es, den Personenbezug bei scheinbar anonymisiertem biologischem Material wiederherzustellen.[103] Als Beispiel für unterschiedliche Beurteilungen im Einzelfall nennt die Botschaft, dass es bei sehr grossen Datenmengen (grosse Personenpopulation) ausreichen könnte, lediglich den Namen der Betroffenen zu streichen, hingegen sei dies bei kleineren Datensätzen nicht ausreichend.[104] Ob diese Beurteilung in Anbetracht der technischen Fortentwicklung im Big Data Processing noch zeitgemäss ist, ist fraglich. Vielmehr sind deshalb grundsätzlich sämtliche personenbezogene Parameter, wie Geburtsdatum, Wohnadresse etc., zu streichen.[105]

Der Gesetzgeber beauftragt in Art. 35 HFG den Bundesrat damit, die korrekte und sichere Anonymisierung und Verschlüsselung sowie die Voraussetzungen für die Entschlüsselung zu konkretisieren. Diesem Auftrag kommt der Bundesrat in Art. 25 bzw. 26 Humanforschungsverordnung (HFV)[106] zwar grundsätzlich nach, jedoch geben diese Bestimmungen nur bedingt mehr Aufschluss zur konkreten Umsetzung der genannten De-Identifizierungstechniken, als ohnehin gesetzlich festgelegt wurde.

Art. 25 HFV legt fest, dass "zur Anonymisierung biologischen Materials und gesundheitsbezogener Personendaten alle Angaben, die in ihrer Kombination die Wiederherstellung des Bezugs zu einer Person ohne unverhältnismässigen Aufwand erlauben, irreversibel unkenntlich gemacht oder gelöscht werden" müssen.

---

99 Rudin, in: Rütsche (Hrsg.), Humanforschungsgesetz, 2015, Art. 35 Rz. 7, siehe Abschnitt Personendaten DSG.

100 Botschaft zum HFG, BBl 2009 S. 8096.

101 Botschaft zum HFG, BBl 2009 S. 8096; Art. 35 HFG.

102 Botschaft zum HFG, BBl 2009 S. 8096.

103 Rudin, in: Rütsche (Hrsg.), Humanforschungsgesetz, 2015, Art. 35 Rz. 13.

104 Botschaft zum HFG, BBl 2009 S. 8096.

105 Vgl. auch die Botschaft zum HFG, BBl.2009 S. 8096, allerdings mit der unklaren Einschränkung, "falls sie nicht unbedingt erforderlich sind".

106 Verordnung über die Humanforschung mit Ausnahme der klinischen Versuche (Humanforschungsverordnung, HFV) vom 20. September 2013, SR 810.301.

"Insbesondere unkenntlich gemacht oder gelöscht werden müssen Namen, Adresse, Geburtsdatum und eindeutig kennzeichnende Identifikationsnummern".[107] Mit dem Einbezug des unverhältnismässigen Aufwands übernimmt die Regelung im Grundsatz die Kriterien, die auch im DSG gelten. Auch hier ist, mangels abweichender Regelung, der erläuterte relative Ansatz massgebend. Weniger klar sind jedoch folgende zwei Aspekte: Anders als nach dem Verständnis, das zum DSG vertreten wird und implizit den Definitionen im HFG zugrunde liegt, wird hier die Irreversibilität nicht explizit in Bezug gesetzt zum unverhältnismässigen Aufwand. Der Wortlaut liesse daher eine Auslegung zu, nach der für die Qualifikation als irreversibel auch Mittel zu berücksichtigen wären, die einen unverhältnismässig hohen Aufwand darstellen. Dies war jedoch offenbar auch nicht beabsichtigt[108] und stünde im Widerspruch zum Verständnis des übergeordneten HFG, das seinerseits dem Verständnis des DSG folgt.

Darüber hinaus ist die Aufzählung der Attribute, die "insbesondere" entfernt werden müssen, bloss exemplarisch und nicht abschliessend. Es kann daher nicht zwangsläufig davon ausgegangen werden, dass die Entfernung dieser Identifikationsmerkmale im Einzelfall zu einer wirksamen Anonymisierung führt. Umgekehrt legt es Mindestanforderungen fest. Das bedeutet, dass jedenfalls so lange nicht von einer Anonymisierung ausgegangen werden kann, als die aufgezählten Attribute nicht entfernt sind. Unklar ist dabei allerdings, was mit "eindeutig kennzeichnenden Identifikationsnummern" gemeint ist und was dies für Folgen hat.[109] Da die Entfernung derselben zur Mindestanforderung gemacht wird, erinnert dies an den bereits erläuterten Ansatz des "Singling-Out",[110] nach dem kein Bezug zu einer konkreten Person notwendig ist, sondern es bereits ausreicht, dass ein Individuum eindeutig von anderen unterschieden werden kann. Eine solche Abweichung von der Systematik des DSG, demzufolge die Möglichkeit des "Singling-Out" bzw. des Aussonderns aus einer Masse alleine noch nicht die Anwendbarkeit des DSG begründet, scheint nicht gewollt, insbesondere da laut Botschaft zum HFG der Begriff der "gesundheitsbezogenen Personendaten" mit jenem der "Daten über die Gesundheit" des DSG gleichgesetzt wird.[111]

Ein Blick auf die Entstehungsgeschichte der Humanforschungsverordnung (HFV) zeigt ferner, dass mit den "eindeutig kennzeichnenden Identifikationsnummern" primär auf die AHV-Nummer abgezielt wurde.[112] Während die AHV-Nummer zahlreiche Besonderheiten aufweist und deren systematische Verwendung nur unter bestimmten Voraussetzungen zulässig ist,[113] handelt es sich bei vergleichbaren nicht-sprechenden Nummern jedoch vielfach um blosse Pseudonyme. Der Einbezug solcher Identifikationsnummern in die Mindestanforderungen führt daher potentiell zu (ungelösten) Konflikten mit den Regelungen zur Verschlüsselung, wo Nummern als "Schlüssel" dienen können. Folglich ist die Bestimmung eng auszulegen und nicht auf jegliche anderen Kennnummern auszudehnen. Es muss jedenfalls auch dann eine Anonymisierung im Sinne des

---

107 Art. 25 Abs. 2 HFV.

108 Vgl. Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 69 f.

109 Der Begriff ist auch nicht identisch mit demjenigen der "persönlichen Identifikationsnummer" in Art. 25 DSG.

110 Siehe oben Abschnitt 3.1.2b)

111 Art. 25 Abs. 2 HFV.

112 Vgl. Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 70.

113 Vgl. Art. 153b ff. AHVG; ferner die Erläuterungen dazu in der Botschaft zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (Systematische Verwendung der AHV-Nummer durch Behörden) vom 30. Oktober 2019, BBl 2018 S. 7359 ff.

HFG vorliegen können, wenn eine Person über eine bestimmte (andere) Kennnummer (als die AHV-Nummer) noch von anderen Personen unterschieden und ausgesondert werden kann, solange sie nicht bestimmbar im Sinne der bereits erläuterten Grundsätze ist.

Abschliessend muss festgehalten werden, dass die Umsetzung einer korrekten Anonymisierung i.S.d. HFG trotz gesetzlicher Definition und einer Konkretisierung in der HFV praktisch ebenfalls mit viel Rechtsunsicherheit verbunden ist. Es könnte zwar argumentiert werden, dass die exemplarische Aufzählung von entscheiden Identifikationsmerkmalen (wie z.B. Name, Adresse, Geburtsdatum), die entfernt werden sollten, einen Anhaltspunkt für eine ausreichende Anonymisierung bietet, jedoch wird dies in einigen Fällen nicht genug sein, um eine Bestimmbarkeit der betroffenen Personen auszuschliessen. Es hat daher auch hier eine mit Unsicherheiten behaftete Prüfung unter Berücksichtigung sämtlicher Umstände im Einzelfall zu erfolgen.

Schliesslich gilt es zu beachten, dass das HFG zwar nicht auf die Bearbeitung von anonymisierten gesundheitsbezogenen Personendaten bzw. biologischem Material anwendbar ist, jedoch der Prozess der Anonymisierung selbst in den Geltungsbereich des HFG fällt. Die betroffene Person muss über die Anonymisierung zu Forschungszwecken informiert werden und kann dieser widersprechen.[114]

3.2.7 Verschlüsselung im HFG

Im Gegensatz zu anonymisierten gesundheitsbezogenen Personendaten bzw. biologischem Material, sind diese in verschlüsselter Form nicht vom Anwendungsbereich des HFG ausgenommen. Das HFG sieht jedoch zahlreiche Erleichterungen für die Bearbeitung von verschlüsselten Gesundheitsdaten vor.

Art. 3 lit. h HFG definiert verschlüsseltes biologisches Material und verschlüsselte gesundheitsbezogene Personendaten als "biologisches Material und Daten, die mit einer bestimmten Person über einen Schlüssel verknüpft sind". Im Grunde handelt es sich bei der Verschlüsselung demnach um eine Pseudonymisierung bzw. Codierung. Die genannten Begriffe können laut Botschaft als Synonyme für die Verschlüsselung verstanden werden.[115] Die Verschlüsselung der Identifikationsmerkmale ist – im Gegenzug zur Anonymisierung – reversibel. Mit dem richtigen Schlüssel bzw. Code kann demnach der Personenbezug wieder hergestellt werden. Bei der Verschlüsselung werden die identifizierenden Attribute nicht alle gelöscht, sondern zum Teil durch Pseudonyme ersetzt, z.B. durch eine Buchstaben- und/oder Zahlenfolge.[116] Bei der Entschlüsselung können die erzeugten Pseudonyme wiederum der jeweiligen bestimmbaren Person zugerechnet werden.

Gemäss Art. 26 HFV gilt biologisches Material bzw. gesundheitsbezogene Personendaten als korrekt verschlüsselt, sobald sie aus Sicht einer Person, die keinen Zugang zum Schlüssel hat, als anonymisiert zu qualifizieren sind. Daraus ergibt sich, dass die Verschlüsselung dieselben Qualitätsanforderungen wie die Anonymisierung einzuhalten hat.[117] Diese Regelung wirft die Frage auf, wie sie in die Auslegung des Bestimmbarkeitsbegriffs einzuordnen ist. Dabei gilt es, zwei Aspekte hervorzuheben. Zunächst stellt die Regelung bloss auf irgendeine beliebige Person ab und legt nicht fest, inwieweit diese aus Sicht des relativen Ansatzes relevant ist. Dies verdeutlicht, dass für den Begriff der Pseudonymisierung bzw. der Verschlüsselung nicht die gleichen Perspektiven massgeblich sind, wie im Rahmen der Prüfung der Bestimmbarkeit nach dem relativen Ansatz. Andernfalls könnten die Begriffe Pseudonymisierung und Anonymisierung auch kaum

[114] Art. 32 Abs. 3 HFG.

[115] Botschaft zum HFG, BBl 2009 S. 8096.

[116] RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 35 Rz. 15.

[117] RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 35 Rz. 17.

mehr sinnvoll unterschieden werden. Wenn für die Pseudonymisierung und nach dem (falsch ausgelegten) relativen Ansatz die Perspektive einer beliebigen Person relevant sein soll, der die strittige Information vorliegt, wäre hiernach stets sowohl die Anonymisierung und die Pseudonymisierung gegeben oder eben nicht gegeben.

Folglich ist für die Pseudonymisierung nach dem hier vertretenen Verständnis – und anders als für die Frage der Anonymisierung – nicht auf den Verantwortlichen und die ihm zuzurechnenden Personen, sondern auf die jeweilige Person abzustellen, der die Information vorliegt. Sind also beispielsweise für eine Datenbearbeitung zwei Organisationen gemeinsame Verantwortliche, so ist zwar für beide von Personendaten und damit nicht von anonymisierten Daten auszugehen, sind doch hier die Mittel des einem dem anderen in jedem Falle zuzurechnen. Jedoch können diese Daten, falls einer der Co-Verantwortlichen keinen Zugang zum Klartext der verschlüsselten Informationen und zum Schlüssel hat, pseudonymisiert sein. Gleiches gilt innerhalb der Organisation eines Verantwortlichen: Hat nur eine Person Zugang zum Schlüssel, reicht dies, um von der Bestimmbarkeit aus der Sicht der Rechtseinheit des Verantwortlichen auszugehen. Gleichwohl kann die Information aus Sicht der Mitarbeiter der Organisation ohne Zugang zum Schlüssel pseudonymisiert sein.

Der zweite Aspekt der Regelung in der HFV betrifft die Bedeutung des Zugangs zum Schlüssel für die Anonymisierung und die Pseudonymisierung. So wird darin nicht der fehlende Zugang zum Schlüssel mit der Anonymisierung gleichgesetzt. Vielmehr enthält die Bestimmung zwei kumulative Tatbestandselemente, um von einer hinreichenden Pseudonymisierung auszugehen. Erstens ist die Sicht einer Person relevant, die keinen Zugang zum Schlüssel hat, und zweites ist aus deren Perspektive zu beurteilen, ob eine Anonymisierung vorliegt. Mit dem zweiten Element wird, abgesehen vom Aspekt der relevanten Perspektive, auf den Anonymisierungsbegriff verwiesen und damit zumindest noch die Beurteilung verlangt, ob – neben dem Schlüssel – andere verhältnismässige Mittel zur Bestimmung der betreffenden Person vorhanden sind. Nur weil eine Person daher keinen Zugang zum Schlüssel hat, sind die verschlüsselten Informationen noch nicht zwingend anonymisiert. Gleichwohl dürfte bei einer angemessenen Verschlüsselungsmethode und Aufbewahrung der Schlüssel vielfach davon auszugehen sein, dass dies der Fall ist. Es wird aber auch hier wieder auf die Beurteilung der relevanten Umstände des Einzelfalls verwiesen, was mit erheblichen Unsicherheiten verbunden ist.

3.2.8 Zwischenfazit: Hindernisse in den Begriffsdefinitionen des HFG

Zusammenfassend lässt sich festhalten, dass das HFG viele wichtige Begriffe definiert, die bereits unter dem DSG zumindest indirekt geregelt werden, wie z.B. gesundheitsbezogene Personendaten, Anonymisierung oder Pseudonymisierung. Das Begriffsverständnis unter dem HFG entspricht dabei zwar zu einem grossen Teil demjenigen des DSG, allerdings ist es dem Gesetzgeber im HFG nicht gelungen, die Zweifel an einem identischen Verständnis in beiden Gesetzen zu beseitigen. Dies wäre vermeidbar gewesen. Darüber hinaus zeigen sich aber auch hier die unter dem DSG erläuterten rechtlichen Unsicherheiten bei den zentralen Begriffen der Anonymisierung und der Pseudonymisierung bzw. der Verschlüsselung. Auch hier hätte der Gesetz- bzw. Verordnungsgeber Gelegenheit gehabt, entweder deutlich auf die Begriffsverständnisse unter dem DSG zu verweisen oder aber abweichende und abschliessende Kriterien für die Forschung aufzustellen, die für eine hinreichende Anonymisierung und Pseudonymisierung vorzukehren sind. Folglich bleibt bereits auf der Stufe der grundlegenden Begriffe eine Vielzahl von Fragen offen. In der Praxis bereitet deshalb insbesondere die konkrete Umsetzung der Anonymisierung und Pseudonymisierung bzw. Verschlüsselung grosse Probleme. Besonders mit Blick auf biologisches Material bzw. die daraus gewonnen genetischen Daten ist nicht eindeutig geklärt, inwieweit diese überhaupt wirksam anonymisiert werden können.

3.3 Rechtliche Spezialbehandlung von Gesundheitsdaten

Ausgehend von dem oben in Abschnitt 3.1 erläuterten Verständnis des Begriffs Gesundheitsdaten wird nachfolgend in einer ersten Übersicht aufgezeigt, inwiefern diese Daten einer rechtlichen Spezialbehandlung unterliegen. Auf die Einzelheiten der zentralen Vorgaben für die Sekundärnutzung wird dann in Abschnitt 4.1 eingegangen.

3.3.1 Datenschutzgesetz

a) Verhältnismässigkeitsmassstab

Wie bereits in Abschnitt 3.1.3 dargelegt, qualifiziert das DSG Daten über die Gesundheit als besonders schützenswerte Daten.[118] Besonders schützenswerte Daten sind eine Unterkategorie von Personendaten, daher gelten für deren Bearbeitung grundsätzlich dieselben Regeln wie für Personendaten im Allgemeinen, sofern das Gesetz keine speziellen Vorkehrungen trifft.[119]

Im Datenschutzrecht gilt jedoch die (ungeschriebene) Regel, wonach umso höhere Anforderungen an die Bearbeitung von Daten zu stellen sind, je sensibler diese sind. Man kann dabei vom Verhältnismässigkeitsmassstab sprechen. Dieser ist bei der Auslegung sämtlicher datenschutzrechtlichen Vorgaben zu berücksichtigen.[120] Indem der Gesetzgeber Gesundheitsdaten als besonders schützenswert bezeichnet, gilt somit bei der Anwendung sämtlicher datenschutzrechtlichen Anforderungen ein strengerer Massstab.

b) Explizite datenschutzrechtliche Vorgaben

Neben dieser, sich aus den allgemeinen Grundsätzen ergebenden, höheren Schwelle für die Bearbeitung von Gesundheitsdaten, erkennt der Gesetzgeber das erhöhte Schutzniveau auch durch explizite Sondervorschriften an. So knüpft das DSG in zahlreichen Bestimmungen an die Begriffe der besonders schützenswerten Personendaten (und Persönlichkeitsprofile) an und unterstellt diese Datenkategorien strengeren Anforderungen als "gewöhnliche" Personendaten.[121] Die Totalrevision des DSG brachte diesbezüglich umfassende Änderungen mit sich, so müssen z.B. Private, die regelmässig besonders schützenswerte Personendaten bearbeiten, ihre Datensammlung – anders als im geltenden Recht – künftig nicht mehr anmelden.[122]

Im Folgenden findet sich ein kurzer Überblick über einige wichtige Sonderbestimmungen für besonders schützenswerte Daten im DSG und nDSG:

---

[118] Art. 3 lit. c DSG bzw. Art. 5 lit. c nDSG.

[119] ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 39.

[120] Vgl. hierzu BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, Rz. 54 m.w.H.

[121] ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 3 Rz. 44.

[122] Art. 11a Abs. 3 lit. a und Abs 5 DSG.

- An die Einwilligung werden strengere Anforderungen gestellt, insbesondere muss sie ausdrücklich erfolgen.[123] Folglich ist eine aktive Willensäusserung des Einwilligenden erforderlich (z.B. durch das Unterzeichnen eines Formulars oder Anklicken einer Checkbox).[124]

- Gemäss Art. 22 Abs. 2 lit. a nDSG gilt die umfangreiche Bearbeitung von besonders schützenswerten Personendaten explizit als besonders riskant, dementsprechend muss – nach dem Vorbild der DSGVO – eine Datenschutzfolgeabschätzung durchgeführt werden. Diese hat eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte zu enthalten.[125]

- Die Bekanntgabe von besonders schützenswerten Personendaten an Dritte stellt gemäss Art. 30 Abs. 2 lit c nDSG stets eine Persönlichkeitsverletzung dar und bedarf daher, anders als "gewöhnliche" Datenbearbeitungen, immer eines Rechtfertigungsgrunds. Mögliche Rechtfertigungsgründe sind die Einwilligung der betroffenen Person oder die Bearbeitung im Rahmen der Forschungsausnahme.[126]

- Ferner benötigen Bundesorgane für die Bearbeitung von besonders schützenswerten Personendaten grundsätzlich eine Ermächtigung in einem Gesetz, weshalb im Unterschied zur "gewöhnlichen" Datenbearbeitung eine Grundlage bzw. Ermächtigung in einer blossen Verordnung nicht genügt.[127]

- Für nicht personenbezogene Zwecke – insbesondere für Forschung, Planung oder Statistik – dürfen Private und Bundesorgane besonders schützenswerte Daten an Dritte grundsätzlich nur dann bekanntgeben, wenn die betroffenen Personen für den Empfänger nicht bestimmbar sind.[128] Laut Botschaft zum totalrevidierten DSG ist diese Voraussetzung erfüllt, wenn die Weitergabe in pseudonymisierter Form erfolgt und der Schlüssel bei der weitergebenden Person verbleibt (faktische Anonymisierung).[129]

3.3.2 Humanforschungsgesetz

Im Gegensatz zum DSG beschäftigt sich das Sonderdatenschutzrecht des HFG ausschliesslich mit der Bearbeitung von besonders sensitiven Daten und biologischem Material, aus welchem solche Daten gewonnen werden können. Der besonders schützenswerte Charakter dieser Datenarten spiegelt sich in der Konzeption sämtlicher Datenschutzbestimmungen des HFG wider, wobei für die Erreichung des öffentlichen Interesses an der Forschung ein gewisser Spielraum geschaffen wird. In Grenzfällen der Abwägung zwischen den Inte-

123 Art. 6 Abs. 7 lit. a nDSG.

124 Vgl. dazu sowie den Lehrmeinungen, BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, Rz. 113 ff. m.w.H.

125 Art. 22 Abs. 3 nDSG.

126 Art. 31 Abs. 2 lit. e nDSG.

127 Art. 34 Abs. 2 lit. a nDSG.

128 Art. 39 Abs. 1 lit. b nDSG.

129 Botschaft zum nDSG, BBl 2017 S. 173.

ressen der Wissenschaft und der Gesellschaft und jenen des einzelnen Menschen überwiegen die Interessen Gesundheit und Wohlergehen des Individuums.[130] Neben datenschutzrechtlichen Erwägungen sind bei der Forschung mit Gesundheitsdaten und biologischem Material auch ethische Standards zu beachten, deren Einhaltung durch die zuständigen kantonalen Ethikkommissionen überwacht wird.[131]

Die Sonderdatenschutzbestimmungen sind im HFG und der HFV verstreut. Überblicksartig sind folgende Bereiche zu nennen, auf die in Kapitel 4 näher eingegangen wird:

- Der zweite Abschnitt des zweiten Kapitels des HFG nennt die Anforderungen an eine wirksame Einwilligung und die Aufklärungspflichten im Zusammenhang mit der Einbeziehung in ein Forschungsprojekt, der Erhebung von Gesundheitsdaten und biologischem Material und der Weiterverwendung für die Forschung. Die konkreten formellen und inhaltlichen Anforderungen an die Aufklärung und Einwilligung werden in der HFV festgelegt. Im Gegensatz zum im DSG verankerten Zweckbindungsgrundsatz[132] kann durch den sogenannten "Generalkonsent" auch ganz allgemein in die Weiterverwendung zu Forschungszwecken eingewilligt werden.[133] Dies gilt jedoch nicht für unverschlüsseltes biologisches Material bzw. genetische Daten, bei denen eine Einwilligung für das bestimmte Forschungsprojekt notwendig ist.[134]

- Kapitel 4 des HFG regelt die Weiterverwendung von biologischem Material und Gesundheitsdaten zu Forschungszwecken. Hierbei werden verschieden strenge Anforderungen an die Bearbeitung von biologischem Material und genetischen Daten einerseits, und nichtgenetischen Gesundheitsdaten andererseits gestellt. Darüber hinaus wird innerhalb dieser beiden Kategorien zwischen verschlüsselten und unverschlüsselten Daten bzw. biologischem Material unterschieden.

3.3.3 Vielzahl von zusätzlichen Sonder-Vorschriften für Gesundheitsdaten

Die oben beschriebenen Bestimmungen des DSG und des HFG regeln die Bearbeitung von Gesundheitsdaten nicht abschliessend. Vielmehr sind zahlreiche weitere einschlägige Vorgaben in einer Vielzahl von kantonalen und eidgenössischen Rechtsakten verstreut. So sind z.B. in folgenden Bundesgesetzen sektorspezifische Datenschutzbestimmungen zu Gesundheitsdaten zu finden:

1. Strafgesetzbuch mit Vorschriften zum Berufsgeheimnis (insb. von Ärztinnen und Ärzten)

2. Bundesgesetz über das elektronische Patientendossier (EPDG[135]),

3. Krankenversicherungsgesetz (KVG[136]),

---

130 Art. 4 HFG.

131 Kapitel 9 HFG.

132 Art. 4 Z. 3 DSG bzw. Art. 6 Z. 3 nDSG.

133 Art. 17 HFG; Art. 29 Abs. 1 lit. a HFV.

134 Art. 28 HFV.

135 Bundesgesetz über das elektronische Patientendossier vom 19. Juni 2015, SR 816.1 (im Folgenden EPDG).

136 Bundesgesetz über die Krankenversicherung (Krankenversicherungsgesetz, KVG), SR 832.10 (im Folgenden KVG).

4. Epidemiengesetz (EPG[137]),

5. Krebsregistrierungsgesetz (KRG[138]).

Noch schwerer fällt der schweizweite Überblick aufgrund der Vielzahl von zusätzlichen Vorschriften auf kantonaler Ebene. Hierzu sind nicht nur die bereichsübergreifenden kantonalen Datenschutzgesetze zu zählen, welche insbesondere im Krankenversorgungs- und Universitätswesen von grosser Bedeutung sind. Vielmehr haben auch die einzelnen Kantone umfangreiche Sondervorschriften für das Gesundheitswesen erlassen, worin auch Regelungen mit Bedeutung für den Umgang mit Gesundheitsdaten enthalten sind (z.B. Regelungen zur Dokumentation und Aufbewahrung von Patienteninformationen).

Die Vielzahl an nur beschränkt aufeinander abgestimmten Sondervorschriften auf verschiedenen Ebenen ist ein weiteres Merkmal, das die rechtliche Sonderbehandlung von Gesundheitsdaten kennzeichnet. Die daraus resultierende teils unübersichtliche Rechtslage erschwert die Bearbeitung von Gesundheitsdaten erheblich und hemmt Innovation in Forschung und der Life-Sciences-Branche. Die dadurch entstehende Rechtunsicherheit ist sowohl für die betroffenen Personen, die ihre Rechte schwer überblicken können, als auch für die Datenbearbeiter nachteilig.

3.4 Fazit zur rechtlichen Spezialbehandlung von Gesundheitsdaten

Die vorangehenden Ausführungen haben aufgezeigt, dass bereits für die rechtliche Erfassung des Begriffs der Gesundheitsdaten eine Vielzahl von offenen Fragen und damit Unsicherheiten bestehen. Der Vergleich zwischen den zwei grundlegendsten Erlassen, dem DSG und dem HFG, wirft für die Bearbeitung von Gesundheitsdaten auf Bundesebene Fragen auf, ob und inwieweit tatsächlich von einem übereinstimmenden Begriffsverständnis ausgegangen wird. Damit verbunden sind Unklarheiten in Bezug auf die Anforderungen an die Anonymisierung und Pseudonymisierung von Gesundheitsdaten, die darüber entscheiden, inwieweit die strengen rechtlichen Voraussetzungen berücksichtigt werden müssen.

Bereits der Überblick über die rechtlichen Vorschriften veranschaulicht, dass für den Umgang mit Gesundheitsdaten im Vergleich zu anderen Daten "erhöhte" und besondere rechtliche Anforderungen gelten. Gesundheitsdaten sind damit nicht nur auf "Begriffsebene", sondern auch in Bezug auf die Vorgaben zum Umgang mit diesen Daten ein rechtlicher Sonderfall. Der Gesetzgeber will mit den erhöhten Anforderungen dem erhöhten Schutzbedürfnis für Gesundheitsdaten Rechnung tragen.

Gleichzeitig, und trotz dieses gesetzlich berücksichtigten Schutzbedarfs, besteht ein wirtschaftlich und gesellschaftlich grosses Interesse an der Nutzung von Gesundheitsdaten. Es liegt daher ein offensichtlicher Zielkonflikt vor. Der Schweizer Gesetzgeber tut sich, wie nachfolgend gezeigt wird, allerdings schwer, eine ausgewogene Abwägung der gegenläufigen Interessen vorzunehmen. Er schafft damit, gerade auch infolge der damit geschaffenen Unsicherheit, Hindernisse für eine an sich oftmals gesellschaftlich erwünschte Nutzung. Bei der Lösung dieses Zielkonfliktes gilt es unter anderem auch den für die Schweiz verbindlichen Art. 2 der Biomedizinkonvention des Europarates zu berücksichtigen, wonach "das Interesse und das Wohl

[137] Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz, EpG), SR 818.101 (im Folgenden EpG).

[138] Bundesgesetz über die Registrierung von Krebserkrankungen (Krebsregistrierungsgesetz, KRG), SR 818.33 (im Folgenden KRG).

des menschlichen Lebewesens haben Vorrang gegenüber dem blossen Interesse der Gesellschaft oder der Wissenschaft".[139] Dieser Grundsatz ist auch in Art. 4 HFG verwirklicht.

4. Übersicht über die geltenden Rahmenbedingungen der Sekundärnutzung von Gesundheitsdaten

Nachdem vorangehend aufgezeigt wurde, was unter Gesundheitsdaten zu verstehen ist und inwiefern diese einen rechtlichen Sonderfall darstellen, folgt in diesem Abschnitt eine Übersicht über die geltenden Rahmenbedingungen der Sekundärnutzung von Gesundheitsdaten. Die nachfolgende Darstellung beginnt mit dem bereichsübergreifenden Datenschutzgesetz auf Bundesebene und fährt mit dem zweiten grundlegenden Bundeserlass fort, dem Humanforschungsgesetz, bevor dann auf ausgewählte kantonale Datenschutzgesetze und abschliessend die weiteren zentralen Vorschriften des Bundes eingegangen wird.

Die Bereitstellung einer Übersicht im eigentlichen Sinn ist anspruchsvoll, wie bereits die einleitenden Erläuterungen zum Sonderfall verdeutlichen. Denn es handelt sich um eine Vielzahl von Sonderbestimmungen mit jeweils eigenem Geltungsbereich und eigenen Begrifflichkeiten und die Erfassung der rechtlichen Rahmenbedingungen gelingt nicht, ohne diese miteinander in Verbindung zu setzen und das Verhältnis der jeweiligen Regelwerke zu beleuchten.

Darüber hinaus wird auch deutlich werden, dass den Bestimmungen sehr häufig die nötige Klarheit fehlt und auch die Lehre und Rechtsprechung dieses Defizit (noch) nicht beseitigen konnte. Folglich setzt die Darstellung der Rahmenbedingungen und die Analyse der Hindernisse ein Mindestmass an Tiefe bei der Auseinandersetzung voraus, was die Erarbeitung der Übersicht erschwert und zugleich selbst ein wesentliches Hindernis zum Ausdruck bringt.

4.1 Sekundärnutzung von Gesundheitsdaten im DSG

4.1.1 Geltungsbereich und Grundbegriffe

Wie bereits eingangs erwähnt, ist das DSG für die Bearbeitung von Gesundheitsdaten zentral und weist einen breiten Anwendungsbereich auf. Es wurde bereits aufgezeigt, wie breit der Begriff der Personendaten ist, wann von anonymisierten Daten auszugehen ist und dass jeder Umgang mit Personendaten (inkl. der Vorgang der Anonymisierung) eine Datenbearbeitung im Sinne des DSG darstellt.[140] Nachfolgend werden die weiteren Elemente des Geltungsbereichs des DSG aufgezeigt.

[139] Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin (Übereinkommen über Menschenrechte und Biomedizin), AS 2008 5137, BBl 2002 271.

[140] Siehe oben insb. Abschnitt 3., insbesondere 3.1.2.

a) Persönlicher Geltungsbereich

Zentral für den Geltungsbereich des DSG ist, dass es nur für die Bearbeitung von Personendaten durch private Personen und durch Bundesorgane gilt. Als Bundesorgan gilt eine Behörde oder Dienststelle des Bundes oder eine Person, die mit öffentlichen Aufgaben des Bundes betraut ist.[141] Zu den Behörden und Dienststellen des Bundes zählen alle der Bundesverwaltung zurechenbaren Einheiten,[142] d.h. sowohl die Zentralverwaltung, aber auch die dezentrale Verwaltung, also namentlich auch verselbständigte Verwaltungseinheiten ohne Rechtspersönlichkeit, öffentlich-rechtliche Körperschaften, Stiftungen und Anstalten sowie vom Bund beherrschte Aktiengesellschaften.[143] Die beiden letztgenannten dezentralen Stellen werden jedoch nur dann der Bundesverwaltung zugerechnet, sofern sie nicht "überwiegend Dienstleistungen am Markt erbringen".[144] Diese Beurteilung fällt nicht immer leicht und muss im Einzelfall vorgenommen werden. Als Orientierungshilfe für die Zugehörigkeit zur Bundesverwaltung ist die Auflistung in Anhang 1 der Regierungs- und Verwaltungsorganisationsverordnung (RVOV) zu sehen. Bei den dort aufgeführten Einheiten ist regelmässig von der Qualifikation als Bundesorgan auszugehen. Zu erwähnen sind dabei bspw. die Eidg. Technischen Hochschulen von Zürich (ETHZ) und Lausanne (EPFL) sowie die Eidgenössische Materialprüfungs- und Forschungsanstalt (EMPA).

Die Auflistung ist nicht vollständig und es gibt eine Vielzahl von Bundesorganen, die nicht aufgeführt sind. Dies ergibt sich bereits aus dem letzten Teil der Begriffsdefinition, wonach auch private Rechtssubjekte Bundesorgane sein können, soweit sie mit Bundesaufgaben betraut sind. Gerade im Gesundheitsbereich sind diese in besonders grosser Zahl anzutreffen. So sind grundsätzlich auch die obligatorischen Krankenversicherer[145] und Unfallversicherer[146] als Bundesorgane zu betrachten. Dies gilt allerdings nur insoweit, als diese Versicherer Personendaten bei der Erfüllung einer öffentlichen Bundsaufgabe bearbeiten.[147] Abgesehen davon, dass bereits der Begriff der öffentlichen (Bundes-)Aufgaben und das Betrautsein mit einer solchen Aufgabe strittig ist und anhand einer Vielzahl von Kriterien zu prüfen sind,[148] fällt auch die Zurechnung von Tätigkeiten und Bearbeitungen zur Erfüllung einer solchen Aufgabe nicht immer leicht[149].

Bundesorgane sind ferner von kantonalen Organen abzugrenzen. Während auf die Umschreibungen der kantonalen Organe an späterer Stelle[150] eingegangen wird, ist bereits hier festzuhalten, dass nicht restlos

---

141 Art. 3 lit. h DSG/Art. 5 lit. I nDSG.

142 Vgl. dazu Art. 6 ff. RVOV.

143 Vgl. WALDMANN/BICKEL, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 12 N 8; ähnlich BELSER/NOUREDDINE, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 12 N 14.

144 Vgl. Art. 7a Abs. 1 lit. c und d RVOV.

145 Vgl. BGE 131 II 413, E. 2.3; Urteil des BVGer vom 19. März 2019, A-3548/2018), E. 4.5.5.

146 Urteil des BVGer vom 30.3.2009, A-6067/2008, E. 5.2.1.

147 Vgl. dazu sowie mit Hinweis auf die Entstehungsgeschichte WALDMANN/BICKEL, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, Bern 2011, § 16 N 16; trotz geändertem Wortlaut der Definition gilt dies aber gleichermassen auch unter dem nDSG, Botschaft zum DSG, BBl. 2017 7023.

148 Vgl. dazu z.B. ROSENTHAL/JÖHRI, Handkommentar zum Datenschutzgesetz, 2008, Art. 3 N 99; WALDMANN/BICKEL, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 12 N 16.

149 EPINEY, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, in: Jusletter 2. März 2015, Rz. 25 ff.

150 Siehe Abschnitt 4.3.1.

klar erscheint, inwiefern welche kantonalen Rechtseinheiten auch Bundesorgane sein können. Im Grundsatz steht immerhin fest, dass dem Bund die Verfassungs-Kompetenz fehlt, den Datenschutz im kantonalen öffentlichen Bereich zu regeln, und den Kantonen diesbezüglich eine verfassungsrechtliche Organisationsautonomie zukommt.[151] Die Kantone bestimmen deshalb grundsätzlich[152] selbst inwieweit die kantonale Datenschutzordnung für die kommunalen Verwaltungen gelten soll.[153] Ausgeschlossen ist die Qualifikation als Bundesorgan somit jedenfalls bei Einheiten, die nach den kantonalen gesetzlichen Vorgaben als Teil der Verwaltung im Sinne von "Behörden oder Dienststellen" anzusehen sind. Dies dürfte bei den Einheiten der Zentralverwaltung stets der Fall sein und sie unterliegen deshalb vollumfänglich für alle Tätigkeitsbereiche den kantonalen Datenschutzgesetzgebungen,[154] zumindest sofern sie nicht wie Private handeln. Weniger klar wird die Einordnung jedoch bereits für öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen sowie spezialgesetzliche Gesellschaften der Kantone sein. Auch hier muss zunächst geprüft werden, ob diese in den kantonalen Vorschriften der kantonalen Verwaltung zugerechnet werden und sie insoweit als Behörden und Dienststellen des Kantons zu betrachten sind, die der Regelungshoheit der kantonalen Datenschutzgesetzgeber unterliegen. Ist dies nicht der Fall, wird auch hier zu prüfen sein, inwieweit die betroffene Einheit Aufgaben des Bundes oder des Kantons wahrnimmt.[155] Mit anderen Worten kann anhand der Trägerschaft alleine noch keine Qualifikation vorgenommen werden.[156] Ist eine Einheit aber nach den genannten Kriterien als kantonales und nicht als Bundesorgan zu qualifizieren, ändert sich daran nach der Rechtsprechung des Bundesgerichts zumindest dadurch nichts, dass das Organ (auch) Bundesrecht vollzieht.[157]

Zudem sagt die Qualifikation als Bundesorgan alleine noch nichts darüber aus, welche Vorschriften des DSG zur Anwendung kommen. Denn wenn das Bundesorgan privatrechtlich handelt, untersteht es für die damit verbundenen Datenbearbeitungen gleichwohl den Vorschriften des DSG für Private.[158] Es stellen sich insofern vergleichbare Fragen wie für privatrechtlich organisierte Rechtseinheiten, die am Markt auftreten, aber mitunter auch Bundesaufgaben übernehmen. Sowohl private Organisationen als auch Verwaltungseinheiten können deshalb für verschiedene Datenbearbeitungen auch von verschiedenen Vorschriften innerhalb des DSG erfasst sein. Folglich ist stets im Einzelfall für die jeweilige Datenbearbeitung zu prüfen, welche Vorschriften des DSG greifen.

b) Räumlicher Geltungsbereich

Der räumliche Geltungsbereich war bisher nicht explizit im DSG normiert. Im Zuge der Totalrevision wurde nun in Art. 3 nDSG verankert, was auch bisher galt. Demzufolge ist das DSG "für Sachverhalte, die sich in

---

151 Botschaft zum DSG, BBl 1988 S. 425 f.; vgl. auch ROSENTAHL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 37 N 1.

152 Auf den Vorbehalt in Art. 37 DSG wird hier nicht näher eingegangen, haben doch mittlerweile alle Kantone ein angemessenes Datenschutzgesetz und wird die Bestimmung im künftigen totalrevidierten Recht auch nicht mehr gelten, vgl. Botschaft zum DSG, BBL 2017 S. 7105.

153 Botschaft zum DSG, BBl 1988 S. 425 f.; vgl. auch ROSENTAHL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 37 N 1.

154 So auch EPINEY, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, in: Jusletter 2. März 2015, Rz. 20.

155 Vgl. EPINEY, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, in: Jusletter 2. März 2015, Rz. 20.

156 Vgl. auch PRIEUR, Welches Datenschutzrecht ist für Spitäler als Arbeitgeber anwendbar? Beispiel: Kanton Bern, in: Jusletter 18. Mai 2015, Rz. 23; anders aber offenbar ISLER, Die Rollenverteilung in klinischen Versuchen, in: digma 2020 S. 68, 69.

157 BGE 122 I 153, E. 2 d.

158 Art. 40 nDSG.

der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden" anwendbar.[159] Ein Bespiel für eine "ausländische Veranlassung" sind Websites, die zwar nicht in der Schweiz gehostet werden, jedoch hier abrufbar sind.[160] Damit wird letztlich auch in der Schweiz eine extraterritoriale Anwendung des Gesetzes verankert, wie sie die EU-DSGVO kennt. Ferner ist für privatrechtliche Ansprüche das internationale Privatrecht einschlägig, insbesondere Art. 139 IPRG, wonach der in seiner Persönlichkeit Verletzte die für ihn günstigere Rechtsordnung wählen darf. Hat der Verletzte seinen gewöhnlichen Aufenthalt in der Schweiz, kann er auch bei im Ausland erfolgten Persönlichkeitsverletzungen das Schweizer Datenschutzrecht wählen, sofern die gesetzlichen Voraussetzungen erfüllt sind.[161] Für die Praxis bedeutet dies, dass die an grenzüberschreitenden Projekten beteiligten Organisationen in vielen Fällen sowohl die Vorschriften des DSG als auch diejenigen der EU-DSGVO zu berücksichtigen haben.

4.1.2 Verhältnis zu anderen Erlassen

Das DSG ist als allgemeines, d.h. bereichsübergreifendes Gesetz ausgestaltet. Es kann daher als Rahmenerlass[162] bezeichnet werden, das die Anforderungen an Datenbearbeitungen losgelöst von einem spezifischen Lebensbereich oder einem bestimmten Sektor vorsieht.[163] Daneben besteht aber bereits auf Bundesebene eine sehr grosse Zahl von sektorspezifischen Gesetzen, die ebenfalls Regelungen mit Bezug zum Datenschutz enthalten. Es stellt sich deshalb die Frage nach dem Verhältnis der Bestimmungen des DSG zu denjenigen in anderen Erlassen.

Im Grundsatz besteht dahingehend Einigkeit, dass das DSG neben den Spezialgesetzen anwendbar bleibt.[164] In diesem Sinne hält auch die Botschaft zur Totalrevision des DSG fest: "Das Datenschutzgesetz gilt für medizinische Daten unter Vorbehalt der Spezialgesetze".[165] Inwieweit aber die jeweiligen Vorschriften einander verdrängen und von einem Vorrang ausgegangen werden muss, ist bereits im Ansatz ungeklärt. So geht die Botschaft zum DSG 1988 offenbar davon aus, dass dieses grundsätzlich "Vorrang vor andern Datenbearbeitungsvorschriften hat."[166] In diesem Sinne wird denn auch teilweise vertreten, dass die datenschutzrechtlichen Grundsätze des DSG durch andere Erlasse nicht relativiert werden dürften.[167] Anders sieht dies das Bundesverwaltungsgericht, nach welchem der bereichsspezifische Gesetzgeber nicht an das

---

159 Art. 3 Abs. 1 nDSG.

160 MAURER-LAMBROU/KUNZ, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 2 Rz. 19b; BGE 1C_230/211 E 3.3.

161 Art. 139 Abs. 3 IPRG.

162 BOLLINGER ET AL., Schlussbericht Evaluation des Bundesgesetzes über den Datenschutz, 2011, S. 11 und 41, www.buerovatter.ch/pdf/2011-Evaluation%20Datenschutzgesetz.pdf (zuletzt aufgerufen: 12.05.2022).

163 EPINEY, in: Belser/Epiney/Waldmann (Hrsg.), Datenschutzrecht, 2011, § 9 N 8.

164 Botschaft zum DSG, BBl 1988 S. 444; ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 2 N 2.

165 Botschaft zum DSG, BBl. 2017 S. 7009.

166 Botschaft zum DSG, BBl 1988 S. 444.

167 EPINEY, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 9 N 8; ähnlich BELSER/NOUREDDINE, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, Bern 2011, § 8 N 90.

Schutzniveau des Datenschutzgesetzgebers gebunden sei; vielmehr könne er andere Wertungen bzw. Regelungen vorsehen.[168] Zum gleichen Schluss gelangte das Bundesgericht in Bezug auf das (frühere allgemeine) Datenschutzgesetz des Kantons Zürich.[169] Dies entspricht unseres Erachtens auch dem richtigen Verständnis, wie es sich bereit aus der erwähnten Stelle der Botschaft ergibt[170] und von der wohl überwiegenden Auffassung vertreten wird.[171]

Danach ist entscheidend, ob mit einer Regelung im Spezialgesetz bewusst von den Vorschriften des DSG abgewichen werden soll und der Bereichsgesetzgeber insofern eine abschliessende Regelung aufgestellt hat.[172] Es ist somit für jede Norm in einem Spezialgesetz im Einzelfall zu ermitteln, inwieweit diese als abschliessende Regelung zu verstehen ist und inwieweit daneben noch Raum für die ergänzende Anwendung des DSG besteht. Mit anderen Worten ist jeweils zunächst zu prüfen, ob Spezialgesetzgebungen bestehen und ob darin Vorschriften enthalten sind, die eine bestimmte Frage abschliessend regeln. Ist dies der Fall, kann das DSG immerhin im Rahmen der Auslegung der (abschliessenden) Bestimmungen beigezogen werden.[173] Ist dies nicht der Fall, gelangt das DSG zur Anwendung. Angesichts der Vielzahl von Spezialgesetzten, gerade im Gesundheitssektor, und der spärlichen Rechtsprechung und wissenschaftlichen Aufarbeitung, fehlen jedoch klare Antworten auf die Frage, ob und inwieweit eine abschliessende Regelung vorliegt.

Bereits daraus wird ersichtlich, dass in der Praxis das Ermitteln der für eine bestimmte Fragestellung einschlägigen Vorgaben Schwierigkeiten und massgebliche Unsicherheiten verursachen kann. Dies wird im Abschnitt 4.2 zu den Vorschriften des HFG im Detail veranschaulicht werden.

4.1.3 Datenschutzrechtliche Rollen

Entsprechend den Vorgaben der EU-DSGVO stellt das nDSG bei der Zuweisung von Pflichten auf verschiedene datenschutzrechtliche Rollen ab. Zentral ist dabei die Rolle des Verantwortlichen. Diesem wird der Grossteil der Pflichten auferlegt und er wird definiert als "private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet".[174] Bereits daraus wird deutlich, dass für eine Datenbearbeitung auch eine gemeinsame Verantwortlichkeit mehrerer Personen vorliegen kann, wenn diese gemeinsam über den Zweck und die Mittel entscheiden. Abzugrenzen ist die Rolle des Verantwortlichen von derjenigen des Auftragsbearbeiters. Dieser existiert bereits im geltenden

168 Urteil des BVGer vom 10.4.2012, A-4467/2011, E. 4.3.

169 BGE 124 I 176, E. 5c/ee.

170 Botschaft zum DSG, BBl 1988 S. 444: "Wenn aber das Spezialrecht strengere Datenschutznormen oder eine in sich geschlossene Datenschutzkonzeption enthält, gehen diese Bestimmungen ausnahmsweise jenen des allgemeinen Datenschutzgesetzes vor."

171 Vgl. Urteil des BVGer vom 10.4.2012, A-4467/2011, E. 4.3; BGE 133 V 359, E: 6.4; BGE 124 I 176, E. 5c/ee; MEIER, Protection des données, 2010, Rz. 372.

172 MEIER, Protection des données, Bern 2010, Rz. 288; ROSENTHAL/JÖHRI, Handkommentar zum Datenschutzgesetz, 2008, Art. 2 N 2; GERSCHWILER, in: PASSADELIS/ROSENTHAL/THÜR (Hrsg.), Datenschutzrecht, 2015, Rz. 3.17; BRUNNER, in: RÜTSCHER (Hrsg.), SHK-HFG, 2015, Vorbemerkungen Art. 56-61 N 4 ff.; vgl. auch die Praxis des BVGer im Asylbereich, z.B. im Urteil des BVGer vom 8.8.2018, E-4293/2018, E. 7 f.

173 Vgl. MEIER, Protection des données, 2010, Rz. 288.

174 Art. 5 lit. j nDSG.

DSG und wird im nDSG definiert als "private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet."[175]

Die Zuordnung der jeweiligen Rollen ist angesichts der immer stärker arbeitsteiligen Datenbearbeitung komplex und wird zu Recht als datenschutzrechtliche "Gretchenfrage" bezeichnet.[176] Für das Schweizer Recht kann durch die Übernahme der Definition aus der EU-DSGVO immerhin im Grundsatz auch die Lehre und Rechtsprechung dazu beigezogen werden und es ist eine einheitliche Auslegung angezeigt.[177] Es gilt deshalb auch in der Schweiz, dass der Gesetzgeber die Möglichkeit hätte, die Rollen in den Spezialgesetzen festzulegen. Leider ist dies aber bisher kaum je der Fall gewesen, wie z.B. der Blick in das Humanforschungsgesetz verdeutlicht. Fehlt eine gesetzliche Regelung, ist auch in der Schweiz auf die faktischen Gegebenheiten abzustellen.[178]

Auch wenn auf Ebene der EU bereits ausführliche Leitlinien veröffentlicht und auch höchstrichterliche Leitentscheide ergangen sind, erweist sich die Zuweisung der Rollen in der Praxis nach wie vor schwierig und ist eine der meist diskutierten Fragen. Erschwerend kommt dazu, dass die Verantwortlichkeiten für jeden Zweck und jede einzelne Bearbeitung zu beurteilen sind, d.h. z.B. gesondert für die Beschaffung der Daten und auch für jede Primärnutzung und jede Sekundärnutzung, und dass daher nicht zwingend für einen gesamten Arbeitsprozess dieselbe Verantwortlichkeit gilt. Wie oben vorstehend bereits in Abschnitt 3.1.2.d) erläutert, lässt sich die Verantwortlichkeit zudem auch nicht durch die Frage der Inhaberschaft oder des Zugangs zu Daten abgrenzen, ist doch eine (gemeinsame) Verantwortlichkeit auch ohne Zugang zu den Daten möglich. All dies erhöht die Komplexität und die damit verbundenen Unsicherheiten.

Veranschaulicht werden kann dies an folgendem Beispiel der EU-Datenschutzbehörden[179]:

> *Ein Gesundheitsdienstleister (der Prüfer) und eine Hochschule (der Sponsor) beschließen, gemeinsam eine klinische Prüfung zu demselben Zweck einzuleiten. Sie arbeiten gemeinsam an der Ausarbeitung des Studienprotokolls (d. h. Zweck, Methodik/Konzeption der Studie, zu erhebende Daten, Kriterien für den Ausschluss/die Einbeziehung der Probanden, ggf. Weiterverwendung der Datenbank usw.). Sie können als gemeinsam Verantwortliche für diese klinische Prüfung betrachtet werden, da sie gemeinsam denselben Zweck und die wesentlichen Mittel für die Verarbeitung festlegen und vereinbaren.*
>
> *Die Erhebung personenbezogener Daten aus der Patientenakte zu Forschungszwecken ist von der Speicherung und Verwendung derselben Daten für die Zwecke der Patientenversorgung zu unterscheiden, für die der Leistungserbringer weiterhin der Verantwortliche bleibt.*
>
> *Nimmt der Prüfer nicht an der Ausarbeitung des Prüfplans teil (er akzeptiert lediglich den vom Sponsor bereits ausgearbeiteten Prüfplan), und wird der Prüfplan nur vom Sponsor konzipiert, so*

---

175 Art. 5 lit. k nDSG.

176 Vgl. ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019.

177 So verweist auch die Botschaft zum DSG, BBl 2017 S. 7023, explizit darauf, dass die Begriffe denjenigen der EU-DSGVO entsprechen.

178 Leitlinien des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, 2021, Rz. 12.

179 Leitlinien des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, 2021, S. 26.

sollte der Prüfer als Auftragsverarbeiter und der Sponsor als Verantwortlicher für diese klinische Prüfung betrachtet werden.

Der erste Absatz des Beispiels zeigt den vermeintlich leicht fassbaren Grundsatz, wobei die anschliessenden Absätze die erforderliche Differenzierung und Abgrenzung zwischen Co-Verantwortlichkeit und Auftragsbearbeitung deutlich machen. Die Realität ist jedoch noch deutlich komplexer, muss doch nur schon in Bezug auf den Vorgang der Pseudonymisierung noch weiter differenziert werden.[180]

Auch das weitere Beispiel in den Leitlinien der EU-Behörden[181] für die Bearbeitungen von Gesundheitsdaten ausserhalb von klinischen Versuchen zeigt, dass in der Praxis bei der Beurteilung eine Vielzahl von Aspekten zu berücksichtigen sind:

Unternehmen ABC, Entwickler einer App für Blutdrucküberwachung, und Unternehmen XYZ, Anbieter von Apps für medizinische Fachkräfte, möchten beide untersuchen, wie Blutdruckveränderungen zur Vorhersage bestimmter Krankheiten beitragen können. Die Unternehmen beschließen, ein gemeinsames Projekt ins Leben zu rufen und beim Krankenhaus DEF anzufragen, ob es sich ebenfalls beteiligen möchte.

Bei den personenbezogenen Daten, die im Rahmen dieses Projekts verarbeitet werden, handelt es sich um personenbezogene Daten, die das Unternehmen ABC, das Krankenhaus DEF und das Unternehmen XYZ jeweils als einzelne für die Verarbeitung Verantwortliche verarbeiten. Die Entscheidung, diese Daten zur Beurteilung von Blutdruckänderungen zu verarbeiten, wird von den drei Akteuren gemeinsam getroffen. Das Unternehmen ABC, das Krankenhaus DEF und das Unternehmen XYZ haben die Zwecke der Verarbeitung gemeinsam festgelegt. Unternehmen XYZ ergreift die Initiative und schlägt die wesentlichen Mittel zur Verarbeitung vor. Sowohl das Unternehmen ABC als auch das Krankenhaus DEF akzeptieren diese wesentlichen Mittel, nachdem sie ebenfalls an der Entwicklung einiger Merkmale der App beteiligt waren, sodass die Ergebnisse von ihnen ausreichend genutzt werden können. Die drei Organisationen einigen sich somit darauf, einen gemeinsamen Zweck für die Verarbeitung zu haben, der darin besteht, zu bewerten, inwieweit Veränderungen des Blutdrucks zur Vorhersage bestimmter Krankheiten beitragen können. Nach Abschluss der Forschungsarbeiten können das Unternehmen ABC, das Krankenhaus DEF und das Unternehmen XYZ von der Bewertung profitieren, indem sie deren Ergebnisse im Rahmen ihrer eigenen Tätigkeiten verwenden. Aus all diesen Gründen gelten sie für diese konkrete gemeinsame Verarbeitung als gemeinsam Verantwortliche.

Wäre Unternehmen XYZ von den anderen lediglich aufgefordert worden, diese Bewertung vorzunehmen, ohne einen eigenen Zweck zu verfolgen und lediglich Daten für die anderen zu verarbeiten, würde das Unternehmen XYZ als Auftragsverarbeiter gelten, selbst wenn es mit der Festlegung der nicht wesentlichen Mittel betraut wäre.

Die praktischen Unsicherheiten bei der Zuweisung der datenschutzrechtlichen Rollen sind als ein weiteres potentielles Hindernis für die Sekundärnutzung von Gesundheitsdaten zu werten. Denn die Praxis zeigt, dass gerade bei einer Vielzahl von involvierten Organisationen unterschiedliche Auffassungen über die eigenen Rollen vorherrschen und dies Vertragsverhandlungen erschweren oder gar zum Scheitern bringen kann.

---

[180] Vgl. zum Ganzen ISLER, Die Rollenverteilung in klinischen Versuchen, digma 2020 S. 68 ff.

[181] Leitlinien des EDSA zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, 2021, S. 27.

Die vertragsrechtliche Zuschreibung der Rollen durch die Parteien ist zwar für die datenschutzrechtliche Einordnung nicht entscheidend, wird aber zumindest die interne Zuweisung der Haftung und Regressmöglichkeiten unter den involvierten Parteien massgeblich beeinflussen.

4.1.4 Vorgaben für Sekundärnutzung

Wie aus den vorangehenden Erläuterungen hervorgeht, unterscheiden sich die Vorgaben des DSG je nachdem, ob es sich bei den Verantwortlichen um Bundesorgane oder Private handelt.

Mit Blick auf die Anforderungen an die Sekundärnutzung ist sodann zwischen Voraussetzungen zu unterscheiden, die den Kern der Datenbearbeitung betreffen (nachfolgend: "Kernanforderungen"), und weiteren Anforderungen, die es bei der Sekundärnutzung wie auch bei anderen Datenbearbeitungen zu beachten gilt.

a) Kernanforderungen für Private

Die besonderen Vorgaben des DSG für Private sind im Grundsatz weniger streng ausgestaltet als diejenigen für Bundesorgane. Für die Zulässigkeit einer Sekundärnutzung kann deshalb entscheidend sein, welche der Vorschriften im Einzelfall zur Anwendung gelangen.

Wie zum Geltungsbereich des DSG ausgeführt, sind Private von den Bundesorganen und kantonalen öffentlichen Organen abzugrenzen. Die nachfolgenden Erläuterungen gelten deshalb grundsätzlich für alle, die nicht Bundesorgan oder öffentliches Organ sind. Es wurde allerdings ebenfalls auch bereits angesprochen, dass auch dies nicht ohne Ausnahme bleibt. Handelt nämlich ein Bundesorgan bei bestimmten Tätigkeiten privatrechtlich, so gelten für die damit verbundenen Datenbearbeitungen gleichwohl die Vorschriften für Private.[182] Umgekehrt unterstehen Private bei Tätigkeiten, mit welchen sie öffentliche Aufgaben des Bundes erfüllen, ihrerseits den Vorgaben für Bundesorgane und die nachfolgenden Ausführungen zu den Vorschriften für Private gelten nicht. Auf den Umstand, dass auch kantonale öffentliche Organe den Vorschriften des DSG für Private unterstehen können, wurde ebenfalls bereits hingewiesen.

i.) Rechtmässigkeitsgrundsatz

Von grundlegender Bedeutung für die datenschutzrechtlichen Anforderungen an die Sekundärnutzung von Gesundheitsdaten ist zunächst der sog. Rechtmässigkeitsgrundsatz.[183] Danach wird festgelegt, dass die Datenbearbeitung in Übereinstimmung mit den rechtlichen Vorschriften erfolgen muss. Nach Ansicht des Bundesverwaltungsgerichts und dem überwiegenden Teil der Lehre führt deshalb aber nicht jede Bearbeitung, die gegen eine Rechtsvorschrift verstösst, auch zu einer Verletzung des Rechtmässigkeitsgrundsatzes. Vielmehr gilt dies nur für Verstösse gegen Vorschriften, welche den Schutz der Persönlichkeit bezweckt. Hierzu können grundsätzlich auch die Vorschriften des Datenschutzgesetzes selbst zählen, [184] anders als bspw. die Vorschriften im Krankenversicherungsgesetz zum Umgang mit den Prämien der Versicherten[185]. Zumindest im Verstoss gegen einen Datenbearbeitungsgrundsatz, wie z.B. dem nachfolgend zu erläuternden Zweckbin-

---

182 Art. 40 nDSG.

183 Art. 6 Abs. 1 nDSG.

184 Vgl. zum Ganzen BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 134.

185 Vgl. Art. 60 ff. KVG; Urteil des Bundesverwaltungsgerichts vom 19.3.2019, A-3548/2018, E. 5.5.

dungsgebot, ist deshalb auch ein Verstoss gegen den Rechtmässigkeitsgrundsatz zu sehen. Das Bundesgericht hat allerdings bereits die Streitfrage geklärt, dass ein solcher Verstoss nicht immer unzulässig ist, sondern im Falle von privaten Verantwortlichen – anders als bei Bundesorganen – gerechtfertigt werden kann, z.B. durch eine Einwilligung des Betroffenen.[186]

Aus dem Rechtmässigkeitsgrundsatz folgt auch die für die Sekundärnutzung von Personendaten zentrale Konsequenz, dass jegliche Weiterbearbeitung von Personendaten, die rechtswidrig erhoben wurden, grundsätzlich ebenfalls rechtswidrig ist.[187] Mit anderen Worten muss grundsätzlich bereits bei der Beschaffung der Daten möglichst sichergestellt und möglichst auch nachweisbar dokumentiert werden, dass die Voraussetzungen für die Beschaffung und eine spätere Weiterbearbeitung erfüllt sind. Wurde bei der Beschaffung gegen Vorschriften zum Schutz der Persönlichkeit verstossen, liegt ein Verstoss gegen den Rechtmässigkeitsgrundsatz vor. Dieser Verstoss ist grundsätzlich verboten, wenn nicht ein Rechtfertigungsgrund angerufen werden kann.

Für die Praxis hat der Rechtmässigkeitsgrundsatz zur Folge, dass bei der Sekundärnutzung, die vielfach erst einige Zeit später als die ursprüngliche Beschaffung der Daten erfolgt, sichergestellt und verifizierbar sein muss, dass die damalige Beschaffung rechtmässig erfolgt war. Andernfalls besteht das Risiko eines Verstosses gegen den Rechtmässigkeitsgrundsatz und die Sekundärnutzung wäre verboten und könnte nur bei privaten Verantwortlichen – anders als bei Bundesorganen –zulässig sein, wenn die Voraussetzungen eines Rechtfertigungsgrunds gegeben sind. Die Erfahrung zeigt, dass die entsprechende Dokumentation häufig ungenügend ist und daher eine Unsicherheit besteht.

ii.) Zweckbindungsgebot

Eine der zentralsten Bestimmungen für die Beurteilung der datenschutzrechtlichen Zulässigkeit von Sekundärnutzungen ist das Zweckbindungsgebot[188]. Nach diesem auch in den kantonalen Datenschutzgesetzgebungen und der EU-DSGVO verankerten allgemeinen Datenbearbeitungsgrundsatz dürfen Personendaten nur zu hinreichend bestimmten und für die betroffene Person erkennbaren Zwecken beschafft werden. Sie dürfen ferner nur so (weiter-)bearbeitet werden, dass es mit diesem (originären) Zweck vereinbar ist. Die Bestimmung enthält zwei Teilgehalte: die Zweckfestsetzung und die Zweckbindung,[189] wobei auch ein enger Bezug zu anderen Grundsätzen, insbesondere zum Transparenzgebot besteht.

Mit dem Teilgehalt der Zweckfestsetzung soll sichergestellt werden, dass Daten nur zu einem hinreichend bestimmten Zweck erhoben und bearbeitet werden. Eine Datenbeschaffung für vage, nicht definierte oder unpräzise Zwecke, gewissermassen "auf Vorrat", soll verhindert werden. Der Zweck einer Bearbeitung soll für die betroffene Person bestimmt und erkennbar sein.[190]

Die Frage, wann und welche Zwecke als erkennbar zu betrachten sind, wird im Wortlaut des nDSG weniger deutlich beantwortet als im geltenden DSG. Eine Änderung der Rechtslage wurde damit jedoch nicht bezweckt. Vielmehr kann auch künftig ein Zweck erkennbar sein, der in einem Gesetz vorgesehen ist oder sich

---

186 Vgl. dazu bereits BGE 136 II 508.

187 Vgl. EPINEY, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 9 N 12; BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 134.

188 Art. 6 Abs. 3 nDSG.

189 Vgl. nur MEIER, Protection des données, 2010, Rz. 722; BAERISWYL, in: BAERISWYL/PÄRLI (Hrsg.), SHK-DSG, 2015, Art. 4 N 34.

190 MEIER, Protection des données, 2010, Rz. 723; Botschaft zum DSG, BBl 2017 S. 7025.

aus den Umständen ergibt.[191] In der Praxis wird jedoch regelmässig im Zweifelsfall in einer Information zugunsten der betroffenen Personen der Zweck festgehalten ("angegeben"), also z.B. in sog. Datenschutzerklärungen.

Der zweite Teilgehalt der Zweckbindung verlangt zusätzlich eine Verbindlichkeit des (erkennbaren bzw. erkennbar gemachten) Zwecks. Die Zweckbindung soll ausschliessen, dass der Zweck nachträglich nach eigenem Gutdünken des Verantwortlichen abgeändert wird. Eine nachträgliche Änderung des Zwecks ist deshalb nur soweit zulässig, als dies erkennbar ist für die betroffene Person bzw. erkennbar gemacht wird.[192]

In der Praxis hat es der Verantwortliche demnach bis zu einem gewissen Grad selbst in der Hand, die Reichweite des Zwecks der Datenbearbeitungen festzulegen. Aus Sicht des Zweckbindungsgebots geht es primär darum, dass der Zweck festgelegt ist und weniger darum, inwieweit der Zweck und die Bearbeitung dann auch zumutbar ist für die betroffene Person und letztlich eine rechtmässige Datenbearbeitung vorliegt.[193] Es stellt sich deshalb die Frage, wie konkret der Zweck bestimmt sein muss. Hierauf gibt es keine pauschale Antwort und die Ansätze bzw. Kriterien für die Beantwortung sind bislang nicht höchstrichterlich verankert.

Unseres Erachtens muss der Massstab dafür, was als hinreichend bestimmter Zweck gilt und ob eine (Weiter-)Bearbeitung mit dem (erkennbaren) Zweck vereinbar ist, auch hier derselbe sein, wie er im Zusammenhang mit dem Grundsatz der Transparenz ist. Zum Transparenzgrundsatz erging die bislang am ausführlichsten begründete Stellungnahme in der Schweizer Lehre und es handelt sich nach den Autoren um dieselben Kriterien, die auch bei der Auslegung von Verträgen heranzuziehen sind, namentlich der Massstab von Treu und Glauben.[194] Daraus folgt, dass der Zweck so klar umschrieben sein muss, dass sich eine durchschnittlich verständige betroffene Person ein Bild davon machen kann, wofür ihre Daten erhoben werden (Zweck) und was konkret mit den Daten geschieht (Bearbeitung) und sie gestützt darauf selbst entscheiden kann, ob sie damit einverstanden ist oder andernfalls Widerspruch erheben oder die Einwilligung verweigern will.[195]

Daraus ergibt sich, dass Umschreibungen mit Begriffen, die aufgrund ihrer Vieldeutigkeit letztlich keine annähernd bestimmte Vorstellung über die Datenbearbeitungen hervorrufen können, als Zweckangaben ungenügend sind. Dass unter dem DSG die Information bspw. über eine «Bearbeitung zu Forschungszwecken» deshalb eigentlich ungenügend für eine wirksame Einwilligung wäre, ergibt sich bereits aus der vom Gesetzgeber aufgestellten Ausnahmeregelung für den sog. «Generalkonsent» im HFG[196]. Wäre der Gesetzgeber davon ausgegangen, dass eine solche Formulierung genügt, wäre keine Sonderregelung erforderlich gewesen. Es muss deshalb unter dem DSG deutlicher festgelegt werden, worin der Zweck genau besteht. Dies gilt umso mehr als, wie erläutert, auch bei der Beurteilung des Zweckbindungsgebots ein strengerer Massstab anzusetzen ist, wenn Gesundheitsdaten und damit besonders schützenswerte Daten bearbeitet werden. Es genügt deshalb auch nicht, wenn der Zweck bloss mit Formulierungen wie bspw. "zur Produktoptimierung" oder zu "statistischen Zwecken" umschrieben wird. Eine solche Beschreibung allein vermittelt der

191 Botschaft zum DSG, BBl 2017 S. 7025.

192 Vgl. MEIER, Protection des données, 2010, Rz. 725.

193 Vgl. auch BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 9 N 31.

194 Vgl. nur Botschaft zum DSG, BBl 2003 S. 2125; ferner ausführlich BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz.56.

195 BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 69.

196 Vgl. Art. 32 ff. HFG; ferner ausführlich dazu nachfolgend Abschnitt 4.2.4d).

betroffenen Person kein hinreichend klares Bild davon, wie und wozu ihre Daten konkret bearbeitet werden. Es muss in den Beispielen also zumindest auch klar sein, für welche (zu "optimierenden") Produkte die Daten verwendet und wozu die Statistiken angefertigt werden. Mangels gefestigter Auffassungen in Lehre und Rechtsprechung sind die genauen Anforderungen jedoch ungewiss.

Die Informationen müssen den betroffenen Personen bereits bei der Erhebung ihrer Personendaten bereitgestellt werden bzw. müssen für sie erkennbar sein. Die zu diesem Zeitpunkt erkennbaren Informationen bestimmen auch, was datenschutzrechtlich als originäre Nutzung (Primärnutzung) und was als Sekundärnutzung zu betrachten ist. Wurde bei der Beschaffung der Daten der Zweck einer Datenbearbeitung einmal im oben erläuterten Sinne genügend bestimmt, sind die Anforderungen in Bezug auf diese Datenbearbeitung, aber nur diese konkrete Datenbearbeitung, erfüllt.

Sollen die Daten auch zu einem anderen Vorhaben genutzt werden, ist unter dem Zweckbindungsgebot zu prüfen, ob diese Nutzung für die betroffene Person erkennbar war. Wurde in den Informationen für Patientinnen und Patienten bei der Datenbeschaffung bspw. nur die Verwendung für das detailliert umschriebene Vorhaben zur Optimierung von Produkt XY erwähnt, ist die Verwendung für das Vorhaben zur Optimierung von Produkt Z grundsätzlich nicht ohne Weiteres erkennbar und es ist damit zu rechnen, dass es sich datenschutzrechtlich um einen anderen und nicht kompatiblen bzw. vereinbaren Zweck handelt. Von der Erkennbarkeit könnte deshalb nur dann mit Sicherheit ausgegangen werden, wenn die Verwendung für das Vorhaben zur Optimierung von Produkt Z ebenfalls bereits bei der Beschaffung der Daten im Detail erläutert wird. In diesem Fall wäre die Verwendung der Daten sowohl für das Vorhaben XY als auch die Nutzung der Daten für Vorhaben Z als Primärnutzung zu betrachten. Wurde bei der Erhebung hingegen nur von der Verwendung für Vorhaben XY gesprochen, könnte die Nutzung derselben Daten für das Vorhaben Z als Sekundärnutzung betrachtet werden und es liegt ein Verstoss gegen das Zweckbindungsgebot vor. Etwas anderes würde dann gelten, wenn die betroffenen Personen vor der Nutzung der (bereits beschafften) Daten für das Vorhaben Z darüber informiert werden. Da dies aber in der Regel eine neuerliche Kontaktaufnahme der (möglichen Vielzahl von) betroffenen Personen erfordern würde, ist dies in der Praxis in der Regel kein gangbarer Weg.

Diese Erläuterungen veranschaulichen, dass es der Verantwortliche bis zu einem bestimmten Grad in der Hand hat, bei der Beschaffung mehrere Zwecke anzugeben und insofern die Nutzung der Daten für mehrere Zwecke zu ermöglichen. Allerdings gilt es bei einer solchen Verwendung zu mehreren Zwecken sicherzustellen, dass die betroffenen Personen die Informationen in zumutbarer Weise zur Kenntnis nehmen können, diese also insbesondere verständlich sind, und die Nutzung der Daten für die betroffenen Personen nicht ungewöhnlich/überraschend ist,[197] was in der Praxis mit erheblichen Unsicherheiten verbunden ist. Mit Blick auf künftige Projekte gibt es auch praktische Hindernisse zu beachten. So müssen bereits bei der Beschaffung der Daten die Detailangaben zu den künftigen Vorhaben vorliegen und erläutert werden können. Hierzu gehören zumindest auch die Kategorien der Empfänger der Daten, also der in das Vorhaben involvierten Gruppen von Personen.[198]

---

197 Vgl. hierzu BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 56 ff.

198 Vgl. dazu und zur (ungeklärten und hier verneinten) Frage, inwieweit (auch) im Schweizer Recht die Identität der (Co-)Verantwortlichen bei der Erhebung anzugeben ist, BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 88; Dies hat auch Einfluss auf die unter bisherigem Recht thematisierte und zu bejahende Frage, inwieweit der angegebene Zweck (ohne gegenteilige Präzisierung) nur eigene Zwecke erfasst oder auch diejenigen Dritter bzw. inwieweit die Nutzung der erhobenen Daten durch (nicht angegebene) Dritte zum gleichen Zweck eine Zweckänderung darstellt (vgl. in: Handkommentar zum Datenschutzgesetz, 2008, Art. 4 N 41 f.); Soweit die Kategorien der Dritten (hinreichend präzis und wirksam) angegeben werden, stellt die Nutzung durch diese jedenfalls per se keine Zweckänderung dar.

Oftmals dürften die notwendigen Angaben aber im Zeitpunkt der Beschaffung der Daten noch nicht vorliegen.

Vor diesem Hintergrund wird sich die Information bei der Datenbeschaffung in der Regel auf eine begrenzte Zahl von hinreichend konkret umschreibbaren Vorhaben beschränken müssen. Die Nutzung der erhobenen Daten für andere Vorhaben wird deshalb oftmals eine Sekundärnutzung und daher ein Verstoss gegen das Zweckbindungsgebot darstellen oder es wird zumindest nicht mit hinreichender Gewissheit ausgeschlossen werden können, dass dies nicht der Fall ist.

iii.) Persönlichkeitsverletzung durch Bekanntgabe von Gesundheitsdaten

Eine Persönlichkeitsverletzung durch die Nutzung von Gesundheitsdaten kann sich nicht nur aus dem Verstoss gegen einen Datenbearbeitungsgrundsatz ergeben. Vielmehr statuiert das DSG explizit, dass die Bekanntgabe von besonders schützenswerten Daten an Dritte eine Persönlichkeitsverletzung darstellt.[199] Anders als für "gewöhnliche" Bearbeitungen von besonders schützenswerten Daten gilt für die Bekanntgabe somit ein grundsätzliches Verbot mit Erlaubnisvorbehalt.[200] Sollen bei einer Nutzung von personenbezogenen Gesundheitsdaten demnach auch Dritte Zugang zu den Daten erhalten[201], ist dies deshalb nur gestützt auf einen Rechtfertigungsgrund, z.B. eine Einwilligung der betroffenen Personen, zulässig. Ein solcher Bedarf nach einer Rechtfertigung ist nicht nur im Falle der Übermittlung an einen ausgewählten Dritten, sondern auch dann gegeben, wenn Gesundheitsdaten veröffentlicht werden sollten.[202]

Wie bereits angesprochen gilt aber bspw. ein Auftragsbearbeiter im Sinne des Art. 9 nDSG bei Einhaltung der entsprechenden Voraussetzungen nicht als Dritter.[203] In diesem Fall führt die Zugänglichmachung der Daten somit nicht zu einer rechtfertigungsbedürftigen Bekanntgabe. Unter welchen Voraussetzungen aber dieses sog. Bekanntgabeprivileg für die Auftragsbearbeitung konkret gilt, ist wiederum nicht restlos klar. So wird bspw. bereits dann wieder ein Rechtfertigungsgrund erforderlich sein, wenn der Auftragsbearbeiter die Daten auch zu eigenen Zwecken nutzt.[204] Gleiches gilt ferner auch dann, wenn nicht einem Auftragsbearbeiter, sondern einem anderen (gemeinsam oder Allein-)Verantwortlichen Zugang zu den Gesundheitsdaten gewährt wird. Dies ist somit verboten, sofern es sich nicht um pseudonymisierte oder anonymisierte Daten handelt oder ein Rechtfertigungsgrund vorliegt.

iv.) Rechtfertigung durch Forschungsausnahme

---

199 Art. 30 Abs. 2 lit. c nDSG.

200 A.A. zum bisherigen Recht wohl einzig WERMELINGER, in: BAERISWYL BRUNO/PÄRLI KURT (Hrsg.), Datenschutzgesetz (DSG), 2015, Art. 12 N 8.

201 Dies stellt, wie erläutert, bereits eine Bekanntgabe dar, vgl. Art. 5 lit. e nDSG.

202 Vgl. dazu ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 12 Rz. 47.

203 Vgl. dazu ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 12 Rz. 45.

204 Vgl. ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 12 Rz. 45.

In den vorangehenden Abschnitten wurden Konstellationen beschrieben, die von Gesetzes wegen als persönlichkeitsverletzende Datenbearbeitung gelten. Hierzu gehört namentlich der Verstoss gegen einen Datenbearbeitungsgrundsatz. Anders als für Bundesorgane[205] und in der EU[206] stellt ein solcher Verstoss für sich allein im Schweizer Recht allerdings noch keine Datenschutzverletzung dar. Vielmehr kann dieser, wie andere persönlichkeitsverletzende Datenbearbeitungen, unter bestimmten Voraussetzungen gerechtfertigt werden. Das Gesetz beinhaltet hierfür eine Liste von Rechtfertigungsgründen. Hierzu gehört auch das sog. Forschungsprivileg in Art. 31 Abs. 2 lit. e nDSG. Bevor auf die Einzelheiten dieser Sonderregelung eingegangen wird, gilt es jedoch, wie bei allen beispielhaften Rechtfertigungsgründen, zu beachten, dass selbst bei Vorliegen der Voraussetzungen des Forschungsprivilegs nicht automatisch eine Rechtfertigung gegeben ist. Vielmehr bringt das Gesetz bereits im Wortlaut zum Ausdruck, dass in diesem Fall eine Rechtfertigung nur "in Betracht fällt". Darüber hinaus darf nach der Rechtsprechung des Bundesgerichts eine Rechtfertigung von Verletzungen der Datenbearbeitungsgrundsätze nur mit Zurückhaltung angenommen werden.[207] Zudem ist hier, wie erläutert, im Falle von Gesundheitsdaten als besonders schützenswerten Daten, ein strenger Massstab anzusetzen.

Diese Ausgangslage verdeutlicht, dass die Berufung auf das Forschungsprivileg eine mit vielen Unsicherheiten behaftete Beurteilung sämtlicher Umstände des Einzelfalls erfordert. Konkret geht es um die Beurteilung der folgenden Einzelvoraussetzungen. Erstens ist erforderlich, dass es sich um eine Bearbeitung zu einem "nicht personenbezogenen Zweck" handelt. Was darunter konkret verstanden werden muss, ist nicht immer leicht zu beantworten. Aus der Botschaft zum noch geltenden DSG, in dem schon dieselbe Formulierung gewählt wurde, geht hervor, dass darunter Fälle zu verstehen sind, in denen zwar Personendaten bearbeitet werden, der Zweck des Bearbeitens aber in keinem Zusammenhang mit den betroffenen Personen steht.[208] Folglich darf die Bestimmung der Identität der betroffenen Person, deren Personendaten bearbeitet werden, für die Bearbeitung keine Rolle spielen.[209] Der Zweck der Bearbeitung steht insbesondere, aber nicht nur,[210] in keinem Zusammenhang mit der betroffenen Person, wenn dieser auch mit pseudonymisierten oder anonymisierten Daten erreicht werden könnte.[211]

Unter den Rechtfertigungstatbestand des Art. 31 Abs. 2 lit. c nDSG können bspw. Bearbeitungsvorgänge fallen, bei denen nicht das Individuum, sondern die Eigenschaften der untersuchten Gesamtheit von Interesse sind.[212] Anwendungsfälle hierfür sind insbesondere Forschungstätigkeiten, Statistiken bzw. Verkehrs-, Bevölkerungs- oder sonstige Planungsstatistiken.[213] In der sozialwissenschaftlichen Forschung könnten bspw.

---

205 Vgl. hierzu nachfolgend Abschnitt 4.1.4b).

206 Vgl. jedoch die Besonderheiten bei der Anwendung des Zweckbindungsgebots im Zusammenhang mit der Forschung, Art. 5 Abs. 1 lit. B i.V.m. Art. 89 DSGVO.

207 BGE 138 II 346, E. 7.2; BGE 136 II 508, E. 5.2.4.

208 Botschaft zum DSG, BBl 1988 S. 483.

209 Koç, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, 2015, Rz. 30.10.

210 Dies ergibt sich aus der Anforderung in Art. 31 Abs. 2 lit. e Ziff. 1 nDSG, die andernfalls wenig Sinn ergeben würde.

211 Koç, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, 2015, Rz. 30.10.; ähnlich Rampini, in: Maurer-Lambrou/Blechta (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 13 N 42.

212 Rampini, in: Maurer-Lambrou/Blechta (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 13 DSG Rz.42.

213 Rampini, in: Maurer-Lambrou/Blechta (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 13 DSG Rz.42.

Fälle denkbar sein, in denen es nicht auf die Identität des einzelnen Betroffenen ankommt, sondern aus einer grossen Menge von Daten verallgemeinerbare Aussagen über eine gesamtgesellschaftliche Fragestellung abgeleitet werden sollen.

Handelt es sich bei einer Bearbeitung von Personendaten um eine solche zu einem nicht personenbezogenen Zweck, müssen gemäss Art. 31 Abs 2 lit e nDSG zusätzlich folgende Voraussetzungen erfüllt sein, damit die Rechtfertigung gestützt auf das Forschungsprivileg in Frage kommt:

1. Der Verantwortliche anonymisiert die Daten, sobald der Bearbeitungszweck es erlaubt, oder er trifft angemessene Massnahmen, damit die Bestimmbarkeit der betroffenen Personen verhindert werden kann, wenn eine Anonymisierung unmöglich ist oder einen unverhältnismässigen Aufwand erfordert.

2. Besonders schützenswerte Personendaten werden Dritten nur so bekanntgegeben, dass die betroffenen Personen nicht bestimmbar sind. Wenn dies nicht möglich ist, muss mittels Massnahmen gewährleistet werden, dass Dritte die Daten nur zu nicht personenbezogenen Zwecken bearbeiten.

3. Die Ergebnisse werden so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind.

Dass die Einhaltung dieser Anforderungen in der Praxis nicht immer leicht und mit erheblichen Unsicherheiten verbunden ist, wurde bereits bei der Erläuterung zur Anonymisierung und Pseudonymisierung verdeutlicht.[214] Hinzu kommt zum einen die zeitliche Unbestimmtheit in der ersten Voraussetzung, die eine Anonymisierung dann verlangt, sobald der Bearbeitungszweck dies erlaubt. Dies engt die praktische Handhabung ein und führt in der Praxis zu Schwierigkeiten, gerade wenn bereits bei Beginn des Projekts festgelegt werden muss, wann dieser Zweck erreicht ist.[215] Darüber hinaus sorgen die verwendeten Begrifflichkeiten zusätzlich für Unsicherheit, indem" bestimmbar" vermeintlich eine andere Bedeutung zugeschrieben wird als der Gegensatz zu "anonymisiert". So bleibt offen, wie die Bestimmbarkeit anders als durch die Anonymisierung verhindert werden kann, also ob die Pseudonymisierung genügen kann. Auch aus diesen Gründen ist bei der Berufung auf die Forschungsausnahme Vorsicht geboten.

Im Zusammenhang mit der medizinischen Forschung stellt sich ferner auch die Frage nach dem Verhältnis der Forschungsausnahme zum HFG und ob es überhaupt Fälle im Bereich der Humanforschung gibt, in denen die Forschungsausnahme Anwendung findet. Weiter unten wird näher auf das Verhältnis zwischen HFG und DSG eingegangen,[216] jedoch kann an dieser Stelle zusammenfassend gesagt werden, dass das HFG für die Bereiche, die es abschliessend regelt, als Spezialgesetz Anwendungsvorrang gegenüber dem DSG (bzw. den kantonalen Datenschutzgesetzen) hat. Inwieweit das HFG sämtliche Bearbeitungsgrundsätze vollumfänglich verdrängt und die Rechtmässigkeit der Datenbearbeitung abschliessend regelt, ist nicht restlos geklärt. Wird dies verneint, kann die Forschungsausnahme als Rechtfertigung von persönlichkeitsverletzenden Bearbeitungen dienen. Wird dies hingegen bejaht, so wäre die Forschungsausnahme für Humanforschungsprojekte im Anwendungsbereich des HFG kaum relevant. Es wird wohl nur wenige Fälle geben, in denen ein Humanforschungsprojekt nicht in den Anwendungsbereich des HFG fällt und dennoch von der Forschungsausnahme umfasst ist. Sowohl das HFG als auch die Forschungsausnahme setzen voraus, dass Forschung betrieben wird, folglich eine methodengeleitete Suche nach verallgemeinerbaren Erkenntnissen

[214] Vgl. oben Abschnitte 3.1.2, 3.2.6 und 3.2.7.

[215] Vgl. KOÇ, in: PASSADELIS/ROSENTHAL/THÜR (Hrsg.), Datenschutzrecht, 2015, Rz. 30.23.

[216] Vgl. nachfolgend Abschnitt 4.2.2.

stattfindet.[217] Darüber hinaus wird es nur wenige Humanforschungsprojekte geben, die nicht zumindest gesundheitsbezogene Daten (oder biologisches Material) bearbeiten (bei anonymisierten Daten sind sowohl das HFG als auch das DSG nicht anwendbar).[218] Schliesslich wird sich ein Grossteil der Humanforschungsprojekte mit der Erforschung von Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers beschäftigen.[219] Sind die genannten Voraussetzungen erfüllt, ist das HFG anwendbar, in allen anderen Fällen ist im Einzelfall zu prüfen, ob die Forschungsausnahme eine geeignete Rechtfertigung darstellt.

Statistische Auswertungen bzw. Planungstätigkeiten anhand von Gesundheitsdaten sind demgegenüber nicht vom Anwendungsbereich des HFG umfasst und können – unter den Voraussetzungen, dass alle gesetzlichen Bedingungen erfüllt sind – sehr wohl unter dem Forschungsprivileg i.S.d. Art. 31 Abs. 2 lit. e nDSG gerechtfertigt sein. Neben den Unsicherheiten bei der Einhaltung der Voraussetzungen in Bezug auf die Anonymisierung bestehen aber auch hier ungeklärte Fragen, was konkret unter statistischen Auswertungen und Planungstätigkeiten verstanden werden kann.

Die Forschungsausnahme könnte somit, zumindest ausserhalb des HFG, als wichtige Grundlage dienen, um Sekundärnutzungen im Gesundheitssektor abzusichern. Als solche Absicherung taugt sie jedoch nur bedingt, kann sie doch nur zurückhaltend angerufen werden und selbst dann nur unter Einhaltung von Anonymisierungsvorgaben, die faktisch schwer umsetzbar sind.

v.) Rechtfertigung durch Einwilligung

Die Unsicherheiten mit dem Forschungsprivileg und auch der Berufung auf anderweitige überwiegende Interessen im Sinne des DSG rufen vielfach den Bedarf nach Alternativen oder mindestens zusätzlichen Absicherungen hervor. Eine dieser Alternativen stellt die Einwilligung der betroffenen Person dar, die ebenfalls explizit als möglicher Rechtfertigungsgrund für die bspw. aus dem Verstoss gegen das Zweckbindungsgebot resultierende Persönlichkeitsverletzung genannt wird.[220]

Das DSG enthält auch die Voraussetzungen für die Gültigkeit der Einwilligung.[221] Zentrale Anforderung ist die hinreichende Information, die der Einwilligung zugrunde liegen muss. Hierzu gehört unter anderem die Information über den Zweck der Bearbeitung, wobei für die Einwilligung im Grundsatz dieselben Anforderungen gelten, wie für die Information im Sinne der Bearbeitungsgrundsätze. Dies bedeutet, dass es für eine gültige Einwilligungserklärung in die Sekundärnutzung von Gesundheitsdaten ausreichen kann, wenn nur Kategorien der (Co-)Verantwortlichen bei der Beschaffung und nicht deren Identität angegeben wird.[222] Eine Einwilligung in künftige Nutzungen würde deshalb zumindest nach dieser Lehrmeinung noch nicht daran scheitern, dass zum Zeitpunkt der Datenbeschaffung die Identitäten aller an einem Datennutzungsprojekt beteiligten Co-Verantwortlichen noch gar nicht bekannt sind. Allerdings setzt eine wirksame Einwilligung

[217] Art. 3 lit. a HFG.

[218] Art. 2 Abs. 1 HFG.

[219] Art. 2 Abs. 1 HFG.

[220] Art. 31 Abs. 1 nDSG.

[221] Art. 6 Abs. 6 nDSG.

[222] Vgl. BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 88.

auch nach Ansicht der Autoren zumindest voraus, dass die Kategorien der Verantwortlichen hinreichend bestimmt umschrieben und nicht überraschend bzw. ungewöhnlich zusammengesetzt sind.[223] Diese Anforderung wird in der Praxis nicht immer leicht zu erfüllen sein und führt zu Unsicherheiten.

Darüber hinaus werden auch bei der Einwilligung dieselben strengen Anforderungen an die Bestimmtheit des Zwecks gestellt, wie sie bereits unter dem Zweckbindungsgebot erläutert wurden.[224] Ungenügend ist demnach auch unter dem Gesichtspunkt der Informiertheit der Einwilligung, wenn bspw. bloss von einer Einwilligung in die Verwendung zu "statistischen Zwecken" gesprochen wird. Dies gilt umso mehr, wenn, wie hier, Gesundheitsdaten betroffen sind und deshalb ein zusätzlich strenger Massstab anzusetzen ist. Folglich hilft auch die Einwilligung im Sinne des DSG nicht weiter, wenn im Zeitpunkt der Datenbeschaffung die Angaben künftiger Bearbeitungsvorhaben noch nicht hinreichend konkret vorliegen und der betroffenen Person auch gar noch nicht mitgeteilt werden können. Es wird sich in den hier interessierenden Konstellationen deshalb vielfach so verhalten, dass entweder bereits hinreichend informiert werden kann, also die Nutzung zu diesen Zwecken gar nicht erst eine Sekundärnutzung mit Zweckänderung darstellt und keine Einwilligung zwingend ist, oder, weil noch nicht genügend Informationen bekannt sind und von vornherein keine gültige Einwilligung eingeholt werden kann. Letzteres gilt unter dem DSG deshalb, weil ein "Generalkonsent", also eine Einwilligung in einen sehr breit und unspezifisch umschriebenen Zweck, anders als unter gewissen Voraussetzungen im HFG, nicht gestattet ist.

Darüber hinaus gilt es auch zu beachten, dass Einwilligungen nur gültig sind, wenn sie freiwillig erteilt wurden. Die Einzelheiten sind umstritten, auch wenn insgesamt von einem liberalen Massstab ausgegangen werden kann. Insbesondere dürfte es bis zu einem gewissen Grad auch zulässig sein, einen Vertragsabschluss an die Erteilung einer Einwilligung in die Datennutzung zu koppeln.[225] Etwas anderes gilt aber für die Leistungen von Unternehmen und Organisationen, von welchen die betroffenen Personen abhängig sind, also die Nichterteilung der Einwilligung und damit der daraus folgende Verzicht auf die Leistung unzumutbar wäre. Im Bereich der privaten Verantwortlichen ist dabei bspw. an die Betreiber von sozialen Netzwerken zu denken. Wird die Bereitstellung einer Plattform für die Nutzer an die Einwilligung in die Verwendung von Gesundheitsdaten gekoppelt, also keine Möglichkeit zur Plattformnutzung ohne Erteilung der Einwilligung geboten, ist wohl in Bezug auf denjenigen Teil des Zielpublikums, für den eine Abhängigkeit von der Plattform bejaht wird, die Freiwilligkeit zu verneinen und damit ist die Einwilligung ungültig.[226] Schliesslich sind im Umgang mit Gesundheitsdaten auch Szenarien denkbar, in welchen es an der Freiwilligkeit fehlen dürfte, bspw. wenn die besondere Situation von Personen mit einer schweren Krankheit zur Erteilung von Einwilligungen ausgenutzt wird. In der Schweiz wurde bislang allerdings soweit ersichtlich noch nicht ein übermässig strenger Standpunkt vertreten, wie in der EU im Kontext von klinischen Studien, wonach ein der Freiwilligkeit abträgliches Ungleichgewicht der Macht bereits vorliegt, wenn eine betroffene Person nicht in gutem Gesundheitszustand sei.[227]

---

223 Vgl. zum DSG Bühlmann/Schüepp, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, Rz. 85 ff.

224 Vgl. dazu oben Abschnitt 4.1.4a) ii.); ferner ausführlich: Bühlmann/Schüepp, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 49 ff., 69 ff.

225 Vgl. dazu ausführlich Bühlmann/Schüepp, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, Rz. 29 ff.

226 Vgl. Bühlmann/Schüepp, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, Rz. 29 ff.

227 EDSA, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO) (Artikel 70 Absatz 1 Buchstabe b), 23.1.2019, Rz. 20.

Auch wenn die Einwilligung somit ein wertvolles Mittel zur Absicherung für die Nutzung von Gesundheitsdaten darstellen kann, bestehen neben praktischen Unwägbarkeiten auch zahlreiche und mitunter hohe rechtliche Anforderungen. Die Beurteilung in der Praxis, inwieweit diese Anforderungen eingehalten wurden, ist ebenfalls mit Unsicherheiten verbunden.

vi.) Zwischenfazit: Hindernisse in den DSG-Vorschriften für private Verantwortliche

Bei der Sekundärnutzung von Gesundheitsdaten könnten die im Vergleich zu Bundesorganen weniger strengen Vorschriften für private Verantwortliche vielversprechend sein. Für private Verantwortliche, die im Gesundheitssektor tätig sind, ist jedoch zunächst zu klären, ob sie nicht in Erfüllung einer öffentlichen Aufgabe tätig sind und deshalb für die damit verbundenen Datenbearbeitungen den strengeren Vorschriften für Bundesorgane unterstehen.

Weiter stellen sich gewisse Schwierigkeiten in Bezug auf die Einhaltung der Datenbearbeitungsgrundsätze für private Verantwortliche in weniger ausgeprägter Form als bei Bundesorganen. Denn bei privaten Verantwortlichen können Verstösse gegen diese Grundsätze gerechtfertigt werden, wenn ein Rechtfertigungsgrund vorliegt. Die Rechtfertigungsgründe sind jedoch ihrerseits so ausgestaltet, dass sie nur beschränkt als Absicherung verwendbar sind. Dies gilt vorab für das Forschungsprivileg. Denn nach der Rechtsprechung darf bei einer Verletzung der Datenbearbeitungsgrundsätze ein Rechtfertigungsgrund und damit auch das Forschungsprivileg nur mit Zurückhaltung bejaht werden. Für die Beurteilung, ob eine Sekundärnutzung zulässig ist, ist deshalb eine Einzelfallprüfung vorzunehmen. Hinzu kommen die Ungewissheiten bei der Umsetzung der besonderen Voraussetzungen des Forschungsprivilegs, namentlich das Anonymisierungserfordernis.

Als zusätzliche Absicherung kann zwar eine Einwilligung dienen, jedoch sind auch hier, gerade bei Gesundheitsdaten, hohe rechtliche Anforderungen einzuhalten. Ferner kann die Einholung einer gültigen Einwilligung für eine Sekundärnutzung auch daran scheitern, dass, anders als im HFG, eine spezifische Beschreibung der Bearbeitungszwecke verlangt wird, ein Generalkonsent also von vornherein nicht zulässig ist. Mit Blick auf zukünftige Sekundärnutzungen werden nicht selten nicht hinreichend detaillierte Informationen vorliegen, um die betroffenen Personen in der gebotenen Tiefe aufzuklären.

b) Kernanforderungen für Bundesorgane

Nachfolgend werden die Kernanforderungen des DSG für Bundesorgane im Bereich der Sekundärnutzung dargestellt. Diese stimmen zu einem wesentlichen Teil mit denjenigen für private Verantwortliche überein. Allerdings gelten im Ergebnis strengere Vorgaben, weshalb es für die Zulässigkeit einer Sekundärnutzung von Gesundheitsdaten entscheidend sein kann, welche der Vorschriften im Einzelfall zur Anwendung gelangen. Es wurde bereits dargelegt, dass auch private Verantwortliche für Tätigkeiten, bei welchen sie öffentliche Aufgaben des Bundes erfüllen, als Bundesorgan gelten und damit für die damit verbundenen Datenbearbeitungen den strengeren Vorschriften unterstellt sind. Es ist daher stets sorgfältig zu prüfen, welche der Vorgaben für die einzelne Datenbearbeitung zur Anwendung gelangen.

i.) Rechtmässigkeitsgrundsatz

Im ersten Abschnitt des DSG sind Vorschriften vorgesehen, die sowohl für Private als auch für Bundesorgane gelten.[228] Darin enthalten sind mitunter auch die Datenbearbeitungsgrundsätze, wozu auch der Rechtmässigkeitsgrundsatz gilt.[229] Auch für die Zulässigkeit der Sekundärnutzung von Gesundheitsdaten durch Bundesorgane ist dieser von grundlegender Bedeutung. Danach wird festgelegt, dass die Datenbearbeitung im Einklang mit den rechtlichen Vorschriften zum Schutz der Persönlichkeit erfolgen muss. Wie erläutert folgt aus dem Rechtmässigkeitsgrundsatz die für die Sekundärnutzung von Personendaten zentrale Konsequenz, dass jegliche Weiterbearbeitung von Personendaten, die rechtswidrig erhoben wurden, grundsätzlich ebenfalls rechtswidrig ist.[230] Wurde bei der Erhebung gegen Vorschriften zum Schutz der Persönlichkeit verstossen, liegt ein Verstoss gegen den Rechtmässigkeitsgrundsatz vor, welcher Bundesorgane, anders als private Verantwortliche, nicht durch einen besonderen Erlaubnistatbestand rechtfertigen können.

Für die Praxis hat der Grundsatz zur Folge, dass bei der Sekundärnutzung, die vielfach erst einige Zeit später als die ursprüngliche Beschaffung der Daten erfolgt, noch sichergestellt und verifizierbar sein muss, dass die damalige Beschaffung rechtmässig erfolgt war. Andernfalls besteht das Risiko eines Verstosses gegen den Rechtmässigkeitsgrundsatz und die Sekundärnutzung ist verboten. Auch bei Verwaltungseinheiten und anderen Bundesorganen zeigt die Erfahrung, dass die entsprechende Dokumentation vielfach ungenügend ist und daher eine Unsicherheit besteht. Anders als bei dem im nachfolgenden Abschnitt erläuterten Zweckbindungsgrundsatz kann eine Verletzung des Rechtmässigkeitsgrundsatzes schliesslich auch nicht durch die Einhaltung sämtlicher ungewisser Voraussetzungen der Forschungsausnahme geheilt werden.[231]

ii.) Zweckbindungsgebot

Neben dem Rechtmässigkeitsgrundsatz zählt auch das bereits erläuterte Zweckbindungsgebot[232] zu den allgemeinen Datenbearbeitungsgrundsätzen. Dieses ist für die Sekundärnutzung von Gesundheitsdaten durch Bundesorgane, wie bspw. die Bundesämter (BAG etc.), ebenfalls von zentraler Bedeutung. Die sich daraus ergebenden Anforderungen an die Sekundärnutzung stimmen im Wesentlichen mit denjenigen überein, die für private Verantwortliche gelten. Es kann deshalb auf die entsprechenden Erläuterungen vorstehend in Abschnitt 4.1.4. a) ii.) verwiesen werden.

Im Unterschied zur Bearbeitung durch Private wird sich der Zweck einer Bearbeitung bei Bundesorganen aber faktisch sehr häufig, aber nicht ausschliesslich, aus den jeweiligen Spezialgesetzen ergeben. So gilt auch für Bundesorgane, dass es genügen kann, wenn der Zweck erkennbar ist, wobei nur solche Zwecke "als erkennbar" in Frage kommen dürften, die mit der öffentlichen Aufgabe des Bundesorgans zusammenhängen.[233] Es wird jedenfalls häufig auch nicht eine eigenständige Festlegung bzw. Ausformulierung der

---

228 Art. 5 ff. nDSG.

229 Art. 6 Abs. 1 nDSG.

230 Vgl. EPINEY, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 9 N 12; BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 134.

231 Vgl. Art. 39 Abs. 2 nDSG e contrario.

232 Art. 6 Abs. 3 nDSG.

233 Im Ergebnis wohl ebenso: BAERISWYL, in: BAERISWYL/PÄRLI (Hrsg.), SHK-DSG, 2015, Art. 4 N 40: "Für Bundesorgane ist der Zweck der Datenbearbeitung regelmässig aus der gesetzlichen Grundlage zu entnehmen (Legalitätsprinzip). Das Bundesorgan kann Daten bearbeiten, soweit die Datenbearbeitung in Zusammenhang mit seiner Aufgabenkompetenz steht und gesetzlich vorgesehen ist (Art. 17 DSG)."

Zwecke durch das Bundesorgan erfolgen und die Interpretation der Reichweite des Zwecks somit auch nicht durchwegs nach den gleichen Grundsätzen vorgenommen werden können. Im Ergebnis kann dies darauf hinauslaufen, dass die Erfüllung des Teilaspekts der Zweckbestimmung Bundesorganen vielfach leichter fallen wird als privaten Verantwortlichen, welche ihre Zwecke in der Regel, mangels Vorliegens einer Gesetzesgrundlage, festlegen und ausformulieren werden müssen.[234] Umso mehr wird bei Bundesorganen aber ein strenger Massstab bei den Anforderungen aus dem zweiten Teilgehalt, der Zweckbindung, anzusetzen sein.

Ein zentraler Unterschied gegenüber privaten Verantwortlichen besteht jedoch darin, dass Bundesorgane Verstösse gegen die Bearbeitungsgrundsätze nicht "rechtfertigen" können. Die Bearbeitungsgrundsätze wie das Zweckbindungsgebot gelten deshalb im Grundsatz jeweils zusätzlich zu den übrigen Anforderungen an eine Datenbearbeitung, wie z.B. dem nachfolgend erläuterten Legalitätsprinzip.[235] Von diesem Grundsatz gilt jedoch, wie im nächsten Abschnitt dargelegt, gerade im Bereich der Forschung eine Ausnahme ("Forschungsprivileg"), wonach die Anforderungen des Zweckbindungsgebots unter bestimmten Voraussetzungen missachtet werden können.

iii.) Legalitätsprinzip

(a) Allgemeines zum Legalitätsprinzip

Die dritte zentrale Kernfanforderung für die Datenbearbeitung durch Bundesorgane besteht im datenschutzrechtlichen Legalitätsprinzip. Unter dem künftigen Recht ist dessen Kern in Artikel 34 nDSG enthalten. Dieses gilt für sämtliche Bearbeitungsformen,[236] wobei für gewisse Datenbearbeitungen Sondervorschriften bestehen. Artikel 34 Absatz 1 übernimmt dabei den Grundsatz von Art. 17 Abs. 1 DSG, wonach Bundesorgane Personendaten nur bearbeiten dürfen, wenn hierfür eine gesetzliche Grundlage oder eine Ausnahme davon vorliegt. Mit der Regelung wird das in Art. 5 BV verankerte Gesetzmässigkeits- oder Legalitätsprinzip konkretisiert, welches für jegliches Verwaltungshandeln gilt.[237]

Für Bundesorgane gilt somit, ähnlich wie generell für alle Verantwortlichen unter der EU-DSGVO, gewissermassen ein Verbot mit Erlaubnisvorbehalt.[238] Die Rede ist auch vom Prinzip der Spezialermächtigung, das für Bundesorgane, anders als für private Bearbeiter, im DSG gilt.[239] Das DSG ist insofern als Rahmengesetz zu verstehen, welches das Legalitätsprinzip datenschutzrechtlich konkretisiert und im Grundsatz eine gesonderte Ermächtigung in einem anderen Erlass verlangt. Das heisst, jede Datenbearbeitung durch Bundesorgane muss sich grundsätzlich auf eine bereichsspezifische bzw. spezialgesetzliche Rechtsgrundlage stützen können. Neben den eigentlichen Ausnahmen vom datenschutzrechtlichen Legalitätsprinzip[240] als solchem kann aber bereits das DSG in einigen ausgewählten Fällen direkt die erforderliche "besondere" Grundlage

---

234 Vgl. zur Ausnahme für private bei gesetzlich vorgeschriebenen Bearbeitungen, BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 65.

235 Vgl. ähnlich auch WALDMANN/BICKEL, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 12 N 5.

236 Vgl. CLAUDIA MUND, in: BAERISWYL/PÄRLI (Hrsg.), SHK-DSG, 2015, Art. 17 N 4.

237 Vgl. nur ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 17 N 3.

238 Vgl. z.B. DOMINIKA BLONSKI, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, Diss. Bern 2015, S. 77.

239 ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 17 N 4.

240 Art. 34 Abs. 3 und 4 nDSG sowie Art. 36 Abs. 2 und 3 nDSG.

bereitstellen. In diesen Konstellationen bedarf es somit ausnahmsweise keiner Spezialermächtigung in einem anderen Erlass.[241]

(b) Forschungsprivileg als besondere Grundlage

Einer dieser für die vorliegende Fragestellung wichtigen Fälle ist die Datenbearbeitung für nicht personenbezogene Zwecke in Art. 39 nDSG. Es gilt hier im Wesentlichen dasselbe, wie im Zusammenhang mit den Anforderungen des DSG für Private in Abschnitt 4.1.4 a) iv.) ausgeführt wurde. So greift die Sonderregelung von vornherein nur dann, wenn der Zweck der Bearbeitung nicht personenbezogen ist. Der Gesetzgeber geht davon aus, dass dies namentlich bei der Forschung, Planung und Statistik der Fall sein kann, weshalb diese Anforderung auch hier insbesondere, aber nicht nur,[242] dann gegeben ist, wenn der Zweck der Bearbeitung auch mit pseudonymisierten oder anonymisierten Daten erreicht werden könnte.[243] Sodann ist nicht gänzlich ausgeschlossen, dass auch Bundesorgane im Bereich der Humanforschung öffentlich-rechtlich tätig sein könnten, sodass sich die Frage nach dem Verhältnis zum HFG stellen würde, also ob das HFG die Vorschriften des DSG verdrängt oder eben nicht. Ist dies nicht vollumfänglich der Fall, könnte das Forschungsprivileg für Bundesorgane zumindest herangezogen werden, um eine Missachtung des Zweckbindungsgebots zu legitimieren.

Ferner gelten auch hier zusätzliche strenge Anforderungen, die erfüllt sein müssen, damit die Ausnahmeregelung greift. Auch hier gilt sie nur, wenn:

a) die Daten anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt;

b) das Bundesorgan privaten Personen besonders schützenswerte Personendaten nur so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind;

c) die Empfängerin oder der Empfänger Dritten die Daten nur mit der Zustimmung des Bundesorgans weitergibt, das die Daten bekanntgegeben hat; und

d) die Ergebnisse nur so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

Die einzelnen Voraussetzungen entsprechen im Wesentlichen denjenigen für Private,[244] sind aber strenger und die dritte Anforderung gilt für Bundesorgane zusätzlich. Bei dieser Regelung bestehen die Unklarheiten zumindest in Bezug auf das Verständnis des Anonymisierungsbegriffs nicht in gleichem Ausmass. Die zeitliche Unbestimmtheit, wann konkret die Anonymisierung erforderlich ist, wird auch hier nicht aufgelöst. Sodann gelten die allgemeinen Unsicherheiten in Bezug auf die Anonymisierung allerdings auch hier. Somit sind auch Bundesorgane gut beraten, von der Ausnahme nur mit Vorsicht Gebrauch zu machen. Angesichts der offenen Punkte kann daher nicht darauf vertraut werden, dass die mit der Ausnahmeregelung vorgesehenen Lockerungen[245] in Bezug auf die gesetzliche Grundlage sowie das Zweckbindungsgebot tatsächlich greifen. Eine Sekundärnutzung von Gesundheitsdaten, die auf keine andere Rechtsgrundlage abgestützt werden kann oder einen Verstoss gegen das Zweckbindungsgebot darstellt, ist daher für Bundesorgane

---

241 Vgl. dazu z.B. auch MICHAEL MONTAVON, Cyberadministration et protection des données, Diss. Freiburg, 2021, S. 219 f.

242 Dies ergibt sich aus der Anforderung in Art. 39 Abs. 1 lit. a nDSG, die andernfalls wenig Sinn ergeben würde.

243 KOÇ, in: PASSADELIS/ROSENTHAL/THÜR (Hrsg.), Datenschutzrecht, Basel 2015, Rz. 30.10.

244 Siehe dazu Abschnitt 4.1.4a) iv.)

245 Vgl. Art. 39 Abs 2 nDSG.

gleichwohl riskant. Ferner entbindet die Forschungsausnahme auch nicht von der Einhaltung des Transparenzgebots, also der Information der betroffenen Personen,[246] sowie des Rechtmässigkeitsgrundsatzes, also insbesondere von der Sicherstellung, dass die unter Umständen von Dritten erhobenen Daten rechtmässig beschafft und übermittelt wurden.

(c) Anforderungen an gesetzliche Grundlagen für die Sekundärnutzung

Ausserhalb dieser besonderen Ausnahmeregelung ist den Bundesorganen jegliche Bearbeitung von Personendaten nur erlaubt, wenn eine gesetzliche Grundlage dies erlaubt. Für besonders schützenswerte Daten, wie namentlich auch für ein Profiling, gilt dabei die erhöhte Anforderung, dass die Ermächtigung in einem Gesetz im formellen Sinne enthalten sein muss, während für alle anderen Verarbeitungen eine Grundlage in einem Gesetz im materiellen Sinne genügen kann.[247] Mit Gesetz im formellen Sinne ist ein Gesetz gemeint, das im ordentlichen Gesetzgebungsverfahren ergeht.[248] Eine Grundlage in einem Gesetz im materiellen Sinne, d.h. eine (Rechts-)Verordnung des Bundesrates, genügt demgegenüber nicht.[249] Bei der Beurteilung, ob die Nutzung von Gesundheitsdaten erlaubt ist, hat das Bundesorgan deshalb Erlasse auf Gesetzesstufe zu suchen, die eine Erlaubnis dafür enthalten.
Bei der Beurteilung, ob eine (Gesetzes-)Norm als Erlaubnis genügt, ist zudem die Anforderung der hinreichenden Bestimmtheit zu beachten. Als Mindestanforderung gilt dabei folgender Inhalt: der Zweck, die beteiligten Organe und das Ausmass der Datenbearbeitung. [250] Allerdings werden teilweise auch höhere Anforderungen gestellt[251] und der datenschutzrechtliche Verhältnismässigkeitsmassstab gilt auch hier:[252] Je sensibler die zu verarbeitenden Daten und je einschneidender die Datenbearbeitung, desto höhere Anforderungen sind an die Bestimmtheit der Norm zu stellen.[253] Mangels gefestigter Rechtsprechung sind jedoch die konkreten Anforderungen unklar. Einigkeit dürfte letztlich zumindest dahingehend bestehen, dass Blankettnormen ohne eine Anbindung der Bearbeitung an einen bestimmten Zweck ungenügend wären.[254] Wie der Gesetzgeber allerdings selbst durch die Ausgestaltung der verschiedenen Ermächtigungsgrundlagen zum Ausdruck bringt, gilt hier ein wesentlich weniger restriktives Verständnis von Bearbeitungszweck und dies auch in Bezug auf besonders schützenswerten Daten. So hat er namentlich in den Sozialversicherungsgesetzen

---

246 Vgl. hierzu auch EDÖB, Datenschutz und Forschung im Allgemeinen: www.edoeb.admin.ch/edoeb/de/home/datenschutz/statistik--register-und-forschung/forschung/datenschutz-und-forschung-im-allgemeinen.html (zuletzt aufgerufen am: 23.5.2022).

247 Vgl. Art. 34 Abs. 2 (und Abs. 3 e contrario) nDSG.

248 PIERRE TSCHANNEN/ULRICH ZIMMERLI/MARKUS MÜLLER, Allgemeines Verwaltungsrecht, 2014, S. 100, §13 Rz. 1.

249 TSCHANNEN/ ZIMMERLI/ MÜLLER, Allgemeines Verwaltungsrecht, 2014, S. 101, §13 Rz. 7.

250 Botschaft zum DSG 1988, 467.

251 Empfehlung des EDÖB betreffend Drogen- und Alkoholtests bei den Schweizerischen Bundesbahnen (SBB), 25. Mai 2007, E. II Ziff. 5. ("*sowohl den Zweck als auch den Umfang der Datenbearbeitung, die dabei verwendeten Mittel und die zur Bearbeitung befugten Behörden*"); Stellungnahme des EDÖB betreffend Bekanntgabe von Arbeitslosendaten an Betreibungsbehörden, April 1997, VPB 61.72, E. A Ziff. 4 ("*insbesondere den Zweck und den Umfang der Bearbeitung präzisieren, indem z. B. die Kategorien der bearbeiteten, besonders schützenswerten Personendaten bestimmt oder die Zugriffe definiert werden*").

252 Vgl. zum Begriff BÜHLMANN/SCHÜEPP Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 54.

253 Vgl. ferner die weiteren Kriterien in der Botschaft zum DSG 1988 sowie ausführlich dazu ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 17 N 11 ff.

254 Vgl. BEAT RUDIN, Anpassungsbedarf in den Kantonen, digma 2017, S. 58 ff., 61.

jeweils bloss eine allgemeine Bestimmung eingeführt, welche die Rechtsgrundlage für sämtliche Bearbeitungen der Personendaten bildet, die zur Erfüllung der auf dem jeweiligen Gesetz basierenden Aufgaben benötigt werden.[255]

Aus diesen Rechtsvorschriften wird aber auch deutlich, dass eine hinreichende Grundlage für die Bearbeitung von besonders schützenswerten Daten nur vorliegen kann, wenn diese Grundlagen ausdrücklich in einem Gesetz im formellen Sinne genannt werden.[256] Mit anderen Worten müssen sich die Begriffe in der Norm wiederfinden bzw. die Erlaubnis zur Bearbeitung der besonders schützenwerten Daten muss benannt, d.h. ausformuliert sein. Bekräftigt wird dies auch durch die bisherige Ausgestaltung der Spezialermächtigungen in anderen Bereichen, die jeweils Formulierungen enthalten wie "Personendaten, insbesondere auch besonders schützenswerte Daten".[257] Selbst wenn sich der Wortlaut der einschlägigen Vorschrift im DSG[258] künftig ändert, und demnach eine "ausdrückliche" Erwähnung nicht mehr erforderlich wäre, deutet abgesehen vom Gesetzestext Nichts auf eine Änderung der Rechtslage hin. Vielmehr befolgt der Gesetzgeber bei den Ermächtigungen in den einzelnen (künftigen) Gesetzen nach wie vor diesen Ansatz.[259]

In Bezug auf die Anforderungen an die Bearbeitung dieser Daten bleibt es sodann ebenfalls bei der bisherigen Rechtslage. Der Gesetzgeber erachtet es grundsätzlich nicht als erforderlich, auch die Bearbeitung näher zu umschreiben. Es genügt deshalb im Grundsatz eine Gesetzesvorschrift, die einem Bundesorgan erlaubt, besonders schützenswerte Personendaten zu bearbeiten. In einer Vorschrift muss somit in Bezug auf die Sekundärnutzung auch nicht von Weiterverwendung oder etwas ähnlichem die Rede sein. Unter dem Legalitätsprinzip genügt für die Sekundärnutzung auch eine Norm, welche bloss das Bearbeiten von besonders schützenswerten Daten gestattet. Allerdings muss auch bei einer sehr weit gefassten Norm, die eine Bearbeitung zur Erfüllung aller nach einem Gesetz erforderlichen Aufgaben erlaubt, der Zweck der Sekundärnutzung noch als Erfüllung einer gesetzlichen Aufgabe verstanden werden können. Insofern wird bspw. die Nutzung von Daten zur Förderung des Absatzes bestimmter Produkte in aller Regel nicht als gesetzliche Aufgabenerfüllung qualifiziert werden. Unabhängig davon ändert auch eine weite Auslegung des Legalitätsprinzips nichts daran, dass das Zweckbindungsgebot hohe Anforderungen in Bezug auf Zweckänderungen enthält. Denn das Legalitätsprinzip gilt, wie erwähnt, zusätzlich und unabhängig von diesem Bearbeitungsgrundsatz der Zweckbindung.

Besonderheiten gelten jedoch für die speziellen Bearbeitungsformen der Bekanntgabe sowie das Profiling. Diese müssen in der Ermächtigungsgrundlage weiterhin explizit aufgeführt sein. Es muss somit in der Norm ausdrücklich (auch) von einer Bekanntgabe gesprochen werden, die vom Bundesorgan vorgenommen werden darf, und es genügt nicht, wenn (nur) von Bearbeitung oder Vornahme eines Profilings die Rede ist. Verdeutlicht wird dies wiederum durch die im Rahmen der Totalrevision des DSG vorgenommenen Anpassungen in einzelnen Spezialermächtigungen.[260] Soll also im Rahmen einer Sekundärnutzung eine Bekanntgabe

---

255 Botschaft über die Anpassung und Harmonisierung der gesetzlichen Grundlagen für die Bearbeitung von Personendaten in den Sozialversicherungen, BBl 2000 S. 255 ff., 261; die parlamentarischen Debatten führten zu keinen Abweichungen in den hier betreffenden Punkten, vgl. für die Einzelheiten die in der Parlamentsdatenbank unter der Geschäftsnummer 99.093 abrufbaren Dokumente.

256 Vgl. ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 17 N 16.

257 Vgl. z.B. Art. 96 Abs. 1 AsylG, Art. 21 Abs. 3 SpoFöG oder Art. 54 Abs. 2 PBG.

258 Vgl. Art. 17 Abs. 2 DSG ("ausdrücklich vorsieht") im Unterschied zu Art. 34 nDSG.

259 Vgl. die bereits erwähnten Grundlagen in ihrer künftigen Fassung: Art. 96 Abs. 1 AsylG, Art. 21 Abs. 3 SpoFöG oder Art. 54 Abs. 2 PBG, im Unterschied bspw. zu Art. 96 Abs. 1 und 2 nUVG oder Art. 110 Abs. 1 und 2 Zollgesetz.

260 Vgl. z.B. die Regelung im künftigen Art. 112 Abs. 2 Zollgesetz, der die Bekanntgabe von Daten aus einem Profiling ausdrücklich erwähnt, im Unterschied zum künftigen Art. 107a Abs. 5 Luftfahrtsgesetz, wo das Profiling zwar gestattet wird, nicht aber die Bekanntgabe von Daten daraus, und dies wiederum anders als die Bekanntgabe von besonders schützenswerten Personendaten.

von oder ein Profiling mit Gesundheitsdaten erfolgen, ist dies nur gestattet, wenn dies ausdrücklich in einer Gesetzesnorm erlaubt wird.

(d) Ausnahmen vom Legalitätsprinzip

Es wurde bereits in Abschnitt 4.1.4. b) iii.) (a) darauf hingewiesen, dass auch gewisse Ausnahmen vom Legalitätsprinzip im DSG enthalten sind. Es geht also um Fälle, in welchen eine formell-gesetzliche Grundlage im beschriebenen Sinne für die Nutzung von Gesundheitsdaten fehlt. Es handelt sich insbesondere um die folgenden beiden Ausnahmen:

1. Mittelbare gesetzliche Grundlage:[261] Unter drei Voraussetzungen ist die Bearbeitung von Gesundheitsdaten durch ein Bundesorgan auch ohne Grundlage in einem Gesetz im formellen Sinne zulässig: Erstens muss die Bearbeitung für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich sein, zweitens darf der Bearbeitungszweck für die Grundrechte der betroffenen Person keine besonderen Risiken bergen und drittens muss mindestens eine Ermächtigungsgrundlage in einem Gesetz im materiellen Sinn vorhanden sein. Selbst für den Fall, dass eine Bearbeitung der Gesundheitsdaten also tatsächlich als unentbehrlich betrachtet und das Vorliegen solcher Risiken verneint werden könnte, müsste zumindest eine Grundlage auf Verordnungsstufe vorliegen.

2. Einwilligung der betroffenen Person im Einzelfall:[262] Eine Einwilligung der betroffenen Personen kann zwar sowohl eine Ausnahme vom Erfordernis der gesetzlichen Grundlage im formellen Sinne als auch vom Erfordernis der gesetzlichen Grundlage im materiellen Sinne darstellen,[263] dürfte aber in der Praxis neben den in Bezug auf Private erläuterten Anforderungen mit zusätzlichen Schwierigkeiten verbunden sein. Erstens dürften infolge des Kriteriums "im Einzelfall" noch strengere Anforderungen an die Bestimmtheit gelten.[264] Zweitens stellen sich angesichts des Verhältnisses zwischen betroffener Person und Bundesorganen zusätzliche Fragen in Bezug auf das Kräfteungleichgewicht und damit Zweifel an der Freiwilligkeit bzw. Wirksamkeit der Einwilligungen.[265] Drittens dürfte auch der praktische Umgang mit dem Umstand, dass Einwilligungen jederzeit widerrufen werden können, Fragen aufwerfen.[266]

Ausgehend davon liefern die Ausnahmen vom Legalitätsprinzip nur einen beschränkten Raum für die Abstützung von Sekundärnutzungen von Gesundheitsdaten.

iv.) Zwischenfazit: Hindernisse in den DSG-Vorschriften für Bundesorgane

Auch wenn somit auch für Bundesorgane eine Forschungsausnahme gesetzlich verankert ist, sind relativ hohe Anforderungen daran geknüpft und viele Fragen, namentlich mit Blick auf das Erfordernis der Anonymisierung, ungeklärt. Des Weiteren kann selbst bei Einhaltung all dieser Erfordernisse ein Verstoss gegen den

[261] Art. 34 Abs. 3. nDSG.

[262] Art. 34 Abs 4 lit. b nDSG.

[263] Vgl. dazu BÜHLMANN/SCHÜEPP Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 25.

[264] Vgl. zu diesem Kriterium BÜHLMANN/SCHÜEPP Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 39 ff.

[265] Vgl. dazu z.B. MEIER, Protection des données, 2010, Rz. 856 ff.

[266] Vgl. dazu z.B. MEIER, Protection des données, 2010, Rz. 840 ff.

Rechtmässigkeitsgrundsatz nicht geheilt werden, sodass bei Daten, die von Dritten unrechtmässig erhoben oder übermittelt wurden, auch deren Weiterbearbeitung für Forschungs- oder Statistikzwecke durch das Bundesorgan unzulässig sein kann. Darüber hinaus sind die Anforderungen an die Ermächtigungsgrundlagen vergleichsweise tief und es genügen unter dem Legalitätsprinzip bereits relativ allgemein formulierte Vorschriften für die Sekundärnutzung von Gesundheitsdaten. Ob aber überhaupt eine solche Norm vorliegt, muss für jedes Bundesorgan und jeden Tätigkeitsbereich gesondert geprüft werden. Es muss deshalb stets in einer Vielzahl von Spezialgesetzen nach einer entsprechenden Norm gesucht werden, was gerade bei der Beteiligung von Bundesorganen aus unterschiedlichen Bereichen aufwändig sein kann.

Unabhängig davon würde aber selbst eine solche Grundlage nicht jegliche Sekundärnutzung von Daten zu anderen Zwecken als zur gesetzlichen Aufgabenerfüllung erlauben und auch nicht von der Einhaltung des (strengen) Zweckbindungsgebots entbinden. Da die Anforderungen des Zweckbindungsgebots zusätzlich gelten, ist selbst eine breite Ermächtigungsgrundlage alleine nur von begrenztem praktischem Wert im Hinblick auf die Sekundärnutzung. Diese Einschätzung wird bereits aus dem gleichen Grund auch auf die gesetzlichen Ausnahmen vom Legalitätsprinzip zutreffen. Soweit es nicht um (tatsächlich) anonymisierte Gesundheitsdaten geht, ist eine Sekundärnutzung durch Bundesorgane derzeit nur eingeschränkt möglich und mit vielen Unsicherheiten verbunden.

c) Weitere Anforderungen für Private und Bundesorgane

Neben diesen Kernanforderungen gilt es bei der Sekundärnutzung, wie bei jeder anderen Datenbearbeitung, auch die weiteren Vorschriften des DSG zu beachten. Je nach Kontext können die unterschiedlichsten aus dieser Vielzahl von Vorgaben hervorgehoben werden. Die praktischen Erfahrungen zeigen jedoch aus unserer Sicht, dass insbesondere die folgenden Punkte grundlegende Fragestellungen aufwerfen und insofern zu einem Hindernis für die Sekundärnutzung werden können:

1. Verhältnismässigkeitsgrundsatz: Das DSG schreibt vor, dass Datenbearbeitungen verhältnismässig sein müssen.[267] Es handelt sich dabei, wie beim Zweckbindungsgebot, um einen Datenbearbeitungsgrundsatz. Eine Sekundärnutzung von Gesundheitsdaten, die dagegen verstösst, ist somit verboten und könnte nur bei privaten Verantwortlichen – anders als bei Bundesorganen – zulässig sein, wenn die Voraussetzungen eines Rechtfertigungsgrunds gegeben sind. Nach diesem Grundsatz dürfen Personendaten nur so weit bearbeitet werden, als dies für den jeweiligen Zweck objektiv geeignet und tatsächlich erforderlich ist. Die Rede ist in diesem Zusammenhang auch vom Grundsatz der Datensparsamkeit oder Datenminimierung. Es soll also vereinfacht gesagt sichergestellt werden, dass nicht mehr Daten erhoben werden als tatsächlich nötig sind. Zudem ist verlangt, dass die Bearbeitung für die betroffene Person sowohl hinsichtlich ihres Zwecks als auch hinsichtlich ihrer Mittel zumutbar ist. Dazu muss geprüft werden, ob zwischen dem Bearbeitungszweck und der mit einer Bearbeitung verbundenen Persönlichkeitsbeeinträchtigung ein vernünftiges Verhältnis besteht.[268] Die praktische Beurteilung, inwieweit diese Vorgaben im konkreten Fall eingehalten werden, ist mit erheblichen Unsicherheiten verbunden, namentlich weil eine Interessenabwägung im Einzelfall vorgenommen werden muss. Es ist mit anderen Worten regelmässig unklar, wann konkret die Grenze überschritten wird, also bspw. zu viele Daten erhoben werden oder die Bearbeitung als solche zumutbar ist für die betroffene Person.
   Gleiches gilt auch mit Blick auf einen weiteren Teilaspekt des Verhältnismässigkeitsgrundsatzes,

[267] Art. 6 Abs. 2 nDSG.

[268] Botschaft zum DSG, BBl 1988 S. 450.

nach dem auch der Kreis der in die Bearbeitung involvierten Personen nicht weiter sein darf als erforderlich (sog. Need-to-Know Prinzip). Haben also bspw. in einem Versicherungsunternehmen mehr Abteilungen als nötig Zugriff auf die Personendaten, ist der Grundsatz verletzt.
Eng verbunden mit dem Verhältnismässigkeitsgrundsatz ist auch der Grundsatz der Speicherbegrenzung.[269] Danach muss die Speicherdauer von Daten auf das für die Erreichung des Bearbeitungszwecks unbedingt erforderliche Mindestmass beschränkt werden.[270] Ist eine Speicherung bzw. der Bezug zu einer bestimmten Person zur Erreichung des Zwecks nicht mehr erforderlich, müssen die Daten gelöscht oder anonymisiert werden.
Die Umsetzung dieser Anforderungen ist in der Praxis schwierig und mit vielen Unsicherheiten verbunden. Namentlich bei Big-Data-Anwendungen kann es hier zu einem grundlegenden Konflikt führen, zielen diese doch gerade auf die Bearbeitung einer möglichst grossen Zahl von Daten ab.
Der Verhältnismässigkeitsgrundsatz und die damit verbundenen Unsicherheiten stellt insofern ein wesentliches Hindernis dar für die Sekundärnutzung von Gesundheitsdaten.

2. Auslandbekanntgabe: Das Datenschutzgesetz sieht besondere Regelungen für die Bekanntgabe von Personendaten in andere Länder vor.[271] Danach dürfen Personendaten nur in Länder bekanntgegeben werden, in welchen ein angemessenes Datenschutzniveau besteht. Zu diesen Ländern zählen nach aktuellem Stand namentlich die Staaten des Europäischen Wirtschaftsraums (EWR), sowie die anderen Staaten, die auf einer Liste des Datenschutzbeauftragten[272] bzw. künftig des Bundesrats[273] aufgeführt sind. Zahlreiche wirtschaftlich bedeutsame Staaten, wie die USA, zählen jedoch nicht dazu. Dies hat zur Folge, dass eine Bekanntgabe in Staaten wie die USA unzulässig ist, wenn nicht weitere Vorkehrungen getroffen werden. Gerade weil bereits die theoretische Zugriffsmöglichkeit aus einem solchen Land als Bekanntgabe gilt[274] und eine Vielzahl von wichtigen Wirtschaftsakteuren ihren Sitz in solchen Ländern hat, kommt der Regelung eine erhebliche praktische Bedeutung zu. In Grundsatzurteilen zu Datenbekanntgaben in die USA hat der Europäische Gerichtshof (EuGH) erhebliche Defizite im Datenschutzrecht festgestellt.[275] Dieser Einschätzung ist auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) gefolgt.[276] Die Unternehmen stehen deshalb aktuell vor der Herausforderung, insbesondere bei der Zusammenarbeit mit US-Anbietern, Massnahmen zu ergreifen, die diese Defizite beseitigen, sodass letztlich sichergestellt ist, dass durch diese Anbieter nur eine aus europäischer Perspektive angemessene Datenbearbeitung erfolgt. Die Praxis zeigt, dass es aktuell kaum Massnahmen, mit Ausnahme einer effektiven Anonymisierung der Daten, gibt, mit welchen diese Anforderungen wirksam umgesetzt werden können. Eine grosse Zahl an Datenbearbeitungen, die mit einer Datenbekanntgabe in Staaten wie die

269 Art. 5 Abs. 4 nDSG.

270 Vgl. Erwägungsgrund 39 EU-DSGVO.

271 Art. 16 f. nDSG.

272 Art. 7 VDSG; ferner die Liste des EDÖB, https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf. (zuletzt aufgerufen am 29.5.2022).

273 Vgl. Art. 16 Abs. 1 nDSG.

274 Vgl. Art. 5 lit. e nDSG; ferner ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 6 Rz. 4.

275 Vgl. zuletzt Urteil des Europäischen Gerichtshofs vom 16. Juli 2020, C-311/18 (Schrems II).

276 EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG, 8.9.2020.

USA verbunden sind, sind deshalb nach aktuellem Stand unzulässig. Dies gilt auch für Sekundärnutzungen von Gesundheitsdaten, bei welchen bspw. auf Software-Lösungen von US-Anbieter zurückgegriffen wird oder ein Datenaustausch mit Organisationen in den USA stattfindet.

d) Konsequenzen von Verstössen gegen das DSG

Für die Praxis der Sekundärnutzung von Gesundheitsdaten ist von grosser Bedeutung, welche Konsequenzen Verstösse gegen DSG nach sich ziehen. Das DSG enthält sowohl strafrechtliche als auch zivil- und verwaltungsrechtliche Konsequenzen. Bei Letzteren ist hervorzuheben, dass die Weiternutzung von Daten unter Androhung einer Ungehorsamsstrafe (für den Fall der Nichtbefolgung) vollumfänglich verboten und die Löschung der Daten angeordnet werden kann.[277] Die Forschenden könnten beim Verstoss gegen das DSG somit ihre wertvollen und über einen grossen Zeitraum aufgebauten Datenbestände vollumfänglich verlieren. Darüber hinaus können grundsätzlich auch Schadenersatz oder Genugtuungsansprüche geltend gemacht werden. Während die zivilrechtlichen Konsequenzen nur bei Verstössen gegen die Vorschriften für private Verantwortliche drohen, können die Verbote und Löschungsanordnungen auch im Anwendungsbereich der Vorschriften für Bundesorgane ausgesprochen werden.

Eine potentiell noch grössere Tragweite kommt den strafrechtlichen Konsequenzen zu. Die Strafbestimmungen des nDSG werden im Vergleich zur aktuellen Rechtslage deutlich verschärft, auch wenn der Katalog der sanktionierten Verhaltensweisen nach wie vor viel weniger weit geht als in der EU-DSGVO.[278] Hervorzuheben ist vorliegend, dass namentlich Verstösse gegen die Informationspflichten, die Vorschriften zur Datenbekanntgabe ins Ausland und die Regeln zur Auftragsbearbeitung in dem Katalog aufgeführt werden. Folglich kann z.B. die mangelnde oder falsche Informationserteilung bei der Beschaffung von Personendaten mit einer Busse sanktioniert werden. Wird die betroffene Person vorsätzlich nicht über eine Weiterverwendung ihrer Personendaten zu anderen – als bei der Beschaffung genannten – Zwecken informiert, wäre der (objektive) Straftatbestand erfüllt. Sanktionen drohen auch bei der Datenübermittlung an Softwareunternehmen oder Forschungspartner in den USA, wenn keine hinreichenden Garantien ergriffen werden. Folglich wiegen insbesondere die oben im Zusammenhang mit dem Zweckbindungsgebot, den Auslandbekanntgaben und den datenschutzrechtlichen Rollen geschilderten Unsicherheiten besonders schwer, muss doch beim Vertrauen auf eine extensive Interpretation der einzelnen Vorschriften eine strafrechtliche Sanktion in Kauf genommen werden.

Ferner erscheint die Strafbemessung von maximal CHF 250.000[279] im Vergleich zu den Strafen der DSGVO (bis zu EUR 20 Millionen oder 4% vom weltweiten Jahresumsatz)[280] zwar relativ moderat, jedoch ist – anders als in der EU – nicht das Unternehmen, sondern die verantwortliche natürliche Person das Strafsubjekt. Dies kann eine Leitungsperson sein, die gesetzlich zur Überwachung der Einhaltung der Datenschutzbestimmungen verpflichtet ist (z.B. die Geschäftsführung). Darüber hinaus können auch andere Personen, welche das Unternehmen nicht organschaftlich vertreten, für Datenschutzverstösse haften, sofern sie über datenschutzrechtliche Prozesse im Unternehmen entscheiden.[281] Nur in Ausnahmefällen und bei Bussen von bis zu CHF

[277] Vgl. Art. 32 und 51 f. nDSG.

[278] Vgl. Art. 60 ff. nDSG.

[279] Art. 60 ff. nDSG.

[280] Art. 83 Abs. 5 DSGVO.

[281] ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 195.

50.000 kann anstatt der verantwortlichen Person auch das betreffende Unternehmen gebüsst werden.[282] Zudem dürfen die Bussen nach verbreiteter Auffassung nicht vom Unternehmen übernommen werden und sie sind nicht versicherbar.[283] Das nDSG stellt weiter lediglich den vorsätzlichen Verstoss unter Strafe, wobei bereits ein Eventualvorsatz ausreichend ist. Ein solcher Eventualvorsatz liegt bereits vor, wenn es die verantwortliche Person für möglich hält, dass ein Straftatbestand (z.B. die Verletzung der Informationspflichten) vorliegen könnte und dieses Risiko in Kauf nimmt.[284]

4.1.5 Fazit: Hindernisse im DSG

Zusammenfassend ist festzuhalten, dass sich aus dem DSG (auch nach der Totalrevision) eine Vielzahl von Hindernissen für die Sekundärnutzung von Gesundheitsdaten ergibt.

Zu den grundlegendsten zählen die bereits in Abschnitt 3 aufgeführten Unsicherheiten in Bezug auf den Anwendungsbereich. Es geht also etwa um die Frage, was vorzukehren ist, um Personendaten tatsächlich zu anonymisieren und dadurch die Anwendung des DSG zu verhindern.

Die Ausführungen im erwähnten Abschnitt haben auch deutlich gemacht, dass die Beurteilung des persönlichen Anwendungsbereichs in vielen Fällen Schwierigkeiten bereiten kann. Gerade im Gesundheitsbereich fällt die Beurteilung nicht immer leicht, ob bei einer Tätigkeit eine öffentliche Aufgabe erfüllt wird, und falls ja, ob es sich um eine kantonale Aufgabe oder eine Bundesaufgabe handelt. Diese Beurteilung ist jedoch wichtig und entscheidet darüber, ob die (strengeren) öffentlich-rechtlichen Vorschriften des DSG oder der Kantone zur Anwendung kommen.

Erschwerend kommt hinzu, dass dieselbe Rechtseinheit für unterschiedliche Bearbeitungen unterschiedlichen Vorschriften innerhalb des Bundesrechts und/oder des kantonalen Rechts unterstehen kann. Bspw. untersteht ein Bundesorgan für Tätigkeitsbereiche, in welchen es privatrechtlich handelt, den Vorgaben des DSG für Private und für seine übrigen Tätigkeiten den strengeren öffentlich-rechtlichen Vorschriften für Bundesorgane. Da im Gesundheitssektor eine grosse Zahl von Spezialgesetzen gilt, ist auch stets zu untersuchen, inwieweit solche Vorschriften denjenigen des DSG vorgehen. Wie anspruchsvoll und ungewiss diese Beurteilung ist, wird in Abschnitt 4.2 zum HFG erläutert.

Somit kann sich bereits die Suche nach den anwendbaren Vorschriften zeitintensiv und anspruchsvoll gestalten und dadurch ebenfalls ein Hindernis für die effiziente Sekundärnutzung von Gesundheitsdaten darstellen.

Weiter besteht eine Vielzahl von Ungewissheiten grundsätzlicher Natur. So kann bei arbeitsteiligen Geschäftsprozessen unklar sein, wem, wofür, welche konkrete datenschutzrechtliche Rolle zukommt. Dies erschwert nicht nur die datenschutzrechtliche, sondern auch die zur Festlegung der Verantwortlichkeiten notwendigen Vertragsverhandlungen und -ausgestaltungen.

Ferner ist innerhalb der Vorschriften bei Daten, die einen Bezug zur körperlichen Verfassung eines Menschen aufweisen, oftmals unsicher, ob die höheren Anforderungen für Gesundheitsdaten, als besonders schützenswerte Daten, gelten oder nicht, hängt dies doch ebenfalls vom Kontext der Bearbeitung ab. Potentiell eine grosse Erleichterung für den praktischen Umgang mit diesen Unsicherheiten kann die sogenannte

[282] Art. 64 Abs. 2 nDSG.

[283] Vgl. ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 191 m.w.H.

[284] Vgl. Art. 12 Abs. 2 StGB.

Forschungsausnahme sein, die in vergleichbarer Form sowohl für private Verantwortliche als auch für Bundesorgane gilt. Der praktische Nutzen derselben als Absicherung für die Sekundärnutzung von Gesundheitsdaten wird jedoch dadurch vermindert, dass hier auf den unklaren Begriff der Anonymisierung abgestellt wird und deshalb stets unklar ist, ob die Voraussetzungen eingehalten werden können.

Ausgehend davon ist in der Praxis Bedarf nach Alternativen oder zusätzlichen Absicherungen vorhanden. Eine davon kann die Einwilligung der betroffenen Personen in die Sekundärnutzung sein. Die Anforderungen an eine gültige Einwilligung sind allerdings nicht immer leicht zu erfüllen. Es bestehen auch betreffend der Anforderungen Unsicherheiten und eine breit gefasste Einwilligung, welche auch künftige, noch nicht näher bekannte Sekundärnutzungen abdecken soll, scheitert ausserhalb des Anwendungsbereichs des HFG oftmals am engen Verständnis des Zweckbegriffs. Einen sog. Generalkonsent, der im HFG unter bestimmten Voraussetzungen gestattet wird, kennt weder das DSG noch das nDSG. Darüber hinaus bestehen insbesondere für Bundesorgane ohnehin zusätzliche Anforderungen, die den praktischen Nutzen der Einwilligung als Mittel zur Ermöglichung von Sekundärnutzungen weiter einschränken. Zu diesen Hindernissen im Bereich der Kernanforderungen für die Sekundärnutzung kommt eine Vielzahl von weiteren Vorschriften hinzu, die in der Praxis bei sämtlichen Bearbeitungen von Personendaten mit Unsicherheiten verbunden sind, wie etwa die Anforderungen an die Datensparsamkeit oder die Datenübermittlungen ins Ausland. Die geschilderten Hindernisse und Unsicherheiten wiegen umso schwerer, als die Konsequenzen bei Verstössen gegen das DSG mit der Totalrevision weiter ausgebaut wurden und namentlich einschneidende strafrechtliche Sanktionen für die verantwortlichen Personen drohen.

4.2 Sekundärnutzung von Gesundheitsdaten im HFG

4.2.1 Geltungsbereich und Grundbegriffe

Es wurde bereits in den Ausführungen zum Begriff der Gesundheitsdaten in Abschnitt 3.2.2 auf zentrale Aspekte des Geltungsbereichs des HFG eingegangen. Es wurde dargelegt, wann von Gesundheitsdaten auszugehen und was unter biologischem Material zu verstehen ist, wie die Begriffe im Verhältnis zu den Definitionen des DSG stehen und wann eine Anonymisierung anzunehmen ist. Nachfolgend wird erläutert, was für die Erfassung des Anwendungsbereichs des HFG weiter bedeutsam ist und inwieweit die Sekundärnutzung von Gesundheitsdaten den Vorgaben des HFG unterstellt ist.

Das HFG gilt für die Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers, die durchgeführt wird:

- mit Personen;
- an verstorbenen Personen;
- an Embryonen und Föten;
- mit biologischem Material;
- mit gesundheitsbezogenen Personendaten.

a) Weiter Begriff der Forschung

Der Forschungsbegriff des HFG ist definiert als die "methodengeleitete Suche nach verallgemeinerbaren Erkenntnissen", wobei keine Einschränkung auf institutionelle Forschungseinrichtungen (bspw. Universitäten) vorgenommen wird. Die Präzisierung "methodengeleitet" verweist auf die Anwendung von wissenschaftlich anerkannten Vorgehensweisen zur Erkenntnisgewinnung. Dabei kann es sich sowohl um natur- als auch um sozialwissenschaftliche Methoden handeln. Generell bildet demnach die Praxis der "scientific community"

den wesentlichen Referenzmassstab, dennoch soll der Methodenbegriff gegenüber neuartigen, unter Umständen gängigen wissenschaftlichen Standards widersprechenden, Methoden offen sein.[285]

Jedenfalls müssen die Abweichungen vom geltenden Wissenschaftsstandard eingehend begründet und die Anforderungen an die wissenschaftliche Qualität eingehalten werden.[286] Die zu gewinnenden Erkenntnisse müssen zudem verallgemeinerbar sein, d.h. sie müssen auch über den Kontext des Forschungsprojekts hinaus Gültigkeit besitzen und dürfen nicht einen nur individuellen Bezug aufweisen. Die Verallgemeinerbarkeit wird bspw. mittels einer genügend hohen Fallzahl sowie einer realitätsnahen Forschungsanlage angestrebt.[287] Der Anwendungsbereich des HFG richtet sich primär nach dem Ziel und nicht direkt nach der Art bzw. Konzeption der Forschungstätigkeit.[288]

Der Anwendungsbereich des HFG ist somit recht weit gefasst: Solange eine von der wissenschaftlichen Gemeinschaft anerkannte Methode zur Gewinnung von Erkenntnissen mit dem Ziel der Verbesserung der medizinischen Standards oder des besseren Verständnisses des menschlichen Körpers (und seiner Bestandteile) eingesetzt wird, gilt das HFG.[289] Fraglich ist, wie konkret diese Zielsetzung verfolgt werden muss. Generell kann im Anwendungsbereich des HFG auf keine umfassende Rechtsprechungspraxis zurückgegriffen werden, was die Beantwortung von strittigen Auslegungsfragen erschwert und zu Rechtsunsicherheit führt.

Die Durchführung der Forschung beginnt mit der ersten forschungsbedingten Interaktion zwischen den Forschenden und den Personen, Daten oder biologischen Materialen, an denen die Forschung i.S.d. HFG durchgeführt wird und endet mit Abschluss des Forschungsprojekts.[290] Erfasst werden auch Vorbereitungshandlungen, wie z.B. die Rekrutierung von Studienmitgliedern oder die Aufbereitung von biologischem Material, an dem die Forschung durchgeführt wird.[291] Selbst Forschungsprojekte, die zum Grossteil im Ausland durchgeführt werden, in der Schweiz aber Personen für die Forschung rekrutieren, fallen unter das HFG.[292]

Inwiefern zeitlich vorgelagerte Vorbereitungshandlungen, wie z.B. die Konzipierung eines Forschungsprojekts und Machbarkeitsstudien, vom Anwendungsbereich des HFG umfasst sind, ist fraglich. Geht man von einem weiten Verständnis der Zielsetzung zur Verbesserung medizinischer Standards bzw. Verständnis des menschlichen Körpers aus, kann man wohl auch diese Handlungen unter den Anwendungsbereich des HFG subsumieren, weil sie langfristig auch dem später verfolgten Ziel im Forschungsprojekt dienen. Selbstverständlich ist diese Frage jedoch im konkreten Einzelfall zu beurteilen. Sofern im Rahmen der genannten Vorbereitungshandlungen noch keine Bearbeitung von gesundheitsbezogenen Personendaten (einschliesslich

---

285 VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 3 Rz. 4; SCHWEIZER/HAFNER, St. Galler Komm. BV, 2014, Art. 20 Rz. 8.

286 VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz 2015, Art. 3 Rz. 4; Art. 10 HFG.

287 Botschaft zum HFG, BBl 2009 S. 8093.

288 Dies steht im Gegensatz zu einem früheren Entwurf des HFG; vgl. Bericht über die Ergebnisse des Vernehmlassungsverfahrens zum Vorentwurf einer Verfassungsbestimmung und eines Bundesgesetzes über die Forschung am Menschen: https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/6005/35/cons_1/doc_10/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-6005-35-cons_1-doc_10-de-pdf-a.pdf (zuletzt aufgerufen am 15.05.2022).

289 MARTANI/EGLI/WIDMER, Data protection and biomedical research in Switzerland: setting the record straight Swiss Med Wkly. 2020, S. 5. MARTANI/EGLI/WIDMER, Swiss Med Wkly. 2020.

290 VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz (2015, Art. 2 Rz. 9.

291 VAN SPYK, in: RÜTSCH*E* (Hrsg.), Humanforschungsgesetz, 2015, Art. 2 Rz. 9.

292 Van Spyk, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 2 Rz. 9.

genetischen Daten) bzw. biologischem Material vorgenommen wird, stellt sich hingegen die Frage nach der Anwendbarkeit der Datenschutzbestimmungen des HFG ohnehin nicht. Die Abgrenzung kann ferner auch Schwierigkeiten bereiten bei Projekten zur Qualitätssicherung, bei Anwendungsbeobachtungen und bei Arbeiten zur wissenschaftlichen Qualifizierung (Dissertationen und Masterarbeiten).[293]

Vom Anwendungsbereich des HFG sind schliesslich nur Forschungshandlungen umfasst, die sich auf Krankheiten des Menschen oder den Aufbau und die Funktion des menschlichen Körpers beziehen. Das Erkenntnisziel des Forschungsprojekts ergibt sich üblicherweise aus den im Prüfplan oder Forschungsplan festgelegten und durch die Studie zu beantworteten Fragen.[294]

b) Ausnahmen vom Geltungsbereich

Explizit vom Geltungsbereich des HFG ausgenommen ist die Forschung an Embryonen in vitro nach dem Stammzellenforschungsgesetz, mit anonymisiertem biologischem Material und mit anonymisierten gesundheitsbezogenen Daten.[295]

Von der Ausnahme für anonymisiertes biologisches Material und anonymisierte gesundheitsbezogene Personendaten sind aber nur retrospektive Studien erfasst, die anonym erhobene bzw. anonymisierte Daten für die Forschung weiterverwenden.[296] Prospektive Studien, im Zuge derer von anonymen Personen gesundheitsbezogene Daten erhoben werden (z.B. durch Umfragen mit anonymer Rückmeldung zu menschlichen Krankheiten), sind nicht vom HFG ausgenommen.[297] Die forschungsbedingte Interaktion zwischen Forschenden und (allenfalls auch anonymen) Personen ist als Forschung mit Personen nach Art. 2 Abs. 1 lit. a HFG zu qualifizieren und daher vom Geltungsbereich des Gesetzes erfasst, obwohl anonyme Daten erhoben werden.[298] Dementsprechend hat auch die Durchführung dieser anonymen Studien im Einklang mit den Bestimmungen des HFG zu erfolgen.

4.2.2 Verhältnis zu den datenschutzrechtlichen Vorschriften

Wie bereits erwähnt, stellt sich bei sektorspezifischen Regelungen die Frage nach ihrem Verhältnis zu den allgemeinen Vorgaben des DSG. Dies gilt auch für das HFG, das eine Vielzahl von Vorschriften mit Datenschutzbezug enthält. Die festgehaltenen Erkenntnisse gelten auch im Verhältnis zwischen den Vorschriften des HFG und denjenigen des DSG sowie denjenigen der (später[299] zu erläuternden) kantonalen Datenschutzgesetzgebungen.

---

[293] Vgl. SAMW, Forschung mit Menschen, Ein Leitfaden für die Praxis, 2. Aufl., 2015, S. 24.

[294] VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 2 Rz. 11.

[295] Art. 2 Abs. 2 HFG.

[296] VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 2 Rz. 27; RÜTSCHE, Neuordnung, 2010, S. 397 Fn. 22; Botschaft zum HFG, BBl S. 8092.

[297] VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 2 Rz. 27; RÜTSCHE, Neuordnung, 2010, S. 397 Fn. 22; Botschaft zum HFG, BBl 2009 S. 8092.

[298] VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 2 Rz. 27; RÜTSCHE, Neuordnung, 2010, S. 397 Fn. 22; Botschaft zum HFG, BBl. 2009 S. 8092.

[299] Vgl. Abschnitt 4.3.

Nach dem Gesagten ist somit für jede Fragestellung und Bestimmung im HFG einzeln durch Auslegung zu ermitteln, inwieweit diese eine abschliessende Regelung enthält und die bereichsübergreifenden Regelungen des DSG und der kantonalen Datenschutzgesetze verdrängt.[300] Trotz der grossen praktischen Bedeutung fehlen aber auch hier zu den meisten Fragestellungen und Bestimmungen begründete und klare Stellungnahmen in Lehre und Rechtsprechung. So wird nicht selten bloss auf die Thematik hingewiesen, die Frage aber nicht beantwortet.[301] Zum Teil wird in Bezug auf die Sekundärnutzung ohne Auseinandersetzung mit den Entstehungsgeschichten der Erlasse oder der oben genannten einschlägigen Lehre und Rechtsprechung pauschal die Auffassung vertreten, dass das HFG als Spezialgesetz die allgemeinen Datenschutzgesetze verdränge, soweit nicht ausnahmsweise ein expliziter Verweis auf das DSG enthalten sei.[302]

Diese Auffassung ist offensichtlich zu wenig differenziert und lässt offen, was genau der Regelungsbereich "Secondary Research in der Humanforschung" umfassen soll, der implizit als "abschliessend geregelt" bezeichnet wird. Soweit damit zum Ausdruck gebracht werden soll, dass bei der datenschutzrechtlichen Beurteilung der Sekundärnutzung im (einleitend beschriebenen) Anwendungsbereich des HFG bloss die Vorschriften des HFG sowie deren Konkretisierungen in der HFV zu prüfen sind, kann dem nicht gefolgt werden. Dies ergibt sich bereits aus einem Blick auf die Botschaft zum HFG. Dort wird zwar richtigerweise ebenfalls der Charakter als Spezialregelung erwähnt und von einem Vorrang gegenüber dem DSG gesprochen. Es wird allerdings nicht pauschal, sondern differenziert festgehalten, dass die Bestimmungen in Art. 32 ff. "bezüglich der vom Geltungsbereich dieses Gesetzes erfassten Forschung den allgemeinen datenschutzrechtlichen Regelungen zur Weiterverwendung von Daten für die Forschung (vgl. Art. 13 und 22 Datenschutzgesetz)" vorgehen.[303] Dies deutet folglich vielmehr darauf hin, dass das HFG auch für die Sekundärnutzung nicht sämtliche Vorgaben der allgemeinen Datenschutzgesetze verdrängt, sondern nur diejenigen zur Weiterverwendung von Daten, und somit nicht sämtliche datenschutzrechtlichen Aspekte, abschliessend regelt.

Es ist deshalb davon auszugehen, dass neben der Regelung im HFG durchaus Raum für die Anwendung des DSG und der kantonalen Datenschutzgesetze besteht.[304] Dies gilt nicht nur im Sinne einer ergänzenden Anwendung auf bestehende Regelungen oder einer Berücksichtigung im Rahmen der Auslegung von Begriffen, die im HFG verwendet werden,[305] sondern umso mehr auch dort, wo eine vergleichbare Regelung im HFG gänzlich fehlt. Konkrete Stellungnahmen zu den einzelnen Bestimmungen des HFG fehlen allerdings in jeglicher Hinsicht. Es kann deshalb nur schwer abgeschätzt werden, wie Gerichte in einem Streitfall entscheiden würden, und die Rechtslage lässt sich auch nur grob skizzieren.

So ist es nach der hier vertretenen Auffassung naheliegend, dass im Bereich der Sekundärnutzung die Vorschriften in Art. 32 ff. HFG die Vorschriften zur Rechtmässigkeit der Datenschutzgesetze grundsätzlich verdrängen. Unzweifelhaft ist dies in Bezug auf die Anforderungen an den Datenbearbeitungsgrundsatz der

---

300 Vgl. auch BRUNNER, in: RÜTSCHE (Hrsg.), SHK-HFG, 2015, Vorbemerkungen Art. 56-61 N 4 ff.

301 S. z.B. WERMELINGER, in: BAERISWYL/PÄRLI (Hrsg.), SHK-DSG, 2015, Art. 13 N 27; vgl. auch ISLER, Die Rollenverteilung in klinischen Versuchen in: digma 2020 S. 68 ff., 69: "Das Humanforschungsgesetz ist somit ein sektorieller Datenschutzerlass, der in seinem Regelungsbereich vor dem allgemeinen Datenschutzrecht Vorrang hat.".

302 So ROSENTHAL, Die rechtlichen und gefühlten Grenzen der Zweitnutzung von Personendaten, in: sic! 2021 S. 168 ff., S. 169 f.

303 Botschaft zum HFG, BBl 2009 S. 8121.

304 Vgl. insbesondere BRUNNER, in: RÜTSCHE (Hrsg.), SHK-HFG, 2015, Vorbemerkungen Art. 56-61 N 4 ff.; ferner ERARD, Les données codées dans le contexte de la recherche personnelles ou anonymes ?, in: AJP 2021 S. 606 ff., 613 f.

305 Vgl. z.B. bei der Regelung zur Aufbewahrung, wo auch die Vorgaben des DSG für anwendbar gehalten werden, so deutlich: RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.) SHK-HFG, 2015, Art. 43 N 8, sowie ZEGG, Benefit Sharing–- Anspruch auf Teilhabe an Forschungsergebnissen, 2020, S. 39; weniger deutlich: Botschaft zum HFG, BBl 2009 S. 8132, wo die Formulierung eher als Aufforderung an den Bundesrat als Verordnungsgeber und nicht an die dem HFG unterstellten Organisationen verstanden werden könnte.

Zweckbindung.[306] Im Anwendungsbereich des HFG braucht deshalb nicht gesondert geprüft zu werden, ob die sich daraus ergebenden Vorgaben eingehalten werden und falls nicht, ob eine Rechtfertigung im Sinne des DSG möglich wäre. Besonders mit Blick auf die Tätigkeit von öffentlichen Organen im Anwendungsbereich des HFG ist davon auszugehen, dass auch das datenschutzrechtliche Legalitätsprinzip nicht gesondert zu prüfen ist, wie der Hinweis in der Botschaft des HFG auf Art. 22 DSG verdeutlicht. Dies ist allerdings nicht unbestritten.[307]

Ähnliches wie für die Zweckbindung dürfte auch in Bezug auf den Bearbeitungsgrundsatz der Transparenz sowie die Einwilligung gelten[308], auch wenn dort weniger klar ist, ob sämtliche Aspekte abgedeckt sind. Umso mehr gilt dies für die eng damit verbundenen Informationspflichten und der strafrechtlichen Sanktionierbarkeit von Verstössen.[309] Unsicherheit besteht auch mit Blick auf die Anforderungen der Bearbeitungsgrundsätze der Rechtmässigkeit[310] und der Verhältnismässigkeit[311] der Bearbeitung, insbesondere dessen Teilaspekt der Datenminimierung, der Speicherbegrenzung[312] und der Datenrichtigkeit[313]. In Bezug auf die Datensicherheit wird sodann in der Lehre zu Recht explizit von der ergänzenden Anwendbarkeit der Bestimmungen der Datenschutzgesetze ausgegangen.[314]

Schliesslich wird man auch die Grundsätze von Privacy-By-Design und Privacy-By-Default im Anwendungsbereich des HFG für anwendbar erklären müssen. Gleiches gilt in Bezug auf die datenschutzrechtlichen Pflichten mit formellem Charakter, die auch im nDSG ausgebaut werden: Pflichten zur Erstellung von Bearbeitungsverzeichnissen, zum Abschluss von Auftragsbearbeitungsverträgen und zur Erstellung von Datenschutz-Folgenabschätzungen.

Es zeigt sich deshalb, dass ähnlich wie in der EU auch in der Schweiz den bereichsübergreifenden Regelungen eine grosse Bedeutung zukommt.[315] In der Praxis besteht aber mangels Gerichtsurteilen und breiter wissenschaftlicher Aufarbeitung auch hier Rechtsunsicherheit.

---

306 Art. 6 Abs. 3 nDSG.

307 A.A. implizit BAERISWYL, Die Einwilligung hilft (nicht) weiter, digma 2020 S. 62 ff..

308 Vgl. Art. 6 Abs. 3 nDSG, Art. 6 Abs. 6 und 7 nDSG sowie BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 49 ff.

309 Art. 19 ff. nDSG, Art. 60 nDSG.

310 Art. 6 Abs. 1 nDSG; ferner dazu oben Abschnitt 4.1.4a) i.) und 4.1.4b) i.).

311 Art. 6 Abs. 2 nDSG; ferner dazu oben Abschnitt 4.1.4c).

312 Art. 6 Abs. 4 nDSG.

313 Art. 6 Abs. 5 nDSG.

314 Vgl. z.B. bei der Regelung zur Aufbewahrung, wo auch die Vorgaben des DSG für anwendbar gehalten werden, so deutlich: RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), SHK-HFG, 2015, Art. 43 N 8, sowie ZEGG, Benefit Sharing–- Anspruch auf Teilhabe an Forschungsergebnissen, Zürich/Basel/ Genf 2020, S. 39; weniger deutlich: Botschaft zum HFG, BBl 2009 S. 8132, wo die Formulierung eher als Aufforderung an den Bundesrat als Verordnungsgeber und nicht an die dem HFG unterstellten Organisationen verstanden werden könnte.

315 Anders wohl ISLER, Die Rollenverteilung in klinischen Versuchen, in: digma 2020, S. 68 ff., 69. "Damit unterscheidet sich die diesbezügliche schweizerische Regulierung von derjenigen in der Europäischen Union, wo die Gesetzgebung über klinische Studien den Datenschutz praktisch vollumfänglich der DSGVO anvertraut".

4.2.3 Allgemeine Anforderungen des HFG für Forschungsprojekte

Nach dem Gesagten kommt somit auch im Bereich der Humanforschung dem DSG und den kantonalen Datenschutzgesetzen massgebliche Bedeutung zu. Gleichwohl richtet sich die praktische Beurteilung, inwieweit die Sekundärnutzung von Gesundheitsdaten im breiten Anwendungsbereich des HFG gestattet ist, zunächst danach, was in der Spezialgesetzgebung vorgesehen ist. Denn anders als im DSG, wo an allgemeine Prinzipien, namentlich das Zweckbindungsgebot, anzuknüpfen ist, besteht im HFG eine explizite Regelung für die Sekundärnutzung von biologischem Material und gesundheitsbezogenen Personendaten. Diese Regelungen stellen eine in der Praxis wertvolle Konkretisierung der allgemeinen Vorschriften des DSG dar, wobei wie erwähnt nicht restlos klar ist, inwieweit die Bestimmungen des DSG gleichwohl noch ergänzend anwendbar bleiben.

Diese besonderen Regelungen zur Sekundärnutzung im HFG bauen auf den allgemeinen Vorschriften des HFG für die Forschungsprojekte auf. Zu diesen allgemeinen Vorschriften zählen erstens die Bewilligungspflicht, die auch für Weiterverwendungs-Forschungsprojekte gilt, sowie zweitens das Erfordernis der Einwilligung und Aufklärung der Teilnehmenden. Bevor auf die Besonderheiten der Regelung zur Weiterverwendung, insbesondere den besonderen Anforderungen an die Einwilligung, eingegangen wird, werden deshalb zunächst diese beiden allgemeinen Vorschriften erläutert.

a) Bewilligungspflicht und Kompetenz der Ethikkommissionen für die Forschung

Die Durchführung eines Forschungsprojekts im Anwendungsbereich des HFG ist gem. Art. 45 Abs.1 lit. a bewilligungspflichtig. Hierbei handelt es sich um ein Verbot mit Erlaubnisvorbehalt, dementsprechend ist die Durchführung eines Forschungsprojekts im Anwendungsbereich des HFG so lange verboten, bis die Bewilligung durch die zuständige Ethikkommission für die Forschung erteilt wurde.[316] Von der Bewilligungspflicht umfasst sind sowohl prospektive Forschungsprojekte mit Personen (z.B. klinische Versuche mit Heilmitteln), als auch retrospektive Forschungsprojekte mit bereits entnommenem biologischem Material oder erhobenen gesundheitsbezogenen Personendaten.[317] Sofern die Entnahme von biologischem Material bzw. die Erhebung von Gesundheitsdaten zu klinischen Zwecken erfolgt (z.B. im Rahmen der Therapie oder zur Diagnosestellung) und diese Daten bzw. dieses Material erst danach in einer Bio- oder Datenbank zu Forschungszwecken aufbewahrt wird, handelt es sich noch nicht um ein bewilligungspflichtiges Forschungsprojekt. Erst wenn dieses Material bzw. die Daten zur Beantwortung einer Forschungsfrage bearbeitet werden, löst dies die Bewilligungspflicht aus.[318] Die Verantwortung für die Bestimmung dieses Zeitpunkts liegt bei der Projektleitung.[319] Werden im Zuge eines klinischen Eingriffs zusätzliche Daten bzw. Material (die nicht im klinischen Kontext benötigt werden) zu Forschungszwecken gesammelt, stellt dies – im Gegensatz zum obigen Beispiel – ein bewilligungspflichtiges Forschungsprojekt dar.[320]

Die Kompetenz der Ethikkommissionen für die Bewilligung von Forschungsprojekten i.S.d. Art 45 HFG ist unstrittig,[321] jedoch ist fraglich, inwieweit die Ethikkommissionen für die Prüfung von datenschutzrechtlichen

316 JENNI, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 45 Rz. 22.

317 JENNI, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 45 Rz. 3.

318 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 60.

319 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 73.

320 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 61.

321 Art. 45 Abs. 1 lit. a.

Fragestellungen bei der Durchführung eines Humanforschungsprojekts zuständig ist. Gemäss Art. 51 HFG ist die Ethikkommission für die Prüfung der ethischen, rechtlichen und wissenschaftlichen Anforderungen von Forschungsprojekten im Rahmen ihrer Aufgaben laut Kapitel 8 HFG zuständig.

Im Vorentwurf des HFG war vorgesehen, dass die Ethikkommission ausschliesslich die gesetzlichen Anforderungen zum Schutz der betroffenen Personen zu überprüfen haben.[322] Diese "unsachgemässe Verrechtlichung" der Ethikkommission wurde in der Vernehmlassung mehrfach kritisiert und gefordert, dass diese die ethische Vertretbarkeit des Forschungsprojekts zu beurteilen hätte.[323] Darüber hinaus sollte der Ethikkommission – gemäss dem Vorentwurf des HFG – die Kompetenz zur Aufsicht über laufende Forschungsprojekte übertragen werden. Dies wurde von einer Mehrheit der Vernehmlassungsteilnehmer abgelehnt, da die Kommissionen als Milizorgan weder personell noch organisatorisch dazu in der Lage sei.[324]

Die in der Vernehmlassung geäusserte Kritik zu den Kompetenzen der Ethikkommission wurde berücksichtigt und der Gesetzestext dementsprechend angepasst, da sich die materielle Prüfung der Ethikkommissionen für die Forschung insbesondere auf die ethischen Prinzipien zur Forschung am Menschen beziehen soll.[325] Da im Zuge des Bewilligungsverfahrens aber gleichwohl rechtliche Fragen mit Bezug zum Datenschutz zu beurteilen sind, muss gemäss Art. 1 Abs. 1 lit. h Organisationsverordnung zum HFG (OV-HFG) zumindest eine Person mit Fachkenntnissen im Bereich des Datenschutzrechts in der Ethikkommission vertreten sein.[326] Es wurde aber darauf verzichtet, den Ethikkommissionen die vollumfängliche Aufsicht über laufende Forschungsprojekte zu übertragen.[327] Vollzugsmassnahmen – wie z.B. Inspektionen – sind folglich den jeweils zuständigen Behörden des Bundes oder der Kantone vorbehalten.[328] Dementsprechend sind für Überwachung und Vollzug des Datenschutzes im Rahmen des HFG primär die kantonalen Datenschutzbeauftragten für Datenbearbeitungen von kantonalen Einrichtungen zuständig und der EDÖB für Bearbeitungen durch Private und Bundesorgane. Die Ethikkommissionen sind hingegen verpflichtet, Meldungen und Berichte entgegenzunehmen und gegebenenfalls zusätzliche Auflagen anzuordnen oder die Bewilligung zu sistieren.

Zusammenfassend ist im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten davon auszugehen, dass die Ethikkommission im Rahmen des Bewilligungsverfahren zwar auch das Vorliegen der Anforderungen mit datenschutzrechtlichem Bezug zu prüfen hat, jedoch keine Kompetenz zur Überwachung datenschutzrechtlicher Vorgaben im Rahmen der Durchführung eines Forschungsprojekts hat.

b) Einwilligung und Aufklärung

i.) Allgemeine Anforderungen an Einwilligung in die Teilnahme an der Humanforschung

322 Botschaft zum HFG, BBl 2009 S. 8084.

323 Botschaft zum HFG, BBl 2009 S. 8084.

324 Botschaft zum HFG, BBl 2009 S. 8084.

325 Botschaft zum HFG, BBl 2009 S. 8086.

326 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 80.

327 Botschaft zum HFG, BBl. 2009, S. 8086.

328 Botschaft zum HFG, BBl. 2009, S. 8086.

Im Zusammenhang mit dem DSG kommt der Einwilligung eine wichtige praktische Bedeutung zu,[329] selbst wenn der Nutzen der Einwilligung als Absicherung für die Sekundärnutzung aus den erläuterten Gründen[330] beschränkt ist. Der Einwilligung kommt aber auch im Anwendungsbereich des HFG eine zentrale Rolle zu. So ist bereits auf Verfassungsstufe[331] der Grundsatz vorgeschrieben, dass für jedes Forschungsvorhaben im Bereich der Humanmedizin eine Einwilligung der Teilnehmenden und eine hinreichende Aufklärung erforderlich ist. Das Gesetz kann Ausnahmen vorsehen, wobei eine Ablehnung in jedem Fall verbindlich ist. Diese Verfassungsregelung wurde im HFG und dessen Ausführungsverordnung konkretisiert.[332]

Wie bereits angesprochen, gilt es die Einwilligung in die originäre Erhebung der Daten für ein Forschungsprojekt, die z.B. im Zusammenhang einer medizinischen Behandlung erfolgen kann, von der Einwilligung in die Weiterverwendung bereits erhobener Daten zu unterscheiden. Auch wenn es, auch dank den nachfolgend zu erläuternden Vorschriften des HFG, unter bestimmten Voraussetzungen möglich ist, in einer einzigen Erklärung beide Einwilligungen einzuholen, dürfen diese nicht gleichgesetzt werden. Denn das HFG enthält unterschiedliche Regelungen für die beiden Einwilligungen.[333] In diesem Abschnitt geht es um die Einwilligung in die Teilnahme an einem Forschungsprojekt und die originäre Beschaffung der Daten. Auf die darauf aufbauenden Vorschriften zur Weiterverwendung von Daten wir unten in Abschnitt 4.2.4 eingegangen.

Damit die Einwilligung in die Teilnahme an einem Forschungsvorhaben gültig ist, ist erforderlich, dass sie von einer einwilligungsfähigen Person (bzw. bei Urteilsunfähigkeit ihre Stellvertretung) vor dem Eingriff freiwillig, gestützt auf hinreichende Information sowie nach angemessener Bedenkzeit, schriftlich erteilt wird.[334] Hinsichtlich der Freiwilligkeit ist im Humanforschungskontext bspw. zu vermeiden, dass die betroffene Person den Eindruck erhält, die Qualität ihrer medizinischen Behandlung hänge von einer Einwilligung in die Forschung ab. Ferner dürfen ihr gemäss Art. 14 HFG auch keine unrechtmässigen Vorteile im Gengenzug für eine Einwilligung versprochen werden. Darüber hinaus ist die Person darüber zu informieren, dass sie die Einwilligung verweigern bzw. jederzeit ohne die Angabe von Gründen widerrufen kann.[335]

Die Einwilligung hat grundsätzlich schriftlich zu erfolgen, wobei der Bundesrat Ausnahmen von der Schriftlichkeit vorsehen kann. Die Ausnahmen sind abschliessend in Art. 9 HFV aufgezählt, wobei strenge Anforderungen gestellt werden und schon aus Beweisgründen eine zumindest dokumentierte[336] Einwilligung empfehlenswert ist. Schriftlichkeit bedeutet nach der Lehre in Analogie zu Art. 13 ff. des Obligationenrechts (OR), dass die Einwilligung eigenhändigen vom Betroffenen bzw. Vertretungsbefugten datiert und unterschrieben wird.[337] Im Gegensatz dazu kann die Einwilligung gemäss DSG auch konkludent bzw. hat bei besonders

---

329 Vgl. dazu ausführlich BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, insb. auch Rz. 37.

330 Siehe dazu oben Abschnitt 4.1.4a)v.) iv.) und 4.1.4b) iii.) (d).

331 Art. 118b BV.

332 Vgl. insb. Art. 7 und Art. 16 ff. und HFG.

333 Vgl. Art. 16 ff. HFG im Unterschied zu Art. 32 ff. HFG.

334 Art. 16 HFG; SPRECHER/VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 16 Rz. 5.

335 Art. 8 Abs. 1 lit. b HFV; SPRECHER/VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 16 Rz. 13.

336 Z.B. durch unabhängige Zeugen oder audiovisuelle Aufnahmen, vgl. SPRECHER/VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 16 Rz. 24.

337 SPRECHER/VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 16 Rz. 23; Vgl. auch Art. 29 Abs. 1 Satz 1 EU VO Klinische Prüfungen sowie Ziff. 4.8.8 ICH GCP-Richtlinie.

schützenswerten Personendaten ausdrücklich zu erfolgen; Schriftlichkeit ist hingegen nicht erforderlich.[338] Auch wenn bei der Auslegung des Schriftformerfordernisses der Rückgriff auf die Regeln des OR nicht zwingend sind,[339] muss aufgrund der Entstehungsgeschichte zumindest davon ausgegangen werden, dass eine Unterschrift des Teilnehmenden verlangt ist.[340] Allerdings ist nicht von vornherein ausgeschlossen, dass auch eine digitale Signatur, bspw. auf einem Touch-Screen, ausreichen könnte, wobei hier Unsicherheit besteht und dies zur Zeit auch nicht der Praxis entsprechen dürfte.

Das strenge Schriftlichkeitserfordernis des HFG kann deshalb in der Praxis negative Auswirkungen haben. Bestätigt haben dies Erhebungen von 2017 zum Generalkonsent, der, wie noch erläutert wird,[341] für die Sekundärnutzung von grosser Bedeutung ist. Danach führte die zwingende Erteilung des Generalkonsents in Papierform dazu, dass nur 10-20 Prozent[342] der an einem Universitätsspital behandelten Patientinnen und Patienten überhaupt nach einer Einwilligung gefragt wurden.[343] Als Alterative für diese unflexible Ausgestaltung der (General-)Einwilligung wird in der Literatur häufig eine digitale dynamische Einwilligung verlangt.[344] Dieses Konzept sieht die Möglichkeit vor, über eine digitale Plattform in die Teilnahme an bestimmten Forschungsprojekten einzuwilligen bzw. die Einwilligung über die Plattform zu widerrufen.[345] Auch hier besteht Rechtsunsicherheit und entspricht zudem nicht der Praxis. Jedenfalls steht fest, dass die Verantwortlichen eine hinreichende Dokumentation der Aufklärung und Einwilligung sicherstellen müssen, was, gerade auch aufgrund der gelebten Umsetzung des Schriftformerfordernisses, mit erheblichem Aufwand verbunden ist.

Wichtig für die Gültigkeit der Einwilligung ist sodann die hinreichende Aufklärung. Die betroffene Person ist gemäss Art. 16 Abs. 2 HFG in verständlicher Form mündlich und schriftlich über folgende Punkte aufzuklären:

- Art, Zweck, Dauer und Verlauf des Forschungsprojekts;
- die voraussehbaren Risiken und Belastungen;
- den erwarteten Nutzen des Forschungsprojekts, insbesondere für sie oder für andere Personen;
- die Massnahmen zum Schutz der erhobenen Personendaten;

---

338 Vgl. BAERISWYL, in: BAERISWYL/PÄRLI (Hrsg.), Datenschutzgesetz, 2015, Art. 4 Rz. 54 ff.

339 Vgl. für das KVG BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 126 ff.: ihnen folgend Kreisschreiben des BAG Nr. 7.1, 20.12.2012, Aufsicht des BAG über datenschutzrelevante Bereiche gemäss KVAG 1, KVAV 2, KVG 3.

340 Botschaft zum HFG, BBl 2009 S. 8106 e contrario: "… nicht in der Lage ist zu *unterschreiben*".

341 Vgl. dazu nachfolgend Abschnitt 4.2.4d).

342 Eine neuere Studie zeigte, dass am Universitätsspital Zürich nur bei 48.7 Prozent der Studienteilnehmer überhaupt eine Aufforderung zur Erteilung eines Generalkonsents abgegeben wurde. Davon stimmten 79.7 % dem Generalkonsent zu und 20.2 Prozent lehnten diesen ab; GRIESSBACH/BAUER/LEBET, The concept of General Consent in Switzerland and the implementation at the University Hospital Zurich, a cross-sectional study, https://smw.ch/article/doi/smw.2022.w30159 (zuletzt aufgerufen am 12.7.2022).

343 JULIAN MAUSBACH, Dynamische Einwilligung zur Forschung am Menschen, in: Jusletter 28 Januar 2019, S. 9.

344 JULIAN MAUSBACH, Dynamische Einwilligung zur Forschung am Menschen, in: Jusletter 28 Januar 2019; RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 29.

345 JULIAN MAUSBACH, Dynamische Einwilligung zur Forschung am Menschen, in: Jusletter 28 Januar 2019, S. 3.

- ihre Rechte.

Diese gesetzlichen Mindestinformationen werden durch Art. 8 HFV ergänzt, sodass eine Vielzahl von Pflichtangaben resultiert. Dies erschwert die Einhaltung der weiteren Anforderung, dass die Informationen verständlich sein müssen.[346] Bereits aufgrund der Komplexität von medizinischen Forschungsaktivitäten und zahlreicher Fachbegriffe ist dieses Erfordernis in der Praxis nicht immer leicht umzusetzen. Es gelten auch hier hohe Anforderungen an die Spezifizität der Informationen, sodass bspw. eine Umschreibung des Zwecks eines Forschungsvorhabens mit "Krebsforschung" offensichtlich nicht ausreicht. Vielmehr ist das konkrete Forschungsziel und die zu beantwortende Forschungsfrage oder zu prüfenden Hypothesen anzugeben.[347]

Die Informationen sind der betroffenen Person in einer Art und Weise zu vermitteln, die diese nachvollziehen kann. Gemäss Botschaft zum HFG ist hierbei auf die Kenntnisse einer Person ohne besondere Fachkenntnisse abzustellen.[348] Art. 16 Abs. 2 HFG sieht nur vor, dass die Information in verständlicher Form zu erteilen ist, hingegen lässt die Bestimmung offen, ob die betroffene Person die Information auch tatsächlich verstanden hat.[349] Gemäss Art. 8 Abs. 4 HFV[350] hat jedoch die aufklärende Person durch geeignete Massnahmen sicherzustellen, dass die betroffene Person die wesentlichen Aufklärungsinhalte verstanden hat.[351] Dementsprechend ist grundsätzlich abstrakt auf das Verständnis des durchschnittlichen Laien abzustellen, jedoch durch weitere Massnahmen (bspw. Rückfragen, Zusammenfassung der wesentlichen Punkte, Fragenkataloge)[352] sicherzustellen, dass die konkret betroffene Person die wesentlichen Punkte auch verstanden hat. Der Massstab an die Verständlichkeit ist dementsprechend strenger als jener des DSG, welches auf das abstrakte Begriffsverständnis einer durchschnittlichen, verständigen Person aus dem Zielpublikum abstellt.[353]

Darüber hinaus verlangt Art. 17 HFG, dass bereits im Zeitpunkt der Entnahme des biologischen Materials bzw. der Erhebung der Gesundheitsdaten über beabsichtigte Sekundärnutzungen informiert wird. Daraus folgt zugleich, dass die Einholung der Einwilligung im Zusammenhang mit der Behandlung oder Probenentnahme zulässig und möglich sein muss, soweit den Anforderungen an die hinreichende Information entsprochen werden kann, also namentlich bereits genügend Angaben zum Vorhaben bekannt sind. Ausgeschlossen ist damit, anders als von den EU-Behörden vertreten,[354] die pauschale Verneinung der Gültigkeit der Einwilligung, wenn eine Patientin oder ein Patient in einem schlechten Gesundheitszustand ist bzw. ein Ungleichgewicht herrsche. Gleichwohl benötigt es hier im Einzelfall einer Beurteilung, ob die betroffene Person

---

346 Art. 16 Abs. 2 HFG.

347 SPRECHER/VAN SPYK, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 16 Rz. 23.

348 Botschaft zum HFG, BBl.2009 S. 8106.

349 BAERISWYL, in: BAERISWYL/PÄRLI (Hrsg.), Datenschutzgesetz, 2015, Art. 4 Rz. 38.

350 So auch Art. 7 Abs. 4 KlinV.

351 BAERISWYL, in: BAERISWYL/PÄRLI (Hrsg.), Datenschutzgesetz, 2015, Art. 4 Rz. 38.

352 BAERISWYL, in: BAERISWYL/PÄRLI (Hrsg.), Datenschutzgesetz, 2015, Art. 4 Rz. 40.

353 BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Rz. 57; Vgl. in diesem Punkt auch ROSENTHAL, Art. 4 N 74.

354 EDSA, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO) (Artikel 70 Absatz 1 Buchstabe b), 23.1.2019, Rz. 20.

in ihrem jeweiligen Gesundheitszustand in der Lage ist, die erteilten Informationen zu verstehen bzw. eine freiwillige Einwilligung abgeben kann.

Ein weiterer Punkt mit Bezug zum Inhalt der Aufklärung betrifft die Frage, wer überhaupt für das Forschungsprojekt und die damit verbundenen Datenbearbeitungen verantwortlich ist. Erstaunlicherweise wird nur in den besonderen Vorschriften für klinische Versuche explizit die Angabe des Sponsors, also der für die Veranlassung eines klinischen Versuchs in der Schweiz verantwortlichen Person[355], verlangt.[356] Ausserhalb von deren Anwendungsbereich ist nur die Hauptfinanzierungsquelle eine ausdrückliche Pflichtangabe, die diese Stossrichtung aufweist. Aus dem Blickwinkel des Datenschutzrechts darf jedoch bezweifelt werden, ob dies ausreicht und insofern von einer abschliessenden Regelung ausgegangen werden kann, welche die bereichsübergreifenden Vorschriften der Datenschutzgesetze verdrängt. Denn die Angabe des für die Datenbearbeitung Verantwortlichen ist zumindest im DSG eine der zentralen Pflichtangaben. Es müsste deshalb davon ausgegangen werden, dass auch diese Angabe, also zumindest die Kategorien[357] der involvierten Sponsoren/Veranlasser (z.B. Pharmaunternehmen) und/oder Prüfpersonen zu den Pflichtangaben des HFG zu zählen ist, welche insoweit im Lichte der Bestimmungen des DSG auszuglegen ist. Selbst wenn man aber eine solche Auslegung ablehnt, verbleibt zumindest auch in dieser Hinsicht eine Rechtsunsicherheit.

Ferner muss die betroffene Person, wie erwähnt, auch über ihre Rechte informiert werden. Hierzu gehört namentlich die Aufklärung über ihr Recht, die Einwilligung ohne Begründung zu verweigern oder zu widerrufen.[358] Zur hinreichenden Information zählt dabei auch die Aufklärung über die Konsequenzen eines Widerrufs der Einwilligung auf die weitere Verwendung des bis zum Widerruf gesammelten biologischen Materials und der bis zum Widerruf erhobenen Personendaten.[359] Auch auf diese Konsequenzen wird zurückzukommen sein.[360]

Aus all diesen Teilaspekten ergeben sich somit hohe Anforderungen an die Einholung gültiger Einwilligungen. In der Praxis führt dies zur Notwendigkeit, Abläufe und Systeme zu implementieren, die nicht nur sicherstellen, dass eine gültige Einwilligung eingeholt wird im erforderlichen Umfang, sondern auch, dass die Gültigkeit und Reichweite dokumentiert und nachweisbar ist. Dabei sind auch die Rechte der betroffenen Personen zu berücksichtigen und es gilt auch technisch sicherzustellen, dass bspw. ein Widerruf der Einwilligung umgesetzt werden kann.

ii.) Verhältnis zu den Anforderungen an die Einwilligung im DSG

Erstaunlicherweise wird, soweit ersichtlich, weder in der Entstehungsgeschichte noch in der Lehre bislang ausführlich Stellung dazu genommen, in welchem Verhältnis die Vorgaben des HFG an die Einwilligung zu denjenigen des DSG stehen. Auch wenn, wie bereits erläutert, im Wesentlichen von einem Vorrang des HFG vor dem DSG auszugehen ist, gilt dies nur für Bereiche und Vorschriften, die als abschliessend zu qualifizie-

355 Vgl. Art. 2 lit. d KlinV.

356 Art. 7 Abs. 1 lit. h KlinV; Art. 3 Abs. 1 lit. b KlinV-Mep i.V.m. Art. 7 Abs. 1 lit. h KlinV.

357 Vgl. zur Frage, ob die blosse Angabe von Kategorien von Verantwortlichen unter dem DSG ausreicht, Bühlmann/Schüepp, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 88.

358 Art. 8 Abs. 1 lit. b HFV.

359 Art. 8 Abs. 1 lit. c HFV.

360 Vgl. dazu nachfolgend Abschnitt 4.2.4f).

ren sind. In Bezug auf die Anforderungen an die Einwilligung und das Transparenzgebot spricht die Ausführlichkeit der Sonderregelung für den abschliessenden Charakter. Gleichwohl handelt es sich bei der Einwilligung in die Teilnahme an einem Forschungsprojekt und der Einwilligung in eine Datenbearbeitung um verschiedene Aspekte, liegt doch der Schwerpunkt bei Ersterer auch auf ethischen Gesichtspunkten.

Gleichwohl ist eine Haltung, wie sie von den EU-Datenschutzbehörden vertreten wird,[361] abzulehnen, wonach die beiden Einwilligungen losgelöst voneinander zu prüfen sind. Hierfür erscheinen die Parallelen zu gross und die beiden Einwilligungen können nicht ein völlig voneinander unabhängiges Schicksal haben. Insbesondere kann es bereits aus praktischen Gründen nicht angehen, eine Teilnahme an einem Forschungsvorhaben gestatten zu müssen, ohne aber – mangels datenschutzrechtlich gültiger Einwilligung der Teilnehmenden – die damit sinnvollerweise verbundenen Datenbearbeitungen durchführen zu können. Wo aber die Grenzen einer solchen Koppelung zwischen Teilnahme und Datenbearbeitung sind, beantwortet das HFG nicht direkt. Es wird deshalb hier, wie auch in den weiteren erläuterten Teilaspekten der Einwilligung, darauf hinauslaufen müssen, bei der Auslegung der Anforderungen des HFG an die Einwilligung ergänzend auf die Grundsätze des DSG zurückzugreifen.[362] Geht es somit bspw. um die Beurteilung, ob die Informationen zu den mit einem Forschungsvorhaben verbundenen Datenbearbeitungen verständlich sind, wäre hierfür, zumindest nach der hier vertretenen Auffassung, auf die unter dem DSG entwickelten Kriterien abzustellen, also ein objektiver Massstab anzuwenden.[363] Mangels verbindlicher Klarstellungen durch den Gesetzgeber oder die Rechtsprechung sind die Einzelheiten rund um das Verhältnis zu den Bestimmungen des DSG ungeklärt.

4.2.4 Besondere Anforderungen des HFG für die Sekundärnutzung

Neben den erläuterten allgemeinen Vorschriften des HFG sind die besonderen Vorgaben in den Artikeln 32 – 35 HFG für die Sekundärnutzung von Gesundheitsdaten von grundlegender Bedeutung, enthalten diese doch die Kernanforderungen für die Weiterverwendung von biologischem Material bzw. gesundheitsbezogenen Personendaten für Forschungszwecke. Bevor näher auf die konkreten Vorgaben, insbesondere die unterschiedlichen Anforderungen an die Einwilligung der Teilnehmenden eingegangen wird, muss geklärt werden, was unter der "Weiterverwendung" i.S.d. HFG zu verstehen ist.

a) Begriff der Weiterverwendung ("Secondary Use")

Die Weiterverwendung wird im HFG selbst nicht definiert, jedoch enthält Art. 24 HFV eine Konkretisierung des Begriffs. Demzufolge ist unter der Weiterverwendung von biologischem Material und gesundheitsbezogenen Personendaten "jeder Umgang zu Forschungszwecken mit bereits entnommenem biologischem Material beziehungsweise mit bereits erhobenen Daten" zu verstehen.[364] Insbesondere gelten folgende Aktivitäten zu Forschungszwecken als Weiterverwendung:

---

361 Vgl. EDSA, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO) (Artikel 70 Absatz 1 Buchstabe b), 23.1.2019, Rz. 15 ff.

362 BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 28 ff.

363 Vgl. dazu ausführlich BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 57 ff.

364 Art. 24 HFV.

- das Beschaffen, Zusammenführen oder Sammeln biologischen Materials oder gesundheitsbezogener Personendaten;
- das Registrieren oder Katalogisieren biologischen Materials oder gesundheitsbezogener Personendaten;
- das Aufbewahren oder Erfassen in Bio- oder Datenbanken;
- das Zugänglichmachen, Bereitstellen oder Übermitteln biologischen Materials oder gesundheitsbezogener Personendaten.[365]

Der Definition zufolge setzt das Weiterverwenden grundsätzlich nur voraus, dass das biologische Material bzw. die Gesundheitsdaten bereits entnommen bzw. erhoben wurde. Es besagt nicht, zu welchem Zweck dies geschah, sondern nur, dass mit der hier definierten und von Art. 32 ff. HFG erfassten Weiterverwendung lediglich solche Weiterverwendungen gemeint sind, die zu Forschungszwecken[366] vorgenommen werden. Wozu und wie die ursprüngliche Erhebung erfolgte, wird nicht thematisiert. Die Definition stellt nur darauf ab, dass die Daten bzw. das Material bereits vorhanden sind.[367] Die Erhebung kann deshalb z.B. im Behandlungskontext oder im Rahmen eines spezifischen Forschungsprojekts erfolgt sein.[368] Wie erwähnt, spielt aber keine Rolle, wie die Erhebung konkret erfolgt war. Deshalb kann, muss es sich hier aber nicht um Fälle handeln, die unter dem DSG eine Zweckänderung darstellen und gegen das erläuterte Zweckbindungsgebot[369] verstossen würden.[370] Es kann sich ebenfalls um Fälle handeln, wie sie in Art. 17 HFG geregelt sind, in denen zwar die Daten bzw. das biologische Material gleichwohl in einem anderen Kontext (z.B. zu Behandlungszwecken) erhoben werden, jedoch die betroffene Person bereits im Zeitpunkt der Entnahme bzw. der Erhebung über die (spätere) Weiterverwendung zu Forschungszwecken informiert wird und seine Einwilligung erteilt.[371]

Die Regelung zur Weiterverwendung trägt insofern aber der mit der Weiterverwendung möglicherweise verbundenen Zweckänderung Rechnung. Wie noch zu zeigen ist, erfordert die Weiterverwendung nach den Art. 32 ff. HFG gerade auch deshalb eine Einwilligung (oder mindestens ein Ausbleiben eines Widerspruchs nach erfolgter Information).

Ausgehend davon ist, wie erläutert, die Einhaltung des Zweckbindungsgebots des DSG im Anwendungsbereich des HFG nicht mehr gesondert zu prüfen. Unklar ist jedoch namentlich, inwiefern dies auch für den Bearbeitungsgrundsatz der Rechtmässigkeit gilt. Dieser besagt ja unter anderem, dass jede Weiterverwendung von Daten, die unrechtmässig erhoben wurden, ebenfalls im Grundsatz unrechtmässig ist. Übertragen auf

---

365 Art. 24 HFV.

366 Keine von Art. 32 ff. HFG erfasste Weiterverwendung liegt demnach vor, wenn diese bspw. zu Behandlungszwecken (also zur Dokumentation in der Krankengeschichte) oder im Rahmen der Qualitätssicherung erfolgen soll, vgl. Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 69.

367 Vgl. Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 69.

368 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 69; RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32-35 Vorbemerkungen Rz. 4.

369 Vgl. dazu oben Abschnitt 4.1.4a).

370 Vgl. auch RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32-35 Vorbemerkungen Rz. 4.

371 Vgl. auch RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32-35 Vorbemerkungen Rz. 5.

die Regelung in Art. 32 ff. HFG ist deshalb fraglich, ob bei Einhaltung der darin festgelegten Anforderungen, also z.B. bei Vorliegen eines gültigen Generalkonsents, auch solche Daten oder Materialien weiterverwendet werden dürfen, die (ursprünglich) unter Verstoss gegen die Vorschriften des HFG oder des DSG erhoben wurden. Mit anderen Worten ist offen, ob die Art. 32 ff. HFG Verstösse gegen datenschutzrechtliche Vorschriften, die bei der Erhebung begangen wurden, "heilen" oder rechtfertigen können, wie dies im DSG für die privaten Verantwortlichen der Fall ist. Nach der hier vertretenen Auffassung ist dies zu verneinen, bereits aus Gründen der Gesetzessystematik, stellt das HFG, wie erläutert, sowohl Anforderungen (insb. die Einwilligung) an die (originäre) Beschaffung als auch die Weiterverwendung, ohne einen solchen Bezug herzustellen.

Es ist somit davon auszugehen, dass der Regelung in Art. 32 ff. HFG das Verständnis zugrunde liegt, dass die originäre Erhebung der Daten, die weiterverwendet werden sollen, bereits rechtmässig erfolgt war.[372] War die Erhebung der Daten unrechtmässig, ist es auch deren Weiterverwendung zu Forschungszwecken, selbst wenn die Vorgaben von Art. 32 ff. HFG eingehalten werden. In aller Regel wird die Beurteilung jedoch zusammenfallen: Ist die Einwilligung für die Erhebung ungültig, wird sie auch für die Weiterverwendung nicht wirksam sein. Die beiden Einwilligungen sind jedoch denklogisch zu trennen. Hieraus ergibt sich im Grundsatz ein weiterer Aspekt der Unsicherheit, der seinen Ursprung im ungeklärten Verhältnis zwischen dem HFG und den sektorübergreifenden Datenschutzgesetzen hat.

b) Übersicht: Anforderungen für die Sekundärnutzung der verschieden Datenarten

Für die nachfolgende Darstellung der besonderen und wichtigen Anforderungen an die Sekundärnutzung gilt es nochmals kurz die Ausgangslage zusammenzufassen: Sollen Daten aus einem Forschungsvorhaben für weitere Forschungszwecke weiterverwendet werden, bedarf dies, wie auch die Teilnahme am Forschungsvorhaben, in der Regel einer Einwilligung. Wie gesehen, kann diese zwar mitunter auch gleichzeitig mit der Zustimmung zu einer Behandlung oder Entnahme von Material erteilt werden. Gleichwohl sind die beiden Einwilligungen zu unterscheiden.

Es gelten grundsätzlich auch für die Einwilligung in die Weiterverwendung die oben erläuterten allgemeinen Anforderungen an die Erteilung einer Einwilligung in die Teilnahme an Forschungsprojekten. Die Regelung in Art. 32 ff. HFG verweist denn auch auf diese allgemeinen Vorschriften, welche zumindest sinngemäss gelten sollen. Die Art und Tragweite der Einwilligung in die Sekundärnutzung und die zu erteilenden Informationen sind aber jeweils abhängig von der erhobenen Datenart.[373] Das HFG nimmt dementsprechend eine Kategorisierung unter den Gesundheitsdaten vor und erkennt diesen ein unterschiedliches Schutzniveau zu. Ferner wird zwischen verschlüsselten und unverschlüsselten Daten bzw. genetischem Material differenziert. Konkret wird unterschieden zwischen folgenden Nutzungen und damit verbundenen Anforderungen:

---

[372] Im Ergebnis wohl ebenfalls so RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32-35 Vorbemerkungen Rz. 4 ("*die Daten bereits vorhanden sind, also bereits vorgängig (mit der entsprechend notwendigen Rechtfertigung) zu einem anderen Zweck entnommen bzw. erhoben worden sind*").

[373] Art. 32 und 33 HFG.

Biologisches Material und genetische Daten in unverschlüsselter Form	Gewöhnliche Einwilligung für ein konkretes Forschungsprojekt ("Informed Consent")
Biologisches Material und genetische Daten in verschlüsselter Form	Generalkonsent für Forschungszwecke ("Broad Consent")
Nichtgenetische gesundheitsbezogene Personendaten in unverschlüsselter Form	
Nichtgenetische gesundheitsbezogene Personendaten in verschlüsselter Form	Widerspruchsrecht ("Opt-Out")
Anonymisierung von biologischem Material und genetische Daten zu Forschungszwecken	

In Ausnahmefällen können Gesundheitsdaten und biologisches Material auch ohne das Vorliegen der oben angeführten Voraussetzungen (Einwilligung oder Belehrung über das Widerspruchsrecht) im Rahmen der sogenannten "Escape Clause" des Art. 34 HFG zu Forschungszwecken weiterverwendet werden. Hierfür bedarf es jedoch unter anderem eine Bewilligung der zuständigen Ethikkommission.[374]

c) Gewöhnliche Einwilligung ("Informed Consent")

Den strengsten Anforderungen unterliegt die Weiterverwendung von biologischem Material und genetischen Daten in unverschlüsselter Form. Für die Weiterverwendung zu Forschungszwecken dieser Daten muss bei der Erhebung eine gewöhnliche informierte Einwilligung ("informed consent") für das spezifische Forschungsprojekt eingeholt werden.[375] Obwohl das Gesetz von der Einwilligung für "*ein* Forschungsprojekt" spricht, ist, wie auch unter dem Zweckbindungsgebot des DSG anzunehmen, dass auch die Einwilligung in mehrere Forschungsprojekte möglich ist, solange all diese in Bezug auf alle Pflichtangaben hinreichend konkret umschrieben werden (können).[376] Sollen die unverschlüsselten Daten im Zuge eines anderen – nicht von der ursprünglichen Einwilligung umfassten – Forschungsprojektes weiterverwendet werden, muss demzufolge eine neue Einwilligung für die spezifischen Zwecke des neuen Forschungsprojekts eingeholt werden.

In der Botschaft zum HFG wird darauf hingewiesen, dass mit der Weiterverwendung von biologischem Material bzw. von gesundheitsbezogenen Personendaten für die Forschung oftmals eine Offenbarung des Berufsgeheimnisses verbunden[377] ist. Deswegen ist es empfehlenswert, gleichzeitig mit der Einholung der Einwilligung bzw. der Information über das Widerspruchsrecht, um Entbindung vom Berufsgeheimnis zu ersuchen.[378]

Sofern die Bearbeitung in unverschlüsselter Form nicht unbedingt notwendig ist, um die angestrebten Forschungsziele zu erreichen, kann sich eine Weiterverwendung der Daten bzw. des biologischen Materials in verschlüsselter oder anonymisierter Form aufdrängen. Einerseits kann dies aus Gründen der Verhältnismässigkeit geboten sein, d.h. aufgrund der möglichen ergänzenden Anwendung der entsprechenden Grundsätze

[374] Vgl. dazu oben Abschnitt 4.2.3a).

[375] Art. 32 Abs 1 HFG.

[376] Vgl. auch RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 6.

[377] Botschaft zum HFG, BBl 2009 S. 8121; Art. 321 und 321bis StGB.

[378] Botschaft zum HFG, BBl 2009 S. 8121; Art. 321bis StGB i.V.m. Art. 34 HFG.

der sektorübergreifenden Datenschutzgesetze, und andererseits hat dies auch praktische Vorteile, da ein nachfolgend zu erläuternder Generalkonsent für Forschungszwecke im Allgemeinen ausreichend ist.

d) Generalkonsent ("Broad Consent")

Der "Generalkonsent" ist von grosser praktischer Bedeutung.[379] Anders als unter dem DSG mit den strengen Anforderungen an die Information über die Bearbeitungszwecke erlaubt das HFG in bestimmten Konstellationen eine weniger präzise und letztlich generische Umschreibung von Zwecken, die mehrere noch unbestimmte Forschungsvorhaben umfassen kann. Mit dem Generalkonsent kann insofern eine sehr breit gefasste Einwilligung ("broad consent") für die Weiterverwendung von Gesundheitsdaten zu Forschungszwecken eingeholt werden. Dies ist jedoch beschränkt auf zwei Arten von Sekundärnutzungen:

1. die Sekundärnutzung von verschlüsseltem biologischem Material und genetische Daten,

2. die Sekundärnutzung von unverschlüsselten (nichtgenetischen) gesundheitsbezogenen Daten.

In diesen Fällen müssen das konkrete Forschungsprojekt bzw. die damit verfolgten Zwecke nicht näher konkretisiert werden. Bei der erstgenannten Sekundärnutzung stellen sich wiederum die bereits angesprochenen Fragen, wann (rechtlich) und wie (technisch) eine hinreichende Verschlüsselung gewährleistet ist.[380]

Ein gültiger Generalkonsent setzt ferner gleichwohl voraus, dass aus der Einwilligung klar hervorgeht, dass die betroffene Person generell für die Verwendung zu Forschungszwecken einwilligt und dass ihr bewusst gemacht wird, dass über die künftige Verwendung in konkreten Forschungsprojekten nicht mehr informiert und dafür keine erneute Einwilligung notwendig ist.[381] Der Generalkonsent kann deshalb auch die Ablage von verschlüsseltem biologischem Material oder genetischen Daten bzw. von (unverschlüsselten) Gesundheitsdaten in einer Biobank rechtfertigen, sofern die Biobank einem Reglement untersteht, welches nur Forschung i.S.d. HFG zulässt.[382]

Des Weiteren ist aber trotz Aufzählung der Pflichtinhalte in der HFV[383] nicht restlos klar, wie die Aufklärung konkret ausformuliert sein muss, damit von einem wirksamen Generalkonsent auszugehen ist. Dies gilt namentlich auch mit Blick auf die geschilderten Anforderungen an die Verständlichkeit, die bezogen auf die einzelnen Teilnehmenden und deren Besonderheiten sichergestellt werden müsste. Ferner sind auch die einzelnen Pflichtinhalte auslegungsbedürftig, wie namentlich die erforderliche Aufklärung über die Massnahmen zum Schutz der Personendaten, wo unklar bleibt, was konkret, in welchem Detaillierungsgrad zu erläutern ist. Es stellen sich ferner auch hier die Fragen nach dem Verhältnis zu den Vorgaben der DSG. In diesem Zusammenhang ist zumindest davon auszugehen, dass die (Kategorien der) datenschutzrechtlichen Verantwortlichen der künftigen Forschungsprojekte nicht anzugeben sind. Verlangt ist insofern lediglich die Angabe, dass die Daten an Dritte weitergegeben werden können.[384] Darüber hinaus sind allerdings weiterhin einige

---

379 Art. 17 HFG.

380 Vgl. dazu oben Abschnitt 3.2.7.

381 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 18; BAERISWYL, "Generaleinwilligung" bei Biobanken, digma 2013 S. 90 ff.

382 BAERISWYL, "Generaleinwilligung" bei Biobanken, digma, 2013, S. 90 ff.

383 Vgl. Art. 29 und Art. 31 HFV.

384 Art. 29 Abs. 1 lit. d und Art. 31 Abs. 1 lit. e HFV.

wichtige Punkte, z.B. ob die jeweiligen Länder der Dritten wie im DSG[385], ebenfalls bekannt zu geben sind, offen.

Dies ist umso bedauerlicher als die Weiterverwendung von biologischem Material und Gesundheitsdaten mittels Generalkonsent für die biomedizinische Forschung eine grosse praktische Rolle spielt. In vielen Spitälern wird die Generaleinwilligung standardmässig über ein Eintrittsformular oder im Zuge der klinischen Behandlung eingeholt. Die Schweizerische Akademie der Medizinischen Wissenschaften (SAMW) hat hierzu gemeinsam mit der swissethics eine Vorlage für die Einholung eines Generalkonsents erarbeitet.[386] Auf Grundlage dieser Vorlage haben die schweizerischen Universitätsspitäler eine zweite harmonisierte Vorlage zum Generalkonsent erarbeitet, die von den fünf Universitätsspitälern verabschiedet und vom Vorstand der swissethics genehmigt wurde.[387] Diese gemeinsame Vorlage wird zwar als Meilenstein betrachtet, jedoch gelang es, wohl gerade auch in Anbetracht der geschilderten Unklarheiten, nicht, eine einheitliche schweizweite Lösung (für alle Spitäler) zu schaffen.[388]

In der Vorlage wird innerhalb der ersten eineinhalb Seiten kurz die notwendige Information zusammengefasst.[389] Von der Einwilligung sind demnach Daten und biologisches Material – das nicht mehr für Behandlungszwecke benötigt wird – umfasst, die bereits im Spital erhoben wurden oder zukünftig erhoben werden. Darüber hinaus wird die betroffene Person darüber informiert, dass nur berechtigte Mitarbeiter des Spitals Zugriff auf unverschlüsselte Daten erhalten und die Daten bzw. das Material vor der Weitergabe an die Forschung verschlüsselt oder anonymisiert wird. In diesem Zusammenhang wird die Verschlüsselung und die Anonymisierung umschrieben und zugesichert, dass der zugehörige Schlüssel (im Falle der Pseudonymisierung) von einer Person verwahrt wird, die nicht am jeweiligen Forschungsprojekt beteiligt ist. Ferner wird der Empfängerkreis der de-identifizierten Daten umschrieben, welcher z.B. Forschende des behandelnden Spitals, anderer Spitäler, Universitäten oder pharmazeutischen Unternehmen umfasst. Zudem wird die Patientin oder der Patient über die Freiwilligkeit der – zeitlich unbegrenzten – Einwilligung und die jederzeitige Widerrufbarkeit dergleichen informiert. Auf der dritten und letzten Seite der Vorlage werden sodann die wichtigsten Punkte in Bulletpoints zusammengefasst und die schriftliche Einwilligung der teilnehmenden Patientin oder des teilnehmenden Patienten eingeholt.

Der beschriebene Versuch, die Einholung der Generaleinwilligung zu standardisieren, ist jedenfalls begrüssenswert. Allerdings würde erst durch ein schweizweit in allen Spitälern verwendetes – von offizieller Stelle verbindlich bewilligtes – Formular die erforderliche Rechtsicherheit schaffen. Bis dahin müssen bei der Durchführung von prospektiven Forschungsprojekten mit Daten aus verschiedenen Spitälern die Gültigkeit und Reichweite der jeweiligen Einwilligungen vorab einzeln geprüft werden, was nicht nur enorm aufwändig ist, sondern auch mit Unsicherheiten verbunden ist.[390] Eine informelle Abstimmung aller Spitäler blieb bisher

---

385 Vgl. Art. 19 Abs. 4 nDSG.

386 BAUR, Personalisierte Medizin im Recht, Humanforschung—- Quo vadis?, 2019, S. 315; Website Akademien der Wissenschaften Schweiz: https://www.samw.ch/de/Ethik/Themen-A-bis-Z/Generalkonsent.html (zuletzt aufgerufen am 18.05.2022).

387 Vgl. Website Universitäre Medizin Schweiz: https://www.unimedsuisse.ch/de/projekte/generalkonsent (zuletzt aufgerufen am 18.05.2022).

388 Vgl. Website Universitäre Medizin Schweiz: https://www.unimedsuisse.ch/de/projekte/generalkonsent (zuletzt aufgerufen am 18.05.2022).

389 Vorlage zum Generalkonsent 2019/2, vgl. Website Universitäre Medizin Schweiz https://www.unimedsuisse.ch/application/files/8815/5082/4588/Vorlage_GK_2019_2_D_def.pdf; das Zitat bezieht sich auf den gesamten Absatz.

390 Vgl. DONZALLAZ, Traité de droit médical—- Volume II, Le médecin et les soignants, Bern 2021, Rz. 6247.

erfolglos, dementsprechend wäre eine staatliche Initiative für ein einheitliches und rechtssicheres Generalkonsentformular zu begrüssen.

e) Widerspruchsrecht

Verschlüsselte nichtgenetische Gesundheitsdaten können zu Forschungszwecken weiterverwendet werden, sofern die betroffene Person – nach entsprechender Information – nicht von ihrem Widerspruchsrecht Gebrauch macht.[391] Art. 32 Abs. 3 HFG sieht ferner auch im Falle der Anonymisierung von biologischem Material und genetischen Daten zu Forschungszwecken ein Widerspruchsrecht vor. Auch in diesem Fall muss die betroffene Person vorab über die Bearbeitung zu Zwecken der Anonymisierung hinreichend informiert werden.[392] Neben den Vorgaben zur Gewährleistung des Widerspruchsrechts stellt sich bei diesen Fallkonstellationen jeweils auch die Frage, wann (rechtlich) und wie (technisch) eine hinreichende Verschlüsselung oder Anonymisierung gewährleistet ist. Diesbezüglich sei auf die einleitenden Erläuterungen verwiesen.[393]

Die Verordnung enthält die Liste der Pflichtangaben für eine hinreichende Aufklärung über das Widerspruchsrecht,[394] wobei sich auch hier die Frage stellt, ob nicht weitere Elemente aufgrund der ergänzenden Anwendung der Datenschutzgesetze notwendig sind. In Bezug auf den Zweck genügt aber, wie beim Generalkonsent, eine breite generische Umschreibung mit «Forschungszwecken». Die Information kann sodann zwar schriftlich oder mündlich erfolgen, jedoch wird in der Praxis der erforderliche Nachweis der Aufklärung (und des ausgebliebenen Widerspruchsrechts) faktisch nur mit schriftlicher Dokumentation erbracht werden können.[395] Schwierigkeiten stellen sich auch beim Nachweis, dass die Information von der betroffenen Person zur Kenntnis genommen werden konnte, sodass sich oftmals gleichwohl eine Unterzeichnung aufdrängt und der Vorgang damit einer Einwilligung gleichkommt.

Wie in den Abschnitten 4.2.1b) beschrieben, ist das HFG grundsätzlich zwar nicht auf korrekt anonymisierte Daten bzw. biologisches Material anwendbar, jedoch stellt die Anonymisierung selbst eine Datenbearbeitung im Anwendungsbereich des HFG dar. Ein Widerspruch ist in diesem Fall nur solange möglich, bis die Daten anonymisiert sind, danach ist dies naturgemäss nicht mehr möglich, weil der jeweilige Datensatz nicht mehr der betroffenen Person zugeordnet werden kann.[396]

Der Widerspruch als solcher muss schliesslich nicht unbedingt bereits im Zeitpunkt der Datenerhebung erfolgen. Wird der Weiterverwendung zu Forschungszwecken erst später widersprochen, entfaltet sie dieselbe Wirkung wie ein Widerruf der Einwilligung,[397] worauf im nachfolgenden Abschnitt näher eingegangen wird.

---

391 Art. 33 Abs. 2 HFG.

392 Art. 32 Abs. 3 HFG.

393 Vgl. dazu oben Abschnitte 3.2.6 und 3.2.7.

394 Art. 30 und 32 HFV.

395 Vgl. auch RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 29.

396 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 29.

397 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 33 Rz. 17; mehr zur Wirkung des Widerrufs unterhalb.

f) Wirkung des Widerrufs der Einwilligung

Die Einwilligung für die Weiterverwendung der erhobenen Gesundheitsdaten bzw. des genetischen Materials zu Forschungszwecken (bzw. in ein konkretes Forschungsprojekt) kann jederzeit ohne die Angabe von Gründen widerrufen werden.[398] Bei der Beurteilung der Wirkung des Widerrufs ist zu unterscheiden, ob das Material oder die Daten für künftige Forschungszwecke aufbewahrt werden (bspw. in einer Biobank) oder bereits im Zuge eines Forschungsprojekts im Einsatz sind.[399] Denn im Grundsatz sind Daten bzw. das Material nach einem Widerruf zu löschen oder zu anonymisieren. Dieser Grundsatz wird jedoch aufgrund des Vertrauens der Forscher, bereits erhobene Daten (entsprechend der erteilten Einwilligung) auch auswerten zu können, eingeschränkt.[400]

Werden das Material bzw. die Daten deshalb nur für zukünftige Forschung aufbewahrt, dann dürfen sie ab dem Zeitpunkt des Widerrufs nicht mehr in Forschungsprojekten verwendet werden.[401] Sind die Daten demgegenüber im Zeitpunkt des Widerrufs im Rahmen eines Forschungsprojektes in Verwendung, müssen diese gleichwohl nicht umgehend gelöscht oder anonymisiert werden, sondern erst nach Abschluss der Auswertung. Denn die Entfernung der Daten wäre in diesem Fall nach Ansicht des Verordnungsgebers aus Gründen der Datenvalidität und damit der Wissenschaftlichkeit des Versuchs ein gravierender und unverhältnismässiger Eingriff in die Forschungstätigkeit.[402]

Dementsprechend erlaubt es Art. 10 HFV die Auswertung der entsprechenden Daten abzuschliessen.[403] Anschliessend müssen die Daten bzw. das biologische Material jedoch anonymisiert werden.[404] Die Anonymisierung kann unterbleiben und die Daten weiterhin für das Forschungsprojekt weiterbearbeitet werden, wenn die widerrufende Person ausdrücklich darauf verzichtet oder zu Beginn des Forschungsprojektes feststeht, dass eine Anonymisierung nicht möglich ist und die betroffene Person hinreichend darüber aufgeklärt wurde.[405]

Wie bereits beschrieben, ist bei diesen Widerrufskonstellationen wiederum fraglich, wie die korrekte Anonymisierung – insbesondere von genetischen Daten und biologischem Material – konkret umzusetzen ist.[406]

g) "Escape Clause"

Für Fälle, in denen den Anforderungen von Art. 32 und 33 HFG nicht entsprochen werden kann, also keine Einwilligung eingeholt oder nicht über das Widerspruchsrecht informiert werden kann, sieht das HFG eine sogenannte "Escape Clause" vor. Diese ermöglicht es auch in diesen Konstellationen, biologisches Material

---

398 Art. 7 Abs. 2 HFG.

399 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 11.

400 Vgl. Art. 10 Abs. 1 HFG.

401 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 12.

402 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 13; Art. 9 KlinV; Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 19 f.

403 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 32 Rz. 13; Botschaft zum HFG, BBl 2009 S. 8099.

404 Art. 10 Abs. 1 HFV; Art. 9 Abs. 1 KlinV.

405 Art. 10 Abs. 2 lit a und b bzw. Art. 9 Abs. 2 lit a und b KlinV.

406 Vgl. Abschnitt 3.3.6.

bzw. Gesundheitsdaten für Forschungszwecke weiterzuverwenden.[407] Laut Botschaft soll Art. 34 HFG nur in "bestimmten, eng umgrenzten Ausnahmefällen" zur Anwendung kommen, in denen es gerechtfertigt ist, dem Forschungsinteresse den Vorrang zu geben.[408] Diese Bestimmung war in der parlamentarischen Debatte nicht unumstritten, da sie im Widerspruch zum grundsätzlichen Vorrang der Individualinteressen der betroffenen Person steht.[409] Die Escape Clause ist nur anwendbar, wenn es "unmöglich oder unverhältnismässig schwierig ist, die Einwilligung einzuholen beziehungsweise über das Widerspruchsrecht zu informieren, oder dies der betroffenen Person nicht zugemutet werden kann".[410] Es sind deshalb folgende drei alternativen Konstellationen denkbar:

1. Fälle, in denen eine Kontaktaufnahme zu der betroffenen Person oder ihren Angehörigen gänzlich unmöglich ist, sind in der Praxis wohl eher selten.[411] In der Botschaft werden hier bspw. Fälle genannt, in denen die betroffene Person verstorben[412] ist und diese keine Angehörigen hat bzw. diese nicht kontaktiert werden können.[413]

2. Unverhältnismässigkeit der Einwilligung liegt dagegen vor, wenn der Aufwand für die Kontaktaufnahme so hoch ist, dass er ungerechtfertigt erscheint. Laut Botschaft kann dies beispielsweise der Fall sein, wenn die zu kontaktierenden Personen nur äusserst schwer auffindbar sind, es sich um einen grossen Personenkreis handelt oder eine lange Zeitspanne zwischen der Entnahme der Proben oder der Datenerhebung und dem Forschungsvorhaben liegt.[414] Nur weil viele Personen kontaktiert werden müssten, kann dies, wie die Lehre zu Recht betont, allerdings noch nicht bedeuten, dass die Einholung der Einwilligung bzw. die Information über ein Widerspruchsrecht als "unverhältnismässig schwierig" zu erachten ist.[415]

3. Alternativ zu der Unmöglichkeit bzw. der Unverhältnismässigkeit, sieht Art. 34 lit.c HFG die Unzumutbarkeit der Kontaktaufnahme für die betroffene Person vor. Gemäss der Botschaft liegt eine solche vor, wenn die Kontaktierung bezüglich der Einwilligung bzw. der Information über das Widerspruchsrecht eine schwere emotionale Belastung bei der betroffenen Person hervorrufen würde oder ihre Angehörigen erneut mit einer schwierigen Situation konfrontiert würden.[416]

Alle der oben beschriebenen Bedingungen sind, als Ausnahme ("in eng umgrenzten Fällen"), streng auszulegen.[417] Zusätzlich zum Vorliegen einer der Bedingungen darf keine dokumentierte Ablehnung vorliegen und

---

407 Art. 34 HFG.

408 Botschaft zum HFG, BBl 2009 S. 8123.

409 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 34 Rz. 4; Votum PRELICZ-HUBER, AB 2011 N 332.

410 Art. 34 lit. a HFG.

411 BAUR, Personalisierte Medizin im Recht, Humanforschung–- Quo vadis? (2019), S. 214.

412 Das HFG schützt, im Gegensatz zum DSG, in gewissen Bereichen auch die Daten bzw. das genetische Material Verstorbener; Art 44 HFG.

413 Botschaft zum HFG, BBl 2009 S. 8123.

414 Botschaft zum HFG, BBl .2009 S. 8123.

415 BAUR, Personalisierte Medizin im Recht, Humanforschung–- Quo vadis? (2019), S. 214.

416 Botschaft zum HFG, BBl 2009 S. 8123.

417 RUDIN, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 34 Rz. 7; Botschaft zum HFG, BBl 2009 S. 8123.

es muss eine Interessenabwägung vorgenommen werden, die für ein überwiegendes Forschungsinteresse spricht.[418] Zudem wird für die Inanspruchnahme des Art. 34 HFG eine Bewilligung der zuständigen kantonalen Ethikkommission benötigt.[419] Die Praxis zeigt, dass in den Kantonen keine vereinheitlichen Kriterien für die Beurteilung der Anwendbarkeit der Ausnahmebestimmung bestehen und sie auch unterschiedlich häufig angewendet wird.[420]

Vor diesem Hintergrund ist die Ausnahmebestimmung mit vielen Unsicherheiten verbunden und bei der Konzipierung von Forschungsprojekten lässt sich der Ausgang des Verfahrens vor den Ethikkommissionen nur schwer abschätzen.

4.2.5 Weitere wichtige Anforderungen

Neben den soeben aufgezeigten Kernanforderungen für die Weiterverwendung der Gesundheitsdaten zu Forschungszwecken bestehen im HFG auch weitere Anforderungen, von welchen drei nachfolgend erläutert werden.

a) Weitergabe zu forschungsfremden Zwecken

Die Weitergabe von gesundheitsbezogenen Daten oder biologischem Material, das zu Forschungszwecken entnommen wurde, darf nur unter gewissen Voraussetzungen zu forschungsfremden Zwecken weitergeben werden.[421] In Art. 41 HFG verwirklicht sich der dem Datenschutzrecht zugrundeliegende Zweckbindungsgrundsatz, welcher besagt, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.[422] Selbst wenn die strenge Zweckbindung durch den im HFG etwas aufgeweicht wird, umfasst dieser nur Forschungszwecke im Anwendungsbereich des HFG. Eine Verwendung der Daten zu forschungsfremden Zwecken ist deshalb gleichwohl potentiell ein Verstoss gegen das Zweckbindungsgebot und an den allgemeinen datenschutzrechtlichen Vorgaben zu messen. Danach sind namentlich im Bereich der Vorschriften für Private verschieden Rechtfertigungsgründe denkbar.

Artikel 41 HFG enthält nun aber eine strengere Spezialregelung, die zwar nicht für jegliche Bearbeitung gilt, aber zumindest für die Weitergabe. Danach gilt die Weitergabe von gesundheitsbezogenen Daten oder biologischem Material, das zu Forschungszwecken entnommen wurde, grundsätzlich als verboten. Einzige mögliche Ausnahmen, gewissermassen als Rechtfertigungsgründe, liegen dann vor, wenn:

- für die Weitergabe eine gesetzliche Grundlage besteht oder
- die betroffene Person im Einzelfall nach hinreichender Aufklärung in die Weitergabe eingewilligt hat.

---

[418] Art. 34 lit. b und c HFG.

[419] Art. 45 Abs. 1 lit. b.

[420] WIDMER ET AL., Evaluation des Humanforschungsgesetzes (HFG), 2019, S. 25.

[421] Art. 41 Abs HFG.

[422] RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 41 Rz. 2; Art. 4 Abs. 3 DSG bzw. Art. 6 Abs. 3 nDSG.

Eine gesetzliche Grundlage für eine zweckfremde Weitergabe besteht bspw. für die Beschlagnahmung von Beweismitteln im Rahmen der Strafverfolgung.[423] Die Einwilligung hat hier für den Einzelfall zu erfolgen, sodass pauschale oder breit gefasste Erklärungen, wie beim Generalkonsent, von vornherein unwirksam sind.[424] Darüber hinaus kann die Einwilligung auch nicht durch eine Bewilligung der zuständigen Ethikkommission ersetzt werden.[425] Aufgrund dieser Regelung gilt es in der Praxis sorgfältig zu prüfen, inwiefern die Voraussetzungen für die Verwendung von Daten aus der Forschung bspw. zu Behandlungs- oder Qualitätssicherungszwecken vorliegen.

b) Ausfuhr

Häufig sind an Forschungsprojekten eine Vielzahl an verschiedenen in- und ausländischen Institutionen beteiligt, die jeweils ihre fachspezifische Expertise einbringen. Sofern im Rahmen dieser grenzüberschreitenden Zusammenarbeit ausländischen Forschungseinrichtungen Zugang zu biologischem Material bzw. Gesundheitsdaten gewährt wird, ist sicherzustellen, dass im Ausland die Rechte der betroffenen Person in einem ähnlichen Ausmass wie in der Schweiz geschützt werden. Die entsprechenden rechtlichen Rahmenbedingungen für die grenzüberschreitende Ausfuhr von biologischem Material und Gesundheitsdaten zu Forschungszwecken sind in Art. 42 HFG geregelt.

Der im HFG verwendete Begriff der Ausfuhr ist weiter als jener der grenzüberschreitenden Bekanntgabe des DSG,[426] da er nicht nur die Bekanntgabe von Daten ins Ausland umfasst, sondern auch die physische Ausfuhr von biologischem Material.[427] Wie bereits unter dem DSG erläutert, liegt bereits eine grenzüberschreitende Bekanntgabe vor, wenn jemand aus dem Ausland Zugriff auf die Daten hat.[428]

Die Vorgaben unterscheiden sich auch hier je nach betroffener Datenkategorie. Die strengsten Anforderungen stellt das HFG an die Ausfuhr von (unverschlüsseltem) biologischem Material bzw. genetischen Daten zu Forschungszwecken. Hierfür bedarf es gemäss Art. 42 Abs. 1 HFG eines "informed consent" der betroffenen Person. Diese Vorgabe gilt allerdings nicht für anonymisiertes biologisches Material bzw. genetische Daten anwendbar, weil diese ohnehin vom Anwendungsbereich des HFG ausgeschlossen sind.[429] Demgegenüber ist die Ausfuhr von verschlüsseltem biologischen Material bzw. genetischen Daten zu Forschungszwecken von Art. 42 Abs. 1 HFG erfasst und bedarf grundsätzlich einer Einwilligung des Betroffenen.

Inwiefern im genannten Fall eine Einwilligung notwendig ist, wenn der Empfänger der verschlüsselten Gesundheitsdaten bzw. des biologischen Materials keine Möglichkeit hat, mit verhältnismässigen Mitteln einen Personenbezug herzustellen, ist jedoch fraglich. Laut dem im DSG vertretenen relativen Ansatz können in solchen Fällen pseudonymisierte Daten aus der Perspektive gewisser Empfänger als anonymisiert gelten.

---

423 RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 41 Rz. 6; Art. 263 Abs. 1 lit. a StPO.

424 RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 41 Rz. 8.

425 RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 41 Rz. 8.

426 Art. 6 DSG bzw. Art. 16 ff. nDSG.

427 RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 42 Rz. 5.

428 ROSENTHAL/JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, Art. 6 Rz. 4.

429 Art. 2 Abs. 2 lit. b.

Im Detail wird dies in Abschnitt 3.2.7 beschrieben. Auch in diesem Zusammenhang gilt es deshalb zu beachten, dass die Anonymisierung und Pseudonymisierung aufgrund einer komplexen Einzelfallbeurteilung stets mit Rechtsunsicherheit einhergeht.

An die Ausfuhr von nichtgenetischen Gesundheitsdaten stellt Art. 42 Abs. 2 HFG weniger strenge Anforderungen. Hinsichtlich dieser Daten verweist das HFG auf die Bestimmungen für die grenzüberschreitende Bekanntgabe von Personendaten des DSG[430] Auf die damit verbundenen rechtlichen Risiken, namentlich bei Datenübermittelungen in die USA, wurde bereits vorstehend in Abschnitt 4.1.4c) hingewiesen. Die Risken, welchen derzeit kaum anders als mit einer Anonymisierung oder Pseudonymisierung begegnet werden kann, gelten somit auch auf die im HFG geregelten Ausfuhren.

c) Aufbewahrung

Die Aufbewahrung von biologischem Material und gesundheitsbezogenen Material in Biobanken hat in den letzten Jahren stark an Bedeutung gewonnen.[431] Einer der Gründe dafür ist der Generalkonsent, unter dem Daten im Anwendungsbereich des HFG – anders als unter dem DSG – gewissermassen auf Vorrat für die Weiterverwendung zu Forschungszwecken gespeichert werden können. Aufgrund der Sensitivität der Daten und Materialen legt das HFG und die HFV allerdings allgemein Standards für die sichere Aufbewahrung fest.

Art. 43 HFG regelt die Pflichten im Zusammenhang mit der Aufbewahrung von biologischem Material und genetischen Daten zu Forschungszwecken. Die Daten und das Material müssen durch geeignete technische und organisatorische Massnahmen gegen unbefugten Zugang geschützt werden sowie die betrieblichen und fachlichen Anforderungen erfüllen.[432] Konkretisiert wird die gesetzliche Grundlage durch Art. 5 HFV, welcher für die Aufbewahrung von gesundheitsbezogene Personendaten folgende Pflichten vorsieht:

- Beschränkung des Umgangs mit den Gesundheitsdaten auf Personen, welche diese Daten zur Erfüllung ihrer Aufgaben benötigen;
- Verhinderung der unbefugten oder versehentlichen Offenlegung, Veränderung, Löschung und Kopie der Gesundheitsdaten und;
- Dokumentation aller massgeblichen Bearbeitungsvorgänge.

Für die Aufbewahrung von biologischem Material gelten die oben beschrieben Anforderungen sinngemäss.[433] Darüber hinaus müssen die technischen Anforderungen für die sachgerechte Aufbewahrung des biologischen Materials gewährleistet werden.[434] Konkret muss dafür durch eine entsprechende (Lager-)Infrastruktur und das nötige Fachwissen sichergestellt werden, dass die Qualität der verschiedenen Proben erhalten bleibt und es zu keinen Verfälschungen des Materials kommt.[435] Ferner müssen die erforderlichen

---

[430] Art. 6 DSG bzw. Art. 16 ff nDSG.

[431] RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 43 Rz. 1.

[432] Art. 43 HFG.

[433] Art. 5 Abs. 2 lit. a HFV.

[434] Art. 5 Abs. 2 lit. b HFV.

[435] RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 43 Rz. 13.

Ressourcen für die Aufbewahrung bereitgestellt werden.[436] Dabei gilt es zu beachten, dass die Aufbewahrung den biologischen Eigenheiten des Materials für die Dauer des gesamten Forschungsprojekts gerecht wird.[437] Zu den dafür notwendigen Ressourcen zählen laut dem Erläuternden Bericht zur Verordnung genügend Raumkapazität, Notstromeinrichtungen und ein dauerhaftes Überwachungskonzept.[438]

Im Zusammenhang mit der Aufbewahrung ist unklar, ob das HFG eine abschliessende Regelung vornimmt, oder ob die Bestimmungen zur Datensicherheit des DSG bzw. der kantonalen Datenschutzgesetze ergänzende Anwendung finden.[439] Nach der hier vertretenen Auffassung sind für die Aufbewahrung von Gesundheitsdaten die Bestimmungen des Art. 7 nDSG jedenfalls ergänzend als Auslegungshilfe heranzuziehen, da sowohl der Wortlaut des Art. 43 Abs. 1 (durch geeignete organisatorische und technische Massnahmen) als auch der angestrebte Zweck (die Gewährleistung der Datensicherheit) den Datenschutzbestimmungen zur Datensicherheit gemäss nDSG entspricht.

4.2.6 Konsequenzen von Verstössen gegen das HFG

Inwieweit ein Verstoss gegen die oben beschriebenen Vorgaben des HFG zivilrechtliche oder verwaltungsrechtliche Konsequenzen nach sich ziehen kann, ist noch ungeklärt. Zumindest dort, wo das Datenschutzrecht ergänzend zur Anwendung gelangt, droht namentlich auch ein Verbot der Weiterverwendung von Daten und die Anordnung einer Datenlöschung. Während also in zivil- und verwaltungsrechtlicher Hinsicht gewisse Unsicherheiten bestehen, steht zumindest fest, dass die Missachtung des HFG im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten und biologischem Material unter gewissen Voraussetzungen strafrechtlich sanktionierbar sind.

So werden bestimmte Verstösse gegen die in Kapitel 4 des HFG geregelten Bestimmungen zur Weiterverwendung von biologischem Material und gesundheitsbezogenen Daten als Übertretung im Sinne des Art. 63 HFG qualifiziert. Demzufolge wird namentlich mit Busse sanktioniert, wer ein Forschungsprojekt ohne die Einwilligung der zuständigen Ethikkommission durchführt, wer biologisches Material oder gesundheitsbezogene Personendaten ohne die erforderliche Einwilligung bzw. Information weiterverwendet oder wer die Daten bzw. das Material ohne gesetzliche Grundlage oder ohne erforderliche Einwilligung weitergibt. Anders als bei den Sanktionen unter dem DSG werden hier nicht nur vorsätzliche, sondern auch fahrlässige Verstösse sanktioniert.

Als Täter der genannten Straftatbestände kommen überwiegend die forschenden Personen in Betracht.[440] Sofern ein Forschungsprojekt im Sinne der HFV vorliegt, wird insbesondere die Projektleitung strafrechtlich

[436] Art. 5 Abs. 2 lit. c HFV

[437] RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 43 Rz. 14.

[438] RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 43 Rz. 13, 14.

[439] Vgl. deutlich: RÜTSCHE/ANNER, in: RÜTSCHE (Hrsg.), SHK-HFG, 2015, Art. 43 N 8; sowie ZEGG, Benefit Shaing - Anspruch auf Teilhabe an Forschungsergebnissen, 2020, S. 39; weniger deutlich: Botschaft zum HFG, BBl 2009 S. 8132, wo die Formulierung eher als Aufforderung an den Bundesrat als Verordnungsgeber und nicht an die dem HFG unterstellten Organisationen verstanden werden könnte.

[440] GRUBERSKI, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 62-64 Rz. 32.

zur Verantwortung gezogen.[441] Für den Vollzug der beschriebenen Straftatbestände sind die kantonalen Strafverfolgungsbehörden zuständig.[442]

4.2.7 Fazit: Hindernisse im HFG

Zusammenfassend ist festzuhalten, dass das HFG zwar viele sinnvolle Erleichterungen vorsieht, um eine effektive Sekundärnutzung von Gesundheitsdaten zu ermöglichen. Der Nutzen dieser Vorkehrungen, wie bspw. des Generalkonsents, wird jedoch – ähnlich wie die Instrumente im DSG – erheblich geschmälert durch eine Vielzahl von Unklarheiten und Unsicherheiten grundlegender Natur. Diese wiegen umso schwerer, als bei Verstössen gegen gewisse Vorschriften einschneidende strafrechtliche Sanktionen für die verantwortlichen Personen drohen.

Die Unsicherheiten beginnen bereits bei den in Abschnitt 3 aufgeführten Unsicherheiten in Bezug auf die Begriffsdefinitionen. Es geht also auch hier um die Frage, was vorzukehren ist, um Personendaten tatsächlich zu anonymisieren oder zu verschlüsseln und dadurch die Anwendung der strengeren Anforderungen an die Sekundärnutzung der Daten zu verhindern. So hätte der Gesetzgeber bspw. auch die Gelegenheit gehabt, explizit von dem offenen, kontextabhängigeren Begriffsverständnis des DSG abzuweichen und für die Forschung konkretere, fassbarere Anforderungen festzulegen, bei deren Einhaltung stets von einer Anonymisierung oder Pseudonymisierung auszugehen ist. Diese Gelegenheit hat der Gesetzgeber jedoch nicht genutzt und es verbleibt deshalb auch hier Unsicherheit in der Praxis.

Eine Quelle erheblicher Rechtsunsicherheit ist auch das ungeklärte Verhältnis zwischen den Anforderungen an die Weiterverwendung der Daten des HFG zu denjenigen des DSG. Auch wenn im Grundsatz unbestritten ist, dass die speziellen Vorschriften des HFG Vorrang vor den allgemeinen Vorschriften des DSG haben, bleibt meist unerwähnt oder jedenfalls ungeklärt, inwieweit einzelne grundlegende Vorschriften des DSG nicht gleichwohl, mindestens sinngemäss, gelten müssen. Zu nennen ist dabei etwa die Anforderung, dass über die für eine Datenbearbeitung Verantwortlichen zu informieren ist. Ob diese Anforderung im Rahmen der Humanforschung tatsächlich nicht gilt, ist zu bezweifeln, wurde aber bislang kaum je thematisiert.

Mit Blick auf die differenzierten Anforderungen an die Weiterverwendung ist die Rechtslage komplex und für die Praxis oft nur schwer verständlich erläuterbar. Hoch sind auch die Anforderungen an die hinreichende Aufklärung der betroffenen Personen bzw. Teilnehmer an Forschungsvorhaben. Dabei führt gerade die Sicherstellung, dass die Verständlichkeit nicht nur für eine Durchschnittsperson, sondern auch für die einzelnen konkreten Teilnehmenden gegeben ist, zu sehr hohem Aufwand. Gleiches gilt – und dies ohne offensichtlichen Nutzen – für die Anforderung der Schriftlichkeit von Einwilligungserklärungen. Auch wenn Raum dafür besteht, darunter auch digitale Lösungen bspw. mit Unterzeichnung auf Touch Screens genügen zu lassen, entspricht dies nicht dem gelebten Verständnis des Schriftformerfordernisses und die Einführung solcher Lösungen ist mit Unsicherheiten behaftet. In der Praxis bleibt es deshalb bei der nicht mehr zeitgemässen Einholung von Einwilligungen in ausgedruckter und unterzeichneter Form.

Dies gilt besonders auch mit Blick auf den für die Sekundärnutzung von Gesundheitsdaten besonders wichtigen Generalkonsent. Auch diese Erscheinungsform der Einwilligung, welche ausnahmsweise unter bestimmten Voraussetzungen auch die Erhebung von Gesundheitsdaten gewissermassen auf Vorrat für Forschungszwecke erlaubt, wird aufgrund des Schriftformerfordernisses weniger als nötig eingeholt. Erschwerend

[441] GRUBERSKI, in: RÜTSCHE (Hrsg.), Humanforschungsgesetz, 2015, Art. 62-64 Rz. 32.

[442] Art. 64 Abs. 1 HFG.

kommt hinzu, dass die einzelnen Pflichtangaben, über welche die betroffenen Personen für den Generalkonsent zwingend aufgeklärt werden müssen, nicht zweifelsfrei klar sind. Dies dürfte auch mit ein Grund dafür sein, weshalb keine Einigung auf ein schweizweit vereinheitlichtes Formular zur Einholung des Generalkonsents zustande gekommen ist. Folglich gelangen in der Praxis die unterschiedlichsten Ausprägungen des Generalkonsents zum Einsatz. Bei der Durchführung von prospektiven Forschungsprojekten mit Daten aus verschiedenen Spitälern muss deshalb die Gültigkeit und Reichweite der jeweiligen Einwilligungen vorab einzeln geprüft werden, was nicht nur enorm aufwändig ist, sondern auch mit Unsicherheiten verbunden ist. Dieser Aufwand könnte durch ein schweizweit in allen Spitälern verwendetes – von offizieller Stelle verbindlich bewilligtes – Formular verhindert werden und es könnte zumindest in dieser Hinsicht die erforderliche Rechtsicherheit geschaffen werden.

4.3 Kantonale Datenschutzgesetze

Wie bereits angesprochen, bestehen auch auf kantonaler Ebene jeweils sektorübergreifende Datenschutzgesetze. Gemäss dem Gutachterauftrag wird nachfolgend auf drei ausgewählte kantonale Datenschutzgesetze und deren Regelungen zur Sekundärnutzung von Gesundheitsdaten eingegangen: das Datenschutzgesetz des Kantons St. Gallen (DSG-SG[443]), das Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG-ZH[444]) und das Datenschutzgesetz des Kantons Waadt (LPrD-VD[445]).

4.3.1 Anwendungsbereich und Grundbegriffe der kantonalen Datenschutzgesetze

Der Anwendungsbereich dieser Gesetze ist grundsätzlich weitgehend identisch definiert und es wird dabei auf die gleichen Begriffe und Begriffsdefinitionen abgestellt wie im DSG. So gelten die Gesetze ebenfalls für die "Bearbeitung von Personendaten", [446] wobei dies im Kanton Zürich zumindest in Bezug auf die im Gesetz enthaltenen datenschutzrechtlichen Vorgaben gilt, das Gesetz im Übrigen aber einen weiteren Anwendungsbereich und Regelungsgegenstand hat.[447] Dabei wird ebenfalls auf einen sehr breiten Bearbeitungsbegriff abgestellt[448] und als Personendaten gelten nicht nur Informationen, die sich auf eine bestimmte, sondern auch auf eine bestimmbare Person beziehen[449]. Wie später verdeutlicht wird, [450]sind die datenschutzrechtlichen Rollen in den Kantonen aber unterschiedlich und bei zwei der Kantone auch abweichend vom DSG geregelt. Da der Gesetzgeber aber gerade in diesen beiden Kantonen sich beim Begriffsverständnis von Personendaten stark an demjenigen des DSG orientiert,[451] bleibt unklar, aus wessen Perspektive die zentrale

---

443 Datenschutzgesetz des Kantons St. Gallen, sGS 142.1 (im Folgenden DSG-SG).

444 Gesetz über die Information und den Datenschutz des Kantons Zürich, 170.4 (im Folgenden IDG-ZH).

445 Loi sur la protection des données personnelles, 172.65 (im Folgenden LPrD-VD).

446 Art. 2 Abs. 1 DSG-SG; Art. 3 Abs. 1 LPrD-VD.

447 Vgl. § 1 Abs. 1 i.V.m. § 8 IDG-ZH.

448 Art. 1 Abs. 1 lit. e DSG-SG; Art. 4 Abs. 1 Ziff. 5 LPrD-VD; § 3 Abs. 5 IDG-ZH.

449 Art. 1 Abs. 1 lit. a DSG-SG; Art. 4 Abs. 1 Ziff. 1 LPrD-VD ("identifiable"); § 3 Abs. 3 IDG-ZH.

450 Vgl. unten Abschnitt 4.3.3a)

451 Vgl. die Weisung des Zürcher Regierungsrats vom 9. November 2005, ABl 2005 Nr. 47 S. 1304, die auf das frühere DSG-ZH verweist, wo ebenfalls bereits die Definition des DSG enthalten war; Stellungnahme des Regierungsrats zum Entwurf der Kantonsratskommission 4.10.1989: " Begriffsanpassungen an Bundesentwurf sinnvoll" vgl. Botschaft und Entwurf der St.Galler Regierung vom 9. Oktober 2018, Nachtrag zum Datenschutzgesetz, ABl. SG Nr. 46 2018 4049 fff, S. 4060 ("analog").

Frage der Bestimmbarkeit einer Person beurteilt werden soll.[452] Es ist deshalb denkbar, dass Daten, die unter den Vorschriften des DSG, des LPrD-VD und der DSGVO als anonym zu betrachten sind, in den beiden Kantonen gleichwohl Personendaten darstellen und umgekehrt.

Unterschiedlich definiert wird ferner, wer als die betroffenen Personen zu betrachten sind. Während das LPrD-VD[453] explizit sowohl natürliche als auch juristische Personen einbezieht und das DSG-SG[454] ausdrücklich nur für Daten natürlicher Personen gilt, liesse der Wortlaut des IDG-ZH[455] beide Auslegungen zu. Die Entstehungsgeschichte macht jedoch deutlich, dass unter dem IDG-ZH auch juristische Personen geschützt sein sollen und auch deren Daten als Personendaten zu behandeln sind.[456] An dieser Ausgangslage wird sich auch durch das Inkrafttreten des nDSG und die damit verbundene Abschaffung des Schutzes juristischer Personen auf Bundesebene nichts ändern.

Darüber hinaus gelten die Gesetze für "öffentliche Organe",[457] wobei dies für das LPrD-VD nur im Ergebnis zutrifft, es aber für den Geltungsbereich nicht explizit auf den Begriff abstellt[458]. Im Ergebnis werden von den Gesetzen aber jedenfalls übereinstimmend zumindest die Behörden und Verwaltungseinheiten des Kantons und der Gemeinden erfasst,[459] wozu neben der Zentralverwaltung grundsätzlich auch die dezentrale Verwaltung zu zählen ist.[460] Wie im Zusammenhang mit den Bundesorganen ausgeführt, ist es der Organisationsautonomie der Kantone überlassen, im öffentlichen Bereich Rechtseinheiten ihrer Datenschutzgesetzgebung zu unterstellen. Wichtig auch für die vorliegende Fragestellung ist daher, inwieweit in den hier untersuchten Kantonen auch selbständige öffentlich-rechtliche Organisationen in einem weiteren Sinne unterstellt werden. Hier präsentiert sich ein unterschiedliches Bild. So sind im Kanton St.Gallen "nur" explizit auch selbständige öffentlich-rechtliche Anstalten des Kantons als öffentliche Organe qualifiziert.[461] Demgegenüber sind in den Kantonen Zürich und Waadt jegliche Personen (und in Zürich gemeinhin auch Organisationen) den kantonalen Datenschutzgesetzen unterstellt, die mit der Erfüllung öffentlichen Aufgaben betraut sind.[462] Dies gilt allerdings jeweils nur, *soweit* sie mit Aufgaben des Kantons betraut werden bzw. diese ausüben.[463] Eine solche Einschränkung fehlt im Kanton St. Gallen, sodass die öffentlich-rechtlichen Anstalten für alle Tätigkeitsbereiche dem kantonalen Datenschutzgesetz unterstellt sind. Dass in den Kantonen Waadt und Zürich die Privaten ebenfalls als öffentliche Organe gelten, soweit sie mit Aufgaben des Kantons betraut werden bzw. diese

---

452 In der Lehre wird dies nicht thematisiert, sondern stillschweigend auf die im Bundesrecht entwickelten Grundsätze abgestellt, wobei jedoch wiederum die Perspektive der Beurteilung unscharf ist und auf den "Interessenten" abgestellt wird, RUDIN, in: BAERISWYL/RUDIN (Hrsg.), Praxiskommentar IDG, 2012, § 3 N 16 ff.

453 Art. 4 Abs. 1 Ziff. 4 LPrD-VD.

454 Art. 1 Abs. 1 lit. c DSG-SG.

455 Art. 2 Abs. 1 DSG-SG; § 1 Abs. 1 IDG-ZH.

456 Weisung des Zürcher Regierungsrats vom 4. Juli 2018, ABl 2018 Nr. 28 (Anmerkungen zu § 3).

457 § 1 Abs. 1 IDG-ZH; Art. 2 Abs. 1 DSG-SG.

458 Vgl. die Aufzählung in Art. 3 Abs. 2 und ferner Art. 4 Abs. 1 Ziff. 8 LPrD-VD.

459 Art. 1 Abs. 1 lit. h Ziff. 1 und 3 DSG-SG; Art. 3 Abs. 2 lit. c und d LPrD-VD; § 3 Abs. 1 lit. b IDG-ZH.

460 WALDMANN/OESCHGER, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 13 N 25.

461 Art. 1 Abs. 1 lit h DSG-SG.

462 Art. 3 Abs. 2 lit. e LPrD-VD; § 3 Abs. 1 lit. c IDG-ZH.

463 Art. 3 Abs. 2 lit. e und d LPrD-VD; § 3 Abs. 1 lit. c IDG-ZH.

ausüben, ergibt sich bereits aus den erwähnten allgemeinen Definitionen. In diesem Punkt im Ergebnis übereinstimmend, stellt der Kanton St.Gallen solche Privaten ebenfalls den öffentlichen Organen gleich.[464]

Daraus erhellt, dass sich auch auf kantonaler Ebene ähnliche Fragen stellen, wie bei der Beurteilung des Geltungsbereichs des DSG. Ist eine Rechtseinheit nach dem kantonalen Recht der Kantonsverwaltung zugerechnet, wird aber nach dem Gesagten eine gleichzeitige Unterstellung unter das DSG ausscheiden. Ist dies nicht der Fall, wird aber jeweils zu beurteilen sein, ob die Rechtseinheit mit einer öffentlichen Aufgabe betraut wurde und ob es sich dabei um eine Bundesaufgabe oder eine kantonale Aufgabe handelt. Auch hier ist sodann auf die jeweilige Tätigkeit bzw. Datenbearbeitung abzustellen und zu prüfen, ob diese im Rahmen der Erfüllung der öffentlichen Aufgabe erfolgt. Es ist deshalb im Grundsatz gleichwohl möglich, dass dieselbe Rechtseinheit für verschiedene Datenbearbeitungen grundsätzlich sowohl Bundesorgan als auch kantonales Organ sein kann.

Erschwerend kommt wiederum hinzu, dass auch kantonale Organe privatrechtlich oder wie Private handeln können. Dabei ist nicht restlos klar, was in diesem Fall gelten soll. Unklar ist namentlich, inwieweit diese Frage ebenfalls unter die verfassungsrechtliche Organisationsautonomie der Kantone fällt. Aus einigen kantonalen Gesetzgebungen geht hervor, dass die Frage bejaht wird. Hierzu gehört auch der Kanton Zürich. Dieser sieht – ähnlich wie andere Kantone auch – eine Ausnahme vom Geltungsbereich des Gesetzes vor, soweit öffentliche Organe am wirtschaftlichen Wettbewerb teilnehmen und dabei nicht hoheitlich handeln. Für diesen Fall erklärt er sodann das DSG für anwendbar, dies jedoch nur "sinngemäss" und auch die Aufsicht soll bei der kantonalen Behörde verbleiben.[465] Die damit ausgedrückte Haltung steht jedoch im Konflikt mit der unseres Erachtens richtigen Auffassung in der Lehre und Rechtsprechung, wonach das DSG hier Vorrang haben muss und daher auch für das Handeln kantonaler Organe als Private die (materiellen[466]) Vorgaben des DSG zu gelten haben.[467]

Diese Schlussfolgerung führt dazu, dass die gesetzlichen Umschreibungen der Ausschlussgründe der Kantone in diesem Zusammenhang nicht massgeblich sind, sondern vielmehr der gesetzliche Geltungsbereich des DSG.[468] Es erübrigt sich daher zu prüfen, was, wie in den Kantonen St.Gallen und Zürich konkret unter dem Ausschluss bei Teilnahme am Wettbewerb und nicht hoheitlichem Handeln zu verstehen ist.[469] Für die Beurteilung, ob ein Handeln als Privater vorliegt, ist deshalb auf die Natur des zugrundeliegenden Verhältnisses abzustellen und daher in einer gesamthaften Betrachtung die Beziehung zwischen dem Datenbearbeiter und dem Betroffenen zu prüfen.[470] Gerade im Gesundheitsbereich fällt die Unterscheidung zwischen öffentli-

464 Art. 2 Abs. 1bis DSG-SG.

465 § 2c IDG-ZH.

466 Unklar bleibt in diesem Fall aber auch, wer für die Aufsicht zuständig sein soll; geht es nach der (wohl richtigen) Ansicht des St.Galler Gesetzgebers soll die Aufsicht bei den kantonalen Behörden verbleiben: Botschaft und Entwurf der St.Galler Regierung vom 9. Oktober 2018, Nachtrag zum Datenschutzgesetz, ABl. SG Nr. 46 2018 4049 fff, S. 4063.

467 Vgl. WALDMANN/OESCHGER, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 13 29; BAERISWYL, in: BAERISWYL/RUDIN (Hrsg.), Praxiskommentar IDG, 2012, § 2 N 13; Urteil des Verwaltungsgerichts des Kantons Bern, 4.2.2013, VGE 100.2012.118, BVR 2013 S. 251 ff., E. 3.6; vgl. ferner die Auffassung des Waadtländischen Gesetzgebers, Exposé des Motifs et Projets de la Loi sur la Protection des Données, Bulletin du Grand Conseil, Législature 2007-2012, Tome 1 Conseil d'Etat 119 ff., S. 27; a.A. BLECHTA, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 3 Rz. 85; differenzierend, in jedem Fall aber von der Massgeblichkeit der kantonalen Gesetze ausgehend, RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012, S. 48 f.

468 Anders im Ansatz RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012, insb. S. 7-11.

469 § 2c IDG-ZH; Art. 2 Abs. 2 lit. a DSG-SG.

470 BGE 122 I 153, 156, E. 3. C.

cher oder privater Natur nicht leicht und führt immer wieder zu Rechtstreitigkeiten und umfangreichen rechtlichen Gutachten.[471] Die Frage muss stets im Einzelfall beantwortet werden und es muss zudem auch hier auf die jeweilige Tätigkeit bzw. Datenbearbeitung abgestellt werden, sodass dieselbe Rechtseinheit für verschiedene Tätigkeiten und womöglich gar in Bezug auf verschiedene betroffene Personen unterschiedlichen Vorschriften unterstellt sein kann.[472]

Die Kriterien für die Abgrenzung zwischen Handeln als Privater und Handeln als öffentliches Organ sind im Einzelnen ebenfalls nicht restlos klar, insbesondere auch weil innerhalb des DSG unterschiedliche Ansatzpunkte zum Ausdruck kommen.[473] Zumindest in Bezug auf die Unterstellung als Private unter das DSG spricht jedoch mehr dafür, primär darauf abzustellen, inwieweit bei einer Tätigkeit eine öffentliche Aufgabe erfüllt wird.[474] Kriterien wie die Trägerschaft sind dabei grundsätzlich irrelevant.[475] Für das im Gesundheitsbereich wichtige Verhältnis zwischen Arzt und Patient ergibt sich dabei kein einheitliches Bild. Beim Tätigwerden im Rahmen des krankenversicherungsrechtlichen oder eines kantonalen Leistungsauftrags ist von einem Handeln als öffentliches Organ auszugehen.[476] Das anwendbare Recht kann deshalb von Behandlung zu Behandlung unterschiedlich sein, sodass z.B. selbständige Zusatzleistungen, die nicht mit Grundversicherungsleistungen verbunden sind, als private Tätigkeit gelten, nicht aber zusatzversicherte Leistungen, für welche ein Sockelbeitrag aus der Grundversicherung geschuldet ist.[477] Darüber hinaus haben die beteiligten Rechtseinheiten aus unterschiedlichen Kantonen bei der Zusammenarbeit in Projekten, namentlich im Rahmen der Forschung, womöglich unterschiedliche Vorgabe zu beachten, sind doch auch in diesem Bereich die Leistungsaufträge nicht kantonsübergreifend einheitlich ausgestaltet.[478] Diese Komplexität wird denn auch zu Recht verschiedentlich kritisiert[479] und erschwert den effizienten Umgang mit personenbezogenen Gesundheitsdaten.

4.3.2 Verhältnis zu anderen Gesetzen

Kantonale Rechtseinheiten können somit als Private (und vereinzelt auch als Bundesorgane) den Vorgaben des DSG unterstellt sein. Neben den bereichsübergreifenden kantonalen Datenschutzgesetzen kann somit

---

471 Vgl. nur RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012; EPINEY, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, in: Jusletter 2. März 2015; PRIEUR, Welches Datenschutzrecht ist für Spitäler als Arbeitgeber anwendbar? Beispiel: Kanton Bern, in: Jusletter 18. Mai 2015, Rz. 23; Gutachten 051124 des Bundesamtes für Justiz vom 24. November 2005, JAAC 70.54; Empfehlung der Beauftragten für Information und Datenschutz des Kantons Solothurn, 8.7.2021, 07.01_2021_04; Urteil des Verwaltungsgerichts des Kantons Bern, 4.2.2013, VGE 100.2012.118, BVR 2013 S. 251 ff., E. 3.6. BGE 122 I 153, 156, E. 3. C.

472 Vgl. BGE 122 I 153, 156, E. 3. E.

473 Vgl. Art. 3 lit. h DSG/Art. 5 lit. i nDSG i.V.m. Art. 2 Abs. 1 lit. a DSG/Art. 2 Abs. 1 lit. a nDSG, wo das Betrautsein mit öffentlichen Aufgaben erwähnt wird, im Unterschied zu Art. Art. 23 Abs. 1 DSG/Art. 40 nDSG, wo von privatrechtlich Handeln die Rede ist; vgl. dazu auch Bühlmann/Schüepp, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 20.

474 So auch RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012, insb. S. 11, wenn auch mit anderer Herleitung; vgl. auch Urteil des Verwaltungsgerichts des Kantons Bern, 4.2.2013, VGE 100.2012.118, BVR 2013 S. 251 ff., E. 3.5.

475 Anders offenbar ISLER, Die Rollenverteilung in klinischen Versuchen, in: digma 2020 S. 68, 69.

476 RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012, insb. S. 36, wenn auch mit anderer Herleitung; vgl. auch Urteil des Verwaltungsgerichts des Kantons Bern, 4.2.2013, VGE 100.2012.118, BVR 2013 S. 251 ff., E. 3.6.

477 RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012, S. 38 f. und 48.

478 Vgl. dazu RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012, insb. S. 40.

479 Vgl. RÜTSCHE, Datenschutzrechtliche Aufsicht über Spitäler, 2012, insb. S. 49 f.; BLECHTA, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 3 Rz. 85.

auch das allgemeine DSG zu beachten sein. Aber selbst für Tätigkeiten, bei denen dies nicht der Fall ist, gelten auch für die kantonalen Organe die Spezialdatenschutzvorschriften des Bundes.[480] Hierzu zählen namentlich die Vorschriften des Sozialversicherungsrechts, aber auch die Vorschriften des HFG, des EPDG etc.[481] Für das Verhältnis der kantonalen Datenschutzgesetzgebungen zu diesen gilt dasselbe wie auf der Bundesebene. Die Spezialvorschriften gehen in ihrem Anwendungs- und Regelungsbereich vor und die Datenschutzgesetze bleiben, soweit nicht von einer abschliessenden Regelung auszugehen ist, ergänzend anwendbar.[482]

Schliesslich ist anzumerken, dass auch auf kantonaler Ebene zahlreiche bereichsspezifische Sondervorschriften mit Datenschutzbezug bestehen. Hierzu gehören beispielsweise Vorgaben in Gesundheitsgesetzen oder damit verbundenen Erlassen, z.B. betreffend Schweigepflicht oder Aufbewahrung von Patientendokumentationen[483]. Auch bei diesen Sonder-Vorschriften, die den allgemeinen bereichsübergreifenden Vorschriften vorgehen,[484] stellt sich jeweils die Frage, ob sie eine abschliessende Regelung enthalten und Raum für die ergänzende Anwendung der allgemeineren Vorschriften belassen.

4.3.3 Kernanforderungen des kantonalen Datenschutzrechts

a) Datenschutzrechtliche Rollen

Vor dem Blick auf die einzelnen Vorgaben der kantonalen Datenschutzgesetze ist zunächst auf die Regelung der datenschutzrechtlichen Rollen einzugehen. Die Untersuchung präsentiert diesbezüglich eine gänzlich unterschiedliche Rechtslage in allen drei Kantonen.

Am einfachsten zu erfassen ist dabei die Reglung im Kanton Waadt. Denn diese entspricht derjenigen des nDSG und damit auch derjenigen der EU-DSGVO. So werden die in den Vorgaben enthaltenen Pflichten jeweils dem Verantwortlichen ("responsable du traitement") auferlegt.[485] Dieser wird ferner identisch umschrieben wie in den genannten beiden Erlassen, indem auf die Entscheidung über Zweck und Mittel abgestellt wird.[486] Dasselbe gilt für den Auftragsbearbeiter ("sous-traitant").[487]

Einen anderen Weg geht der Kanton St.Gallen. Dieser sieht eine Sondervorschrift vor, die ähnlich auch (noch) im geltenden DSG enthalten ist.[488] Danach ist für die Einhaltung des Datenschutzes verantwortlich,

---

480 Botschaft zum DSG, BBl 1988 S. 483.

481 Vgl. für das HFG, BRUNNER, in: RÜTSCHE (Hrsg.), SHK-HFG, 2015, Vorb. Zu Art. 56 ff. N 8 ff.

482 Vgl. dazu oben Abschnitte 4.1.2 und 4.2.2; ferner für das HFG, BRUNNER, in: Rütsche (HRSG.), SHK-HFG, 2015, Vorb. Zu Art. 56 ff. N 5 ff.

483 Vgl. z.B. § 15 des Zürcher Gesundheitsgesetzes (GesG) sowie das Zürcher Patientinnen- und Patientengesetz; die St.Galler Verordnung über die Rechtsstellung der Patientinnen und Patienten (PatV); das Waadtländer Loi sur la santé publique (LSP-VD).

484 BGE 124 I 176, E. 5c/ee; WALDMANN/OESCHGER, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 13 N 11; a.A. PRIEUR, Welches Datenschutzrecht ist für Spitäler als Arbeitgeber anwendbar? Beispiel: Kanton Bern, in: Jusletter 18. Mai 2015, Rz. 8, nach welcher nur ein Vorrang der besonderen Vorschriften bestehen soll, wenn diese strengere Regeln enthalten.

485 Vgl. nur Art. 10, Art. 13 und 14 LPrD-VD.

486 Art. 4 Abs. 1 Ziff. 8 LPrD-VD.

487 Art. 4 Abs. 1 Ziff. 9 LPrD-VD.

488 Vgl. Art. 16 DSG; ferner die Hinweise zu den praktischen Schwierigkeiten und dem Bezug zum Inhaber der Datensammlung WALDMANN/BICKEL, in: BELSER/EPINEY/WALDMANN (Hrsg.), Datenschutzrecht, 2011, § 12 N 119.

"wer Personendaten bearbeitet oder bearbeiten lässt".[489] Verantwortlich meint hier auch beweispflichtig für die Einhaltung der datenschutzrechtlichen Vorgaben.[490] Bei diesem Ansatz bleibt die faktische Entscheidungsbefugnis somit irrelevant und es wird ausschliesslich auf die Vornahme einer Bearbeitung abgestellt. Immerhin ergibt sich implizit aus der Regelung, dass die Verantwortlichkeit dem (bearbeitenden) öffentlichen Organ und nicht den Mitarbeitenden zugeschrieben wird. Entsprechend ist bei der Bearbeitung durch mehrere Organe, das verantwortliche Organ zu bezeichnen.[491] Hieraus lässt sich schliessen, dass die Organe dies auch selbst und losgelöst von der Entscheidungsbefugnis festlegen können.

Wiederum anders präsentiert sich die Ausgangslage im Kanton Zürich. Hier fehlt eine explizite Regelung zur und Definition der Verantwortlichkeit. Auch die einzelnen Pflichten werden grundsätzlich dem "öffentlichen Organ" als solchem auferlegt. Gleichwohl wird vereinzelt vom verantwortlichen Organ gesprochen[492] und, wie im Kanton St.Gallen, bei der gemeinsamen Bearbeitung durch mehrere Organe verlangt, dass die "Verantwortlichkeit" geregelt wird[493]. Gleichermassen wird festgelegt, dass das öffentliche Organ auch bei der Auftragsbearbeitung verantwortlich bleibt.[494] Die Kriterien dafür, welches Organ verantwortlich sein soll, werden jedenfalls nicht festgelegt und es scheint insofern bei der gemeinsamen Bearbeitung ebenfalls möglich zu sein, dies nach eigenem Ermessen und losgelöst von der Entscheidungsbefugnis festlegen zu können.[495]

b) Zweckbindungsgebot

Das bereits oben im Rahmen des DSG beschriebene Zweckbindungsgebot ist in allen der hier untersuchten kantonalen Gesetzen ebenfalls vorgesehen. Allerdings sind die Regelungen nicht einheitlich formuliert und weichen vom Wortlaut des nDSG ab.

Die Umschreibung im DSG-SG entspricht allerdings derjenigen des geltenden DSG. Denn die Regelung sieht vor, dass das öffentliche Organ Personendaten nach Massgabe des Zwecks, der in der Rechtsgrundlage festgelegt ist, bei der Beschaffung angegeben wurde oder aus den Umständen ersichtlich ist, bearbeitet. Insofern sind alle drei Elemente des DSG enthalten, wenn auch in anderer Reihenfolge und leicht anderer Umschreibung. Es gelten im Kanton St.Gallen insofern auch die beiden Teilgehalte der Zweckbestimmung und Zweckbindung.[496] Da auf Bundes-Ebene nach der hier vertretenen Auffassung keine Änderung

489 Art. 3 Abs. 1 DSG-SG.

490 Art. 3 Abs. 3 DSG-SG.

491 Art. 3 Abs. 2 DSG-SG.

492 § 12 Abs. 2 lit. a IDG-ZH und § 12a Abs. 1 IDG-ZH.

493 § 5 Abs. 1 IDG-ZH.

494 § 6 Abs. 2 IDG-ZH.

495 Auch die zum IDG-ZH ergangene Verordnung legt nur die Umsetzungsverantwortung fest, also letztlich, welche Stellen innerhalb der jeweiligen Verwaltungseinheit innerhalb ihres Zuständigkeitsbereichs zur Umsetzung der gesetzlichen Vorgaben verpflichtet sind, vgl. § 1 IDV-ZH.

496 Botschaft und Entwurf der St.Galler Regierung vom 20. Mai 2008, Datenschutzgesetz, ABl. SG Nr 25 2299 fff, S. 2312 f.

der Rechtslage erfolgt, also der Aspekt der Vereinbarkeit der Zwecke bzw. die Zweckkompabilität bei richtiger Auslegung bereits im geltenden Recht verankert ist,[497] sieht das DSG-SG ein mit dem (künftigen) Bundesrecht übereinstimmendes Zweckbindungsgebot vor. Es kann deshalb hierfür nach oben verwiesen werden.

Im Kanton Zürich enthält das IDG-ZH wiederum einen abweichenden Wortlaut.[498] Wiederum zeigt aber auch hier der Blick auf die Entstehungsgeschichte, dass die Regelung des bisherigen DSG übernommen wurde und die Änderung des Wortlauts bloss zur Vereinfachung und nicht zur Abweichung davon erfolgt.[499] Ferner ergibt sich daraus ebenfalls, dass auch hier beide Teilgehalte des Zweckbindungsgebots vorgesehen sind und hierfür auf die obigen Ausführungen zum DSG verweisen werden kann.

Nochmals anders ist der Wortlaut im LPrD-VD formuliert. Dieser deutet auf eine strengere Regelung hin als in den beiden anderen Kantonen oder auf Bundes-Ebene. Denn danach ist es nicht ausreichend, dass ein Zweck sich bloss aus den Umständen ergibt. Ferner ist dem öffentlichen Organ auch nur die Festlegung eines Zwecks gestattet, der sich aus dem Gesetz oder der Erfüllung der jeweiligen öffentlichen Aufgabe ergibt. Dass diese gegenüber dem DSG strengere Regelung gewollt war, zeigt die Entstehungsgeschichte der Vorschrift. So war nach dem Entwurf der Regierung noch eine mit dem aktuellen DSG entsprechende Formulierung vorgesehen.[500] Im Parlament des Kanton Waadt wurde dann jedoch die abweichende Formulierung gewählt und dies mit der Begründung, dass der Verwaltung mit der Regelung im Entwurf ein zu grosser Ermessensspielraum überlassen worden wäre.[501] Insofern präsentiert sich die Ausgangslage im Kanton Waadt etwas strenger als in den anderen beiden Kantonen. Wie bereits bei den Bundesorganen ausgeführt, dürfte die Auslegung, was ein bloss aus den Umständen erkennbarer/ersichtlicher Zweck ist, aber ohnehin darauf hinauslaufen, dass nur Zwecke darunterfallen, die sich aus der öffentlichen Aufgabe des Organs ergeben. Ferner sind auch hier die beiden erläuterten Teilgehalte verankert. Abgesehen von den erwähnten Besonderheiten kann jedoch ebenfalls auf die Ausführungen zu den Bundesorganen verwiesen werden.

Die Untersuchung der jeweiligen Normen macht deutlich, dass diesbezüglich einige Unterschiede gegenüber dem DSG und im Vergleich zueinander bestehen. Auch wenn die Regelungen in den Grundzügen übereinstimmen, hat gleichwohl stets eine Beurteilung im Einzelfall unter den jeweiligen kantonalen Vorschriften zu erfolgen. Bei der Sekundärnutzung von Gesundheitsdaten kann daher nicht darauf vertraut werden, dass bei der Einhaltung der auf Bundes-Ebene geltenden Vorschriften auch denjenigen des kantonalen Datenschutzrechts entsprochen wird.

c) Legalitätsprinzip

i.) Allgemeines zum Legalitätsprinzip

---

497 Insbesondere sind "kompatible"/"vereinbare" Zwecke als aus den Umständen ersichtliche bzw. erkennbare Zwecke zu qualifizieren; abzulehnen ist deshalb die Auffassung von ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 36.

498 § 9 Abs. 1 IDG-ZH: "Das öffentliche Organ darf Personendaten nur zu dem Zweck bearbeiten, zu dem sie erhoben worden sind, soweit nicht eine rechtliche Bestimmung ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall einwilligt.".

499 Vgl. Weisung des Zürcher Regierungsrats vom 9. November 2005, ABl 2005 Nr. 47 S. 1297, S. 1307, wo auf die bisherige Regelung des § 4 Abs. 4 DSG-ZH verwiesen wird, die derjenigen des geltenden DSG entspricht.

500 Vgl. Exposé des Motifs et Projets de la Loi sur la Protection des Données, Bulletin du Grand Conseil, Législature 2007-2012, Tome 1 Conseil d'Etat 119 ff., S. 33.

501 Vgl. Bulletin du Grand Conseil, Législature 2007-2012, TOME 1 Grand Conseil, S. 217.

Die zweite zentrale Anforderung des kantonalen Datenschutzrechts besteht im Legalitätsprinzip. Wie erwähnt, ist dieses Prinzip eine Konkretisierung einer Anforderung, die generell im öffentlichen Recht gilt und daher auch ohne explizite Regelung im kantonalen Recht zur Anwendung gelangen würde. Gleichwohl sehen alle Kantone ausdrückliche Vorschriften mit ähnlichen Inhalten vor, die allerdings, wie noch zu zeigen ist, zumindest in den Details nicht einheitlich und auch abweichend vom DSG ausgestaltet sind.

ii.) Forschungsprivileg als besondere Grundlage

Zunächst findet sich aber in allen drei Kantonen zumindest eine dem Forschungsprivileg auf Bundes-Ebene entsprechende Ausnahmeregelung.[502] Der Geltungsbereich erstreckt sich – identisch wie im DSG – in allen Regelungen auf die Bearbeitung von Personendaten zu nicht personenbezogenen Zwecken. In den Augen aller drei kantonaler Gesetzgeber soll dies ebenfalls wie im DSG insbesondere zumindest bei der Statistik und Forschung denkbar sein.[503] Folglich darf von einem identischen Verständnis ausgegangen werden und die Bestimmungen werden insbesondere, aber nicht nur,[504] dann greifen können, wenn die Zwecke der Bearbeitung auch mit pseudonymisierten oder anonymisierten Daten erreicht werden könnte.[505]

Für Bearbeitungen, die in den so definierten Anwendungsbereich der Forschungsausnahme fallen, stellen die Kantone sodann im Wesentlichen dieselben Anforderungen, wie sie zumindest im geltenden DSG enthalten sind:

1. Erforderlich ist demnach grundsätzlich auch in den Kantonen, dass die Daten anonymisiert werden, sobald der Zweck der Bearbeitung die Anonymisierung zulässt. Zürich weicht allerdings hiervon ab, indem die Anonymisierung vermeintlich stets verlangt wird und nicht erst, "sobald" es der Zweck zulässt. Der erforderliche Zeitpunkt der Anonymisierung ist insofern noch weniger klar als durch die andere aus dem DSG bekannte Umschreibung.

2. Bei einer Bekanntgabe des Ergebnisses müssen Rückschlüsse auf betroffene Personen ferner ausgeschlossen sein, wobei im Kanton Zürich aus den Auswertungen generell, also unabhängig von einer Bekanntgabe, keine solchen Rückschlüsse möglich sein dürfen.

3. Die zusätzliche Anforderung für die Bekanntgabe und Weiterbearbeitung durch Dritte sieht der Kanton Zürich sodann im Unterschied zu den beiden anderen Kantonen sowie zum DSG nicht vor. Im Kanton Waadt ist hierbei zumindest verlangt, dass ein Empfänger der Daten diese seinerseits nur mit der Zustimmung des Organs, das die Daten bekanntgegeben hat, (weiter-)bekanntgeben darf. Der Kanton St.Gallen verlangt für die Bekanntgabe demgegenüber eine schriftliche Verpflichtung des Datenempfängers zur Einhaltung der anderen beiden bereits genannten Voraussetzungen und zur Unterlassung von (jeglichen) Weitergaben an andere Dritte.

---

502 § 9 Abs. 2 IDG -ZH; Art. 24 LPrD-VD; Art. 7 DSG-SG.

503 In den Kantonen St.Gallen und Waadt werden diese, gemeinsam mit Planung, bereits im Gesetz selbst erwähnt, vgl. Art. 24 Abs. 1 LPrD-VD; Art. 7 Abs. 1 DSG-SG, während in Zürich nur in der Weisung entsprechende Hinweise enthalten sind, aber Planung nicht explizit genannt wird, Weisung des Zürcher Regierungsrats vom 9. November 2005, ABl 2005 Nr. 47 S. 1297, S. 1307.

504 Dies ergibt sich aus den jeweiligen Anforderungen betr. Anonymisierung in Art. 24 Abs. 1 lit. a LPrD-VD; Art. 7 Abs. 1 DSG-SG, § 9 Abs. 2 IDG -ZH, die andernfalls wenig Sinn ergeben würden.

505 KOÇ, in: PASSADELIS/ROSENTHAL/THÜR (Hrsg.), Datenschutzrecht, 2015, Rz. 30.10.; ähnlich RAMPINI, in: MAURER-LAMBROU/BLECHTA (Hrsg.), BSK-DSG/BGÖ, 2014, Art. 13 Rz. 42.

Es fehlt in allen Kantonen aber die neu eingeführte Anforderung, wonach das öffentliche Organ privaten Personen besonders schützenswerte Personendaten nur so bekanntgeben darf, dass die betroffenen Personen nicht bestimmbar sind.

Selbst wenn somit im Grundsatz auch den kantonalen Organen eine Berufung auf die Forschungsausnahme möglich ist, sind die Anforderungen, gerade in Fällen, wo mehrere Gesetze zur Anwendung gelangen könnten, mit besonderer Sorgfalt zu prüfen, bestehen doch zahlreiche Abweichungen. Die gesetzlichen Bezugnahmen auf Anonymisierung und Bestimmbarkeit führen hier ferner zu noch mehr Unklarheiten als auf Bundesebene. Grund dafür ist, dass noch weniger klar ist, welche Perspektive für die Bestimmbarkeit einer Person massgeblich sein soll. Hinzu kommt, dass in den Kantonen Waadt und Zürich auch keine juristischen Personen bestimmbar sein dürfen. Die Hindernisse für die Berufung auf die Ausnahme sind auf kantonaler Ebene insofern noch höher als auf Bundesebene.

iii.) Anforderungen an gesetzliche Grundlagen für die Sekundärnutzung

Wie eingangs erläutert, ist auch den kantonalen Organen ausserhalb dieser besonderen Ausnahmeregelung jegliche Bearbeitung von Personendaten grundsätzlich nur erlaubt, wenn eine gesetzliche Grundlage dies ermöglicht. Neben der Verankerung des Grundsatzes ist allen drei kantonalen Regelungen Folgendes gemeinsam:

1. Für die Bearbeitung besonders schützenswerter Daten ist grundsätzlich eine Grundlage in einem Gesetz im formellen Sinne erforderlich, eine Ermächtigung in einer Verordnung der Regierung genügt demnach nicht.[506]

2. Für die Bekanntgabe von Daten ist eine besondere Regelung vorgesehen,[507] wobei auch hier für besonders schützenswerte Daten grundsätzlich eine Ermächtigung in einem formellen Gesetz verlangt wird[508].

Weiter sind in den Kantonen jedoch zahlreiche Besonderheiten vorgesehen. So ist im Kanton Zürich bspw. für die gewöhnliche Bearbeitung von gewöhnlichen Personendaten keine explizite Ermächtigung erforderlich. Vielmehr soll es genügen, wenn die Bearbeitung zur Erfüllung einer Aufgabe erforderlich ist, also bloss eine sog. mittelbare gesetzliche Grundlage existiert.[509]

Schwierigkeiten bereitet sodann die Beantwortung der Frage, welche Anforderungen konkret an eine hinreichende Grundlage gestellt werden. Ausdrückliche Regelungen zur inhaltlichen Bestimmtheit der Normen sind in den einzelnen Gesetzen jedenfalls keine enthalten.[510] Allgemein lässt sich aber festhalten, dass der datenschutzrechtliche Verhältnismässigkeitsmassstab auch hier gelten dürfte:[511] Je sensibler die zu verarbei-

[506] § 8 Abs. 2 IDG -ZH; Art. 5 Abs. 2 LPrD-VD; Art. 5 Abs. 2 DSG-SG.

[507] § 16 IDG -ZH; Art. 15 LPrD-VD; Art. 11 ff. DSG-SG.

[508] § 17 Abs. 1 lit. a IDG -ZH; Art. 15 Abs. 1 lit. a i.V.m. Art. 5 Abs. 2 LPrD-VD; Art. 13 Abs. 1 lit. a DSG-SG.

[509] § 8 Abs. 1 IDG-ZH; Weisung des Zürcher Regierungsrats vom 9. November 2005, ABl 2005 Nr. 47 S. 1297.

[510] Vgl. immerhin der Hinweis in der Weisung des Zürcher Regierungsrats vom 9. November 2005, ABl 2005 Nr. 47, S. 1313.

[511] Vgl. zum Begriff BÜHLMANN/SCHÜEPP Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 54.

tenden Daten und je einschneidender die Datenbearbeitung, desto höhere Anforderungen sind an die Bestimmtheit der Norm zu stellen.[512] Eine stichprobenartige Auswertung der Vielzahl von möglichen bereichsspezifischen Erlassen in den einzelnen Kantonen lässt dabei nur schwer ein Muster erkennen.

Ohne Anspruch auf Vollständigkeit der Auswertung ist jedoch davon auszugehen, dass auch in den Kantonen im Wesentlichen die unter dem DSG erläuterten Anforderungen gelten. Damit eine Norm hinreichend bestimmt ist und damit als Ermächtigung gilt, muss also namentlich das jeweilige Organ, der Zweck und das Ausmass der Bearbeitung vorgesehen sein. Soll auch die Bearbeitung von besonders schützenswerten Daten gestattet sein, muss dies im betreffenden Gesetz ausdrücklich erwähnt sein. Unklar ist diesbezüglich aber, ob hier im Vergleich zum DSG ein strengerer Massstab gelten soll, wird doch vereinzelt nicht bloss von besonders schützenswerten Daten gesprochen, sondern bspw. explizit von Daten zur Religionszugehörigkeit.[513]

Soll auch eine Bekanntgabe gestattet sei, muss diese ebenfalls gesondert aufgeführt sein und die blosse Ermächtigung zur Bearbeitung genügt nicht.[514] Nicht ausdrücklich erwähnt, aber von selbst versteht sich angesichts der verfassungsrechtlichen Hierarchie,[515] dass die Ermächtigung auch in einem auf das kantonale Organe anwendbaren Spezialgesetz des Bundes enthalten sein kann.[516]

iv.) Ausnahmen vom Legalitätsprinzip

Ähnlich wie auch auf Bundesebene bestehen auch in den untersuchten Kantonen weitere Ausnahmen und Sonderregelungen, die das soeben erläuterte Legalitätsprinzip bis zu einem gewissen Grad relativieren. Im vorliegend interessierenden Kontext sind dies ebenfalls primär die folgenden beiden Ausnahmeregelungen:

3. Mittelbare gesetzliche Grundlage:[517] Anders als im Kanton Zürich, wo eine Regelung dazu fehlt, kann die Bearbeitung von Gesundheitsdaten durch die öffentlichen Organe der anderen beiden Kantone auch ohne Grundlage in einem Gesetz im formellen Sinne zulässig sein. Vorausgesetzt ist dabei, dass die Bearbeitung für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich ist. Nicht restlos klar ist jedoch, ob, wie künftig auf Bundesebene[518] eine Ermächtigungsgrundlage in einem Gesetz im materiellen Sinn vorhanden sein muss. Selbst für den Fall, dass eine Bearbeitung der Gesundheitsdaten also tatsächlich als unentbehrlich betrachtet werden könnte, müsste zumindest eine Grundlage auf Verordnungsstufe vorliegen.

---

512 Vgl. auch WALDMANN/OESCHGER, in: BESLER/EPINEY/WALDMANN, Datenschutzrecht, 2011, § 13 N 46.

513 S. z.B. für den Kanton Zürich §3a Abs. 2 lit. f. Volksschulgesetz mit expliziter Aufzählung im Vergleich zu § 52 Abs. 5 des Polizeigesetzes.

514 Weisung des Zürcher Regierungsrats vom 9. November 2005, ABl 2005 Nr. 47, S. 1312.

515 Art. 49 Abs. 1 BV.

516 S. z.B. auch Beispiel als hinreichenden Grundlage bezeichneten Meldepflicht in Art. 314d Abs. 1 ZGB, im Merkblatt der Datenschutzbeauftragten des Kantons Zürich, Datenschutz im Sozialbereich, S. 9; Unvollständig deshalb aber die gesetzliche Definition in Art. 4 Abs. 13 LPrD-VD sowie die Umschreibung in Botschaft und Entwurf der St.Galler Regierung vom 20. Mai 2008, Datenschutzgesetz, ABl. SG Nr. 25 2299 fff, S. S. 2310.

517 Art. 5 Abs. 2 lit. b DSG-SG; Art. 5 Abs. 2 lit b LPrD-VD.

518 Vgl. zur Diskussion unter dem geltenden DSG, BÜHLMANN/SCHÜEPP Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 25.

4. Einwilligung der betroffenen Person:[519] Eine Einwilligung der betroffenen Personen kann zumindest eine Ausnahme vom Erfordernis der gesetzlichen Grundlage im formellen Sinne darstellen. Unklar ist aber, ob dies auch für das Erfordernis der gesetzlichen Grundlage im materiellen Sinne gilt.[520] Inwieweit die Ausnahme im Kanton Zürich, abgesehen von der Bekanntgabe, wo eine Regelung enthalten ist,[521] überhaupt greifen kann, bleibt sodann ebenso fragwürdig. Hinzu kommen die bereits erläuterten Anforderungen an die Gültigkeit der Einwilligung. Erstens dürften infolge des im Kanton St.Gallen vorgesehen Kriteriums "im Einzelfall" noch strengere Anforderungen an die Bestimmtheit gelten.[522] Zweitens stellen sich angesichts des Verhältnisses zwischen betroffener Person und öffentlichen Organen zusätzliche Fragen in Bezug auf das Kräfteungleichgewicht und damit Zweifel an der Freiwilligkeit bzw. Wirksamkeit der Einwilligungen.[523] Drittens dürfte auch der praktische Umgang mit dem Umstand, dass Einwilligungen jederzeit widerrufen werden können, Fragen aufwerfen.[524] Immerhin kann die Ausnahme in den Kantonen Waadt und St.Gallen, anders als im nDSG, aber auch bei (Gesundheits-)Daten greifen, die von der betroffenen Person allgemein zugänglich gemacht wurden.[525] Allerdings dürfte hier die Einschränkung bestehen, dass eine Nutzung nur im Rahmen des erkennbaren Veröffentlichungszweck zulässig ist.

Ausgehend davon bieten die Ausnahmen vom Legalitätsprinzip auch auf kantonaler Ebene nur einen beschränkten Raum für die Abstützung von Sekundärnutzungen von Gesundheitsdaten.

4.3.4 Weitere Anforderungen

Neben den soeben beschriebenen Kernanforderungen, sind auch bei Datenbearbeitungen durch kantonale Organe diverse weitere Anforderungen zu beachten. Hervorzuheben ist dabei zunächst wiederum der Datenbearbeitungsgrundsatz der Verhältnismässigkeit, der lediglich im Kanton Waadt ausdrücklich so gesetzlich verankert ist.[526] Eine konkrete Umschreibung fehlt, wobei die Gesetzesmaterialien bekräftigen, dass der Grundsatz im Wesentlichen verstanden wird wie auf Bundesebene. Es dürfen demnach nur die Daten verarbeitet werden, die für die Erfüllung der Aufgaben der für die Verarbeitung Verantwortlichen erforderlich sind, und es ist eine Interessenabwägung zwischen der potenziellen Beeinträchtigung durch die Verarbeitung personenbezogener Daten und dem Nutzen der Datenbearbeitung vorzunehmen.[527] Im Ergebnis ähnlich findet sich Kanton Zürich eine Bestimmung, die verlangt, dass Datenbearbeitungssysteme und -programme so gestaltet werden, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig

---

519 Art. 5 Abs. 2 lit. c Ziff. 1 DSG-SG; Art. 5 Abs. 2 lit c LPrD-VD.

520 Vgl. dazu auf Bundesebene BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 25.

521 § 16 Abs. 1 lit. b IDG-ZH.

522 Vgl. zu diesem Kriterium BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021, Rz. 39 ff.

523 Vgl. dazu z.B. MEIER, Protection des données, 2010, Rz. 856 ff.

524 Vgl. dazu z.B. MEIER, Protection des données, 2010, Rz. 840 ff.

525 Art. 5 Abs. 2 lit. c Ziff. 2 DSG-SG; Art. 5 Abs. 2 lit c LPrD-VD.

526 Art. 7 LPrD-VD.

527 Exposé des Motifs et Projets de la Loi sur la Protection des Données, Bulletin du Grand Conseil, Législature 2007-2012, Tome 1 Conseil d'Etat 119 ff., S. 33.

sind.[528] Festgehalten wird in derselben Bestimmung explizit auch der verwandte Grundsatz der Speicherbegrenzung, wonach Personendaten gelöscht, anonymisiert oder pseudonymisiert werden müssen, sobald und soweit dies möglich ist.[529] Die Regelungen stimmen somit im Ergebnis überein und sind im Einklang mit der Regelung auf Bundesebene.

Demgegenüber fehlt im Kanton St.Gallen eine vergleichbare Norm. Erst ein Blick in die Gesetzesmaterialien macht jedoch deutlich, dass der Grundsatz der Verhältnismässigkeit gleichermassen auch in St.Gallen gelten soll. Es wurde lediglich auf die ausdrückliche Erwähnung im SG-DSG verzichtet, weil es sich um ein verfassungsrechtliches Prinzip handle, das ohnehin gelte und nicht auf Gesetzesstufe wiederholt werden solle.[530] Insofern muss sich in allen drei Kantonen die Datenbearbeitung auf das für die Erfüllung der jeweiligen Aufgabe erforderliche beschränken und für die betroffenen Personen zumutbar sein. Eine diesem Grundsatz widersprechende (und somit unverhältnismässige) Datenbearbeitung durch kantonale Organe ist rechtswidrig und kann – anders als bei privaten Verantwortlichen – auch nicht durch einen Rechtfertigungsgrund legitimiert werden. Die Umsetzung dieser Anforderungen in der Praxis gestaltet sich dabei auch auf kantonaler Ebene nicht leichter.

Wie das DSG für Private und Bundesorgane, sehen auch die kantonalen Datenschutzgesetze Regelungen für die Auslandsbekanntgabe von Personendaten vor.[531] Alle drei untersuchten Kantone schreiben vor, dass Personendaten grundsätzlich nicht in Länder ohne angemessenes Datenschutzniveau bekanntgegeben werden dürfen. Solche Bekanntgaben können jedoch dann ausnahmsweise zulässig sein, wenn zusätzliche Massnahmen ergriffen werden.[532] Die Ausgangslage ist demnach in allen Kantonen im Wesentlichen gleich wie auf Bundesebene. Die Urteile des Europäischen Gerichtshofs in Bezug auf das Datenschutzniveau in den USA[533] haben auch in den Kantonen dazu geführt, dass Bekanntgaben in diese Länder als problematisch betrachtet werden.[534] Auch wenn somit im Grundsatz ein einheitliches Grundverständnis herrscht, sind in der Praxis doch Unterschiede bemerkbar, wie bspw. der aktuelle Beschluss des Zürcher Regierungsrats zeigt, mit welchem die Nutzung von Microsoft Office 365, die eine Übermittlung in die USA beinhalten kann,[535] bewilligt wurde. Demgegenüber erachtet bspw. die Fachstelle Datenschutz des Kantons St.Gallen die Speicherung von Daten in den USA als nicht angemessen und verlangt in Bezug auf Gesundheitsdaten, als besonders schützenswerte Daten, die Wahl von Anbietern ohne US-Bezug.[536] Dies verdeutlicht, dass jeder Kanton mit der Ausgangslage potentiell unterschiedlich umgeht. Dies kann nicht nur die grenzüberschreitende-, sondern auch die kantonsübergreifende Kooperation beeinträchtigen.

---

528 § 11 Abs. 1 IDG-ZH.

529 § 11 Abs. 2 IDG-ZH.

530 Botschaft und Entwurf der St.Galler Regierung vom 20. Mai 2008, Datenschutzgesetz, ABl. SG Nr. 25 2299 fff, S. 2335.

531 Vgl. Art. 16 Abs. 1 DSG-SG; Art. 17 Abs. 1 LPrD-VD; § 19 IDG-ZH.

532 Art. 16 Abs. 2 DSG-SG; Art. 17 Abs. 2 LPrD-VD; § 19 lit. c IDG-ZH.

533 Zuletzt Urteil des Europäischen Gerichtshofs vom 16. Juli 2020, C-311/18 (Schrems II).

534 Vgl. nur das Merkblatt von Privatim (Konferenz der schweizerischen Datenschutzbeauftragten), Cloud-spezifische Risiken und Massnahmen, S. 2.

535 Beschuss vom 30. März 2022, RRB-2022-0542, Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365).

536 Tätigkeitsbericht der kantonalen Fachstelle für Datenschutz über das Jahr 2020, S. 3 und 7.

Schliesslich sei darauf hingewiesen, dass auf kantonaler Ebene eine Vielzahl weiterer einschlägiger Spezialgesetze besteht, ist doch das Gesundheitswesen grundsätzlich Sache der Kantone.[537] Hier sind bspw. die aus der kantonalen Gesundheitsgesetzgebung hervorgehenden Regelungen zu den Patientenrechten zu nennen.[538] Diese enthalten wiederum detaillierte Vorschriften, welche vielfach auch einen Bezug zum Datenschutz aufweisen. Der Einbezug dieser Regelung in die Prüfung wird dabei regelmässig neue Fragen auf und es stellt sich bei jeder Vorschrift die Frage nach dem Verhältnis zu den übrigen Vorschriften auf Bundes- und kantonaler Ebene.[539] Diese Sonderregelungen führen zusätzlich zur Unübersichtlichkeit der Regelungen im Gesundheitswesen und können eine praktische Hürde für die Weiterverwendung von Gesundheitsdaten darstellen.

4.3.5 Konsequenzen bei Datenschutzverletzungen

Die Verletzung der oben beschriebenen kantonalen Datenschutzbestimmungen kann verschiedene negative Rechtsfolgen nach sich ziehen. Diese sind jedoch wiederum nicht einheitlich geregelt. Hervorzuheben ist einerseits, dass auch in sämtlichen untersuchten Kantonen Strafsanktionen für bestimmte Datenschutzverletzungen drohen. So sehen die kantonalen Datenschutzerlasse in Zürich und in St.Gallen Bussen für auftragswidrige Datenbearbeitungen durch die beauftragte Person vor [540], während im Kanton Waadt generell Vertraulichkeitsverletzungen strafrechtlich geahndet werden können.[541] Anderseits können die zuständigen Stellen bei mangelhafter Umsetzung der datenschutzrechtlichen Vorschriften Anordnungen, wie z.B. Bearbeitungsverbote oder Datenlöschungen, erlassen[542] oder solche zumindest bei der zuständigen Stelle beantragen.[543]

4.3.6 Fazit: Hindernisse nach kantonalem Datenschutzrecht

Die Analyse der ausgewählten drei kantonalen Datenschutzgesetze verdeutlicht, dass sich die Anforderungen grundsätzlich sehr nahe an denjenigen des Bundes orientieren. Die Nutzung von Gesundheitsdaten ist deshalb auch für kantonale Organe unter vergleichbaren Bedingungen wie auf Bundesebene erlaubt. Gleichwohl wird in vielerlei Hinsicht von den Vorgaben des DSG abgewichen. Bereits dies führt zu einem grossen Prüfungsaufwand in Projekten, wo kantonsübergreifende Datenbearbeitungen erfolgen sollen. Die Unterschiede in den einzelnen Bereichen verstärken die bereits auf Bundesebene festgestellten Unsicherheiten und die föderale Ausgestaltung der Datenschutzgesetzgebung ist als sehr grosses Hindernis für die Sekundärnutzung von Gesundheitsdaten zu bezeichnen. Auch hier wiegen die Unsicherheiten umso schwerer als für gewisse Verstösse ebenfalls strafrechtliche Sanktionen drohen.

---

[537] Vgl. nur BGE 139 I 242, E. 3.1.

[538] Vgl. Zürcher Patientinnen- und Patientengesetz; Loi sur la santé publique (LSP-VD); Verordnung über die Rechtsstellung der Patientinnen und Patienten (PatV-SG).

[539] Vgl. z.B. auch § 29 Zürcher Patientinnen- und Patientengesetzes oder Art. 25 des Loi sur la santé publique (LSP-VD), wo ebenfalls Einwilligungsregelungen für die Forschung enthalten sind.

[540] Art. 40 DSG-SG; § 40 IDG-ZH.

[541] Art. 41 LPrD-VD.

[542] § 36 und 36a IDG-ZH und Art. 38 Abs. 1 lit. c LPrD-VD.

[543] Art. 33 und 34 DSG-SG.

4.4 Weitere relevante Rechtsakte auf Bundesebene

Wie bereits einleitend ausgeführt, existiert auf Bundesebene eine grosse Zahl weiterer Vorschriften für die Nutzung von Gesundheitsdaten. Gleiches gilt auch auf kantonaler Ebene. Nachfolgend werden die zentralsten Bundes-Vorschriften und deren Anforderungen an die Sekundärnutzung dargestellt.

4.4.1 Strafgesetzbuch: Berufs-, Amts- und Forschungsgeheimnis

Von grundlegender Bedeutung im Gesundheitssektor sind die strafrechtlichen geschützten Geheimnisse, namentlich das Berufsgeheimnis der Ärztinnen und Ärzte in Art. 321 StGB. Darüber hinaus wird die Tätigkeit im Gesundheitswesen, wo öffentliche Aufgaben erfüllt werden, sehr oft auch vom Amtsgeheimnis nach Art. 320 StGB erfasst, wie z.B. bei Angestellten der SUVA[544]. Weiter existiert bereits im Strafgesetz selbst eine Sonderbestimmung für Personen, die in der Humanforschung tätig sind.[545] Es ergibt sich deshalb bereits aus diesen im Strafgesetz verankerten Bestimmungen ein breites Netz an Geheimhaltungsvorschriften, die durch die Vielzahl an zusätzlichen Schweigepflichten in anderen Gesetzen[546] verdichtet werden. Die jeweiligen Anwendungsbereiche und das (teilweise strittige) Verhältnis zueinander ist nicht immer leicht und in der Praxis oftmals nur schwer verständlich erklärbar.[547] Die parallele Anwendung der einzelnen Vorschriften führt im Ergebnis aber dazu, dass im Gesundheitswesen kaum mehr eine Tätigkeit einer Berufsgruppe denkbar ist, die nicht von einem der geschützten Geheimnisse oder Schweigepflichten erfasst ist. Die erwähnten Vorschriften gelten ferner parallel und unabhängig vom jeweils anwendbaren Datenschutzrecht.[548]

Den Geheimhaltungsvorschriften liegt im Wesentlichen derselbe Geheimnisbegriff zugrunde. Unter die Geheimhaltungspflicht fällt alles, was den Personen in der Ausübung ihrer Tätigkeit, also des Berufs, des Amts oder der Forschung, anvertraut worden ist oder was sie in dessen bzw. deren Ausübung wahrgenommen haben.[549] Als Geheimnis kommen nur Tatsachen in Frage, die weder offenkundig noch allgemein zugänglich, sondern nur einem beschränkten Kreis von Personen bekannt ist. Ferner ist erforderlich, dass die Person, welche die Tatsache betrifft ("Geheimnisherr"), also z.B. die Patientin oder der Patient, einen ausdrücklich oder stillschweigend bekundeten Geheimhaltungswillen und ein schutzwürdiges Geheimhaltungsinteresse hat.[550] Diese Anforderungen sind bei Gesundheitsdaten in der Praxis rasch gegeben. Als geschütztes Geheimnis gilt schon die Tatsache der Beziehung einer Person zum Geheimnisträger, also bspw. der Behandlung durch einen Arzt.[551]

---

544 Vgl. BGE 135 IV 198, wo diese ebenfalls als Beamte (und damit implizit als mögliche Täter einer Amtsgeheimnisverletzung) qualifiziert wurden.

545 Art. 321bis StGB.

546 Vgl. z.B. Art. 33 ATSG für den Bereich der Sozialversicherungen.

547 Vgl. z.B. nur schon in Bezug auf die Unterstellung von Ärzten in Spitälern: AEBI-MÜLLER/FELLMANN/GÄCHTER/ RÜTSCHE /TAG, Arztrecht, 2016, S. 459 : "*Medizinalpersonen im öffentlichen Gesundheitsdienst, namentlich Stadt-, Kantons- und Gefängnisärzte sowie solche an kantonalen und kommunalen Spitälern, unterstehen alternativ Art. 320 StGB oder Art. 321 StGB, je nachdem, ob das Geheimnis ihre amtlichen – dann gilt Art. 320 StGB – oder therapeutischen Aufgaben – hier gilt Art. 321 StGB – betrifft*"; ähnlich WOHLERS, in. Handkommentar StGB, 2020, Art. 320 N 12 mit Hinweis auf abweichende Meinungen.

548 Vgl. BISCHOF, Datenschutz und Berufsgeheimnis im ambulanten Leistungsbereich, 2020, S. 41 f.

549 Vgl. den fast identischen Wortlaut der Bestimmungen in Art. 320 ff. StGB.

550 WOHLERS, in: Handkommentar StGB, Art. 320 N 3.

551 TRECHSEL/VEST, in: TRECHSEL/PIETH (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, Art. 321 N 20.

Die Geheimhaltungsvorschriften verbieten die Offenbarung von Geheimnissen. Ein Geheimnis offenbart, wer es einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme zumindest ermöglicht.[552] Zur Vermeidung von Verstössen gegen Geheimhaltungsvorschriften im Rahmen der Sekundärnutzung von Gesundheitsdaten besteht der erste Ansatz deshalb darin, eine solche Kenntnisnahme von vornherein zu verhindern. Die rechtliche Schwierigkeit besteht allerdings darin, den Kreis der berechtigten Personen zu umschreiben, innerhalb dessen die Information geheim zu halten ist. Dieser Kreis unterscheidet sich je nach betroffenem Geheimnis und ist im Übrigen auch strittig. Irrelevant ist dabei zunächst aber, inwieweit die andere Person ebenfalls einer Geheimhaltungspflicht untersteht.[553] Berichtet der Arzt eines Kantonsspitals somit dem zuweisenden Hausarzt vom Verlauf der Operation seines Patienten, liegt bereits eine Offenbarung vor. In Bezug auf das Amtsgeheimnis zählen aber auch Personen innerhalb derselben Verwaltungseinheit oder Mitarbeitende einer in der Verwaltungshierarchie übergeordneten Behörde, sofern der Dienstweg eingehalten ist.[554] Demgegenüber ist namentlich beim Berufsgeheimnis der Ärztinnen und Ärzte (sowie Anwältinnen und Anwälte) unklar und strittig, wie weit der Kreis der ermächtigten Personen zu ziehen ist.[555] Es werden mitunter sehr strenge Auffassungen vertreten, die praktisch kaum noch umsetzbar wären.[556] Denn danach werden externe Dritte, d.h. auch jegliche beigezogenen Dienstleister (z.B. Cloud-Anbieter) mit Möglichkeit des Zugriffs auf die geheimnisgeschützten Daten, anders als die mit den entsprechenden Aufgaben betrauten internen Mitarbeiter, regelmässig nicht zu diesem Kreis gezählt.

Auch wenn ein grosser Teil der Lehre diese Auffassung zu Recht ablehnt[557] und auch das Bundesgericht[558] – zumindest im Grundsatz – von einem weiteren Begriff der Hilfspersonen und damit einem weiteren Kreis der berechtigten Personen ausgeht, verbleibt in diesem Punkt erhebliche Rechtsunsicherheit. Verstärkt wird diese durch Fragestellungen, die sich bei Unternehmen mit Bezug zu den USA und den potentiellen Zugriffsmöglichkeiten der US-Behörden (insb. Nachrichtendienste) ergeben.[559]

Vor diesem Hintergrund wird zwar in vielen Fällen auch eine Mitteilung von Gesundheitsdaten an Personen ausserhalb des engen Teams der zuständigen Mitarbeitenden keine Offenbarung darstellen. Allerdings bleibt stets ein Restrisiko, das angesichts der Strafdrohung kaum jemand in Kauf nehmen will. Es gilt deshalb bei jeder Person, der Zugriff auf Gesundheitsdaten gewährt wird, zu prüfen, inwieweit dies als Offenbarung betrachtet werden muss und zusätzliche Massnahmen zu ergreifen sind oder nicht. Dies gilt somit nicht nur, wenn bspw. Patientendaten eines Spitals im Rahmen eines Forschungsvorhabens auch an andere Spitäler übermittelt werden sollen, sondern auch wenn im Rahmen der Sekundärnutzung von Gesundheitsdaten externe Dienstleister Zugriff erhalten sollen.

---

552 BGE 142 IV 65, E. 5.1.

553 Vgl. z.B. BGE 114 IV 44, E. 3 b.

554 WOHLERS, in: Handkommentar StGB, 4. Aufl., 2020, Art. 320 N 7.

555 Vgl. z.B. ausführlich SCHWARZENEGGER/THOUVENIN /STILLER, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, 2019.

556 WOHLERS, Outsourcing durch Berufsgeheimnisträger, digma 2016 S. 114, 116: Danach soll auf den objektivierten Willen des Geheimnisherrn abgestellt werden und danach geprüft werden, inwieweit dieser das Geheimnis nicht nur mit dem primären Geheimnisträger, z.B. dem Arzt, sondern auch mit anderen Personen teilen will. Von einem solchen Willen könne nur ausgegangen werden, wenn die Offenbarung an den Dritten zur sachgerechten Erledigung der vom Geheimnisherr.

557 Vgl. insbesondere BISCHOF, Datenschutz und Berufsgeheimnis im ambulanten Leistungsbereich, 2020, S. 89 ff.

558 Vgl. in Bezug auf das Anwaltsgeheimnis: BGer Urteil vom 4.6.2017, 2C_1083/2017, E. 7.3.

559 Vgl. dazu ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020.

In der Praxis suchen die Verantwortlichen deshalb regelmässig nach zusätzlichen Mitteln zur Absicherung. Eines dieser Mittel ist, neben der Anonymisierung, auch die Pseudonymisierung. Denn richtigerweise stellt die Übermittlung verschlüsselter Daten keine Offenbarung dar, wenn der Empfänger über keinen Zugang zum Schlüssel verfügt.[560] Wie bereits erläutert, bestehen allerdings auch hier nicht nur rechtliche, sondern auch beweistechnische und faktische Unsicherheiten. Auch bei einer verschlüsselten Bereitstellung von Daten kann die Ergreifung weiterer Absicherungen ratsam sein. Hierzu zählt die Zustimmung zur Offenbarung seitens des Geheimnisträgers, also die Entbindung von der jeweiligen Geheimhaltungspflicht. Hier gelten im Wesentlichen dieselben Anforderungen wie in Bezug auf die erläuterten datenschutzrechtlichen Einwilligungen. Allerdings ist in der Lehre umstritten, ob die Geheimnisträgerin bereits zu Beginn der Beziehung zum Geheimnisherrn eine Einwilligung in die Bekanntgabe an mögliche Dritte einholen kann oder die Patientin oder der Patient im konkreten Einzelfall in die jeweilige Offenbarung einwilligen muss.[561] Es ist jedoch anerkannt, dass eine informierte Einwilligung, bspw. im Eintrittsformular oder vergleichbaren Dokumenten, erfolgen kann. Die Anforderungen an die Informationen sind dann allerdings hoch. Im Ergebnis muss aber auch hier gelten, was unter dem DSG ausgeführt wurde. Es müsste daher zulässig sein, bloss die Kategorien der Personen (Personengruppen), welchen die geheimnisgeschützten Daten im Rahmen einer Sekundärnutzung offenbart werden sollen, zu nennen, solange die Kategorie hinreichend bestimmt umschrieben und nicht überraschend bzw. ungewöhnlich zusammengesetzt ist.[562] Da die Entbindung auch stillschweigend erteilt werden kann, ist es grundsätzlich auch nicht zwingend, eine ausdrückliche oder gar schriftliche Entbindung zu verlangen.[563] Zu Beweiszwecken ist dies jedoch ratsam, d.h. in einem schriftlichen bzw. mindestens durch Text nachweisbaren Einwilligungsdokument, explizit auch die Entbindung zu erwähnen.

Aus Sicht des Geheimnisschutzes ist somit die (unverschlüsselte) Offenlegung von Gesundheitsdaten im Rahmen der Sekundärnutzung dann unproblematisch, wenn von den Geheimnisträgern die Zustimmung hierfür eingeholt werden kann. Hier bestehen jedoch regelmässig auch praktische Hindernisse, gerade, wenn eine Vielzahl von Geheimnisträgern involviert ist. In diesem Fall bleibt zu prüfen, ob es andere Rechtfertigungsmöglichkeiten für die grundsätzlich verbotene Offenbarung der geheimnisgeschützten Informationen gibt. Solche Rechtfertigungsgründe finden sich verstreut in vielen Vorschriften, etwa in Form von Meldepflichten, wie bspw. in Bezug auf die Meldungen an das Krebsregister. Mit Blick auf die hier interessierende Sekundärnutzung von Gesundheitsdaten ist allerdings auf die besondere Ausnahme-Regelung für die Humanforschung in Artikel 32bis Abs. 2 hinzuweisen. Nach dieser Vorschrift dürfen Berufsgeheimnisse für die Forschung dann offenbart werden, wenn die Voraussetzungen der sog. "Escape Clause" in Artikel 34 des HFG erfüllt sind und die zuständige Ethikkommission die Offenbarung bewilligt hat. Damit wird auf die bereits erläuterten Voraussetzungen dieser Bestimmung im HFG verwiesen und es wurde der besondere Ausnahmecharakter der Regelung sowie die damit verbundenen Unsicherheiten deutlich gemacht. Folglich erleichtert dieser Rechtfertigungsgrund die mit der Sekundärnutzung einhergehende Offenbarung von geheimnisgeschützten Informationen auch aus strafrechtlicher Sicht nur beschränkt.

---

560 Vgl. zum Bankgeheimnis mit eingehender Analyse der Rechtsprechung, JACOT-GUILLARMOD /HIRSCH, Pseudonymisierung von Bankkundendaten, digma 2020 S. 216 ff., 219 f.; zum Berufsgeheimnis im Ergebnis wohl auch STEINER, Digitalisierter Arztbesuch und Cloud-Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, sic! 2020 S. 677 ff., 68, allerdings ohne Bezugnahme zur Pseudonymisierung.

561 Befürwortend: SCHWARZENEGGER/THOUVENIN/STILLER, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, 2019, S. 46 f.; ablehnend: WOHLERS, Outsourcing durch Berufsgeheimnisträger, digma 2016, 116.

562 Vgl. zum DSG BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, Rz. 85 ff.

563 Vgl. bereits BGE 98 IV 217, E. 2.

4.4.2 Elektronisches Patientendossier (EPDG)

Ein grosses Potential für die Sekundärnutzung von Gesundheitsdaten kommt dem elektronischen Patientendossier (ePD) gemäss dem Gesetz über das elektronische Patientendossier (EPDG) zu. Damit wollte der Gesetzgeber die Qualität der medizinischen Behandlung stärken, die Behandlungsprozesse verbessern, die Patientensicherheit erhöhen und die Effizienz des Gesundheitssystems steigern sowie die Gesundheitskompetenz der Patientinnen und Patienten fördern.[564] Beim ePD handelt es sich definitionsgemäss um ein virtuelles Dossier, über das dezentral abgelegte behandlungsrelevante Daten aus der Krankengeschichte von Patientinnen und Patienten oder von diesen selber erfasste Daten in einem Abrufverfahren in einem konkreten Behandlungsfall zugänglich gemacht werden können.[565]

Wie aus dieser Definition hervorgeht, sollen im ePD nicht alle Patientendaten erfasst werden, sondern lediglich behandlungsrelevante. Hinsichtlich der Patientendaten ist zwischen dem Primär- und Sekundärsystem zu unterscheiden. Das Primärsystem beinhaltet die elektronische Krankengeschichte, also die interne Dokumentation der behandelnden Gesundheitsfachperson bzw. Gesundheitsinstitution.[566] Hierbei legt bspw. der Arzt oder seine Mitarbeitenden die relevanten Daten im eigenen Praxis- oder dem Klinikinformationssystem ab.[567] Die Patientendaten aus diesen Primärsystemen sollen allerdings nicht vollumfänglich im ePD aufgenommen werden. Im ePD als Sekundärsystem werden, nach Einwilligung der Patientinnen und Patienten, nur die für die Weiter- und Nachbehandlung relevanten Daten und Dokumente erfasst.[568] Die Zurverfügungstellung der wichtigsten behandlungsrelevanten Daten im Sekundärsystem wird für den Austausch von Informationen zwischen den verschiedenen Gesundheitsfachpersonen verwendet.[569] Welche Informationen und Daten im konkreten Fall als behandlungsrelevant zu qualifizieren sind, hängt vom Krankheitsverlauf der Patientinnen und Patienten ab, weshalb diesbezüglich ein gewisser Interpretationsspielraum besteht.[570]

Neben der grundsätzlichen Verfügbarkeit behandlungsrelevanter Informationen im ePD ist für die Praxis ebenso relevant, in welcher Form die Daten bereitgestellt werden. In der Anfangsphase ist das ePD primär eine Sammlung von PDF-Dokumenten, da aktuell noch kein Austausch von strukturierten dynamischen Daten (z.B. eMedikation, eImpfdossier) möglich ist.[571] Die im ePD vorhandenen Suchmasken sollen zwar den

---

564 Art. 1 Abs. 3 EPDG.

565 Art. 2 lit. a EPDG.

566 E-Health-Suisse, Fragen und Antworten zur Umsetzung des EPD, Version vom 22.02.2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/factsheet-fragen-antworten-epd-umsetzung.pdf (zuletzt aufgerufen am 29.5.2022), S. 3.

567 E-Health-Suisse, Fragen und Antworten zur Umsetzung des EPD, Version vom 22.02.2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/factsheet-fragen-antworten-epd-umsetzung.pdf (zuletzt aufgerufen am 29.5.2022), S. 3.

568 E-Health-Suisse, Fragen und Antworten zur Umsetzung des EPD, Version vom 22.02.2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/factsheet-fragen-antworten-epd-umsetzung.pdf (zuletzt aufgerufen am 29.5.2022), S. 3.

569 E-Health-Suisse, Fragen und Antworten zur Umsetzung des EPD, Version vom 22.02.2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/factsheet-fragen-antworten-epd-umsetzung.pdf (zuletzt aufgerufen am 29.5.2022), S. 3.

569 E-Health-Suisse, Fragen und Antworten zur Umsetzung des EPD, Version vom 22.02.2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/factsheet-fragen-antworten-epd-umsetzung.pdf (zuletzt aufgerufen am 29.5.2022), S. 3.

570 Bericht des Bundesrats, Elektronisches Patientendossier. Was gibt es noch zu tun bis zu seiner flächendeckenden Verwendung?, 11.08.2021, https://www.parlament.ch/centers/eparl/curia/2018/20184328/Bericht%20BR%20D.pdf, S. 23.

571 Bericht des Bundesrats, Elektronisches Patientendossier. Was gibt es noch zu tun bis zu seiner flächendeckenden Verwendung?, S. 22 f.

Umgang mit grossen Datenmengen für Gesundheitsfachpersonen erleichtern,[572] jedoch sind unstrukturierte Datensätze für automatisierte Weiterverarbeitungen von Gesundheitsdaten (bspw. durch Softwareanwendungen, die bei der Diagnose unterstützen) ungeeignet.

Die dezentrale Verwaltung des ePD obliegt den sogenannten (Stamm-)Gemeinschaften. Dabei handelt es sich um eine organisatorische Einheit von Gesundheitsfachpersonen und deren Einrichtungen.[573] Die Mitgliedschaft in einer (Stamm-)Gemeinschaft ist für Spitäler und andere Einrichtungen i.S.d Art. 39 KVG bereits verpflichtend.[574] Für ambulant tätige Gesundheitsfachpersonen war die Teilnahme am ePD bisher freiwillig. Seit dem 1.1.2022 müssen sich nun auch neu zugelassene ambulant tätige Ärztinnen und Ärzte obligatorisch einer Stammgemeinschaft anschliessen.[575] Nach der Annahme der Motion 19.3955[576] sollen nun alle Leistungserbringer bzw. Gesundheitsfachpersonen dazu verpflichtet werden, sich einer zertifizierten (Stamm-)Gemeinschaft anzuschliessen.[577]

Neben der generellen Verwaltung des ePD, müssen die Stammgemeinschaften auch sicherstellen, dass das ePD und die darin enthaltenen Daten zugänglich sind.[578] In seiner aktuellen Form gewährt das EPDG nur Gesundheitsfachpersonal sowie Patientinnen und Patienten Zugriff auf das ePD.[579] Kranken-, Unfall- und weitere Sozialversicherer sind bisher nicht am ePD beteiligt.[580] Mittlerweile hat jedoch der Bundesrat das Eidgenössische Departement des Innern (EDI) beauftragt, eine Vernehmlassungsvorlage auszuarbeiten, welche die Einbindung der Krankenversicherungen vorsieht.[581]

In Bezug auf die Forschung hat der Gesetzgeber bewusst darauf verzichtet, spezifische Regelungen zu erlassen.[582] Folglich gelten für die Bearbeitung von Daten des ePD zu Forschungszwecken die Bestimmungen des HFG bezüglich der Weiterverwendung von Gesundheitsdaten für die Forschung.[583] Dementsprechend ist je nach Art von Daten entweder ein "informed consent", ein Generalkonsent oder die Information über das

---

572 Bericht des Bundesrats, Elektronisches Patientendossier. Was gibt es noch zu tun bis zu seiner flächendeckenden Verwendung?, S. 22 f.

573 Art. 2 lit. d EPDG.

574 Art. 39 Abs. 1 lit. f KVG.

575 Art. 37 Abs. 3 KVG.

576 Motion 19.3955 "Ein elektronisches Patientendossier für alle am Behandlungsprozess beteiligten Gesundheitsfachpersonen" der SGK-N vom 08.03.2021, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193955.

577 Bericht des Bundesrats, Elektronisches Patientendossier. Was gibt es noch zu tun bis zu seiner flächendeckenden Verwendung?, S. 22 f.

578 Art. 10 Abs. 1 lit. a EPDG.

579 Art. 7 EPDG.

580 Sprecher/Hofer, Das elektronische Patientendossier, in: Epiney Astrid/Sangsue Déborah (Hrsg.), Datenschutz und Gesundheitsrecht, 2019, S. 53.

581 Vgl. Website des BAG: https://www.bag.admin.ch/bag/de/home/das-bag/aktuell/medienmitteilungen.msg-id-88245.html (zuletzt aufgerufen am 19.05.2022).

582 Vgl. Stellungnahme des Bundesrats zu Interpellation 19.4136: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20194136 (zuletzt aufgerufen am 19.05.2022).

583 Vgl. Stellungnahme des Bundesrats zu Interpellation 19.4136: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20194136 (zuletzt aufgerufen am 19.05.2022); Art 32 f. HFG.

Widerspruchsrecht notwendig, um die Daten für Forschungszwecke weiterverwenden zu können.[584] Für die betroffene Person muss dabei klar verständlich sein, dass Daten in ihrem ePD nicht nur für Behandlungs-, sondern auch für Forschungszwecke verwendet werden. Für die Sekundärnutzung durch öffentliche Organe wird zudem bspw. die erforderliche gesetzliche Ermächtigung zur Sekundärnutzung der Daten regelmässig[585] fehlen.[586]

In der noch zu entwerfenden Vernehmlassungsvorlage soll eine ausdrückliche Regelung der Zugriffsmöglichkeit auf das ePD für Forschungszwecke vorgesehen werden.[587] Der Bundesrat deutete dies Ende 2019 in einer Stellungnahme zu einer parlamentarischen Interpellation an.[588] Darin führte er aus, dass "die konkreten Prozesse und Vorgehensweisen zur Durchführung von Forschungsprojekten mit Daten des EPD zu gegebener Zeit zu beschreiben sein werden". Zudem sei die Frage zu klären, für welche Forschungsfragen sich die – in einer ersten Phase noch nicht strukturierten – Daten des ePD eignen. Wie beschrieben, enthält das ePD als Sekundärsystem nicht die vollständige Krankengeschichte, sondern nur die für die Weiterbehandlung relevanten Informationen, was eine weitere Hürde für die sinnvolle Sekundärnutzung der Daten darstellen kann.

Die Einführung und die Weiterentwicklung des ePD ist zu begrüssen, allerdings ist die konkrete Umsetzung bislang noch ungenügend. Auch verbesserte technische Rahmenbedingungen sind zu schaffen, damit eine effiziente Weiterverwendung der Daten möglich ist. Insbesondere die heutige Ablage von unstrukturierten Daten (bspw. PDF-Dokumente) erschwert deren Nutzung sowohl im Behandlungs- als auch im Forschungskontext. Ferner wird dadurch die Automatisierung der Pseudonymisierung bzw. Anonymisierung der Daten erschwert, welche notwendig ist, um die Daten ausserhalb des Behandlungskontexts zu nutzen. Der Bundesrat hat auch dieses Problem erkannt und will eine zentrale Ablage für dynamische Daten schaffen, um deren Bearbeitung zu vereinfachen.[589]

4.4.3 Krankenversicherungsgesetz (KVG)

Es wurde bereits erläutert, dass die Versicherungen im Bereich der obligatorischen Krankenversicherung mit öffentlichen Aufgaben betraut sind und damit als Bundesorgane gelten. Sie unterstehen daher den öffentlich-rechtlichen Vorschriften des DSG, soweit sie bei der Erfüllung dieser Aufgaben Personendaten bearbeiten. Im Krankenversicherungsgesetz besteht allerdings eine Vielzahl von Sondervorschriften, die diesen bereichsübergreifenden Regelungen vorgehen. Auch gelangen die Vorschriften des DSG zumindest dann dort ergänzend zur Anwendung, wo das KVG keine abschliessende Regelung enthält.

---

584 Vgl. oben Abschnitt 4.2.4.

585 Vgl. für das BAG immerhin Art. 22 Abs. 3 der Verordnung über das elektronische Patientendossier (EPDV).

586 Vgl. E-Health-Suisse, Fragen und Antworten zur Umsetzung des EPD, Version vom 22.02.2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/factsheet-fragen-antworten-epd-umsetzung.pdf (zuletzt aufgerufen am 29.5.2022), S. 26.

587 Vgl. Website des BAG: https://www.bag.admin.ch/bag/de/home/das-bag/aktuell/medienmitteilungen.msg-id-88245.html (zuletzt aufgerufen am 19.05.2022).

588 Vgl. Stellungnahme des Bundesrats zu Interpellation 19.4136: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20194136 (zuletzt aufgerufen am 19.05.2022); Art 32 f. HFG.

589 Vgl. Website des BAG: https://www.bag.admin.ch/bag/de/home/das-bag/aktuell/medienmitteilungen.msg-id-88245.html (zuletzt aufgerufen am 27.05.2022).

In Bezug auf die Datenbearbeitung sieht das KVG in Artikel 84 eine Generalklausel zur Umsetzung des bereits erläuterten datenschutzrechtlichen Legalitätsprinzips vor. Die Anforderungen an die Bestimmtheit solcher Ermächtigungsgrundlagen ist, wie erläutert, relativ niedrig, selbst wenn es um die Bearbeitung von besonders schützenswerten Gesundheitsdaten geht. Es ist nicht zu beanstanden und genügt unter dem Blickwinkel des Legalitätsprinzips, dass Art. 84 KVG allgemein eine Ermächtigung vorsieht für alle Bearbeitungen von Daten, einschliesslich besonders schützenswerter Daten, die zur Erfüllung der den Krankenversicherern nach dem KVG oder dem KVAG übertragenen Aufgaben benötigt werden. Dies gilt umso mehr als die konkreten Aufgaben und Zwecke in Form einer Auflistung weiter konkretisiert werden. Genannt werden darin bspw. auch die Führung von Statistiken oder die Berechnung des Risikoausgleichs.

Wie im Zusammenhang mit dem Legalitätsprinzip ausgeführt, entbindet jedoch selbst eine (weit gefasste) Ermächtigungsgrundlage nicht von der Einhaltung des Zweckbindungsgebots. Darüber hinaus ist im Falle einer Sekundärnutzung auch zu beurteilen, ob der Zweck der Sekundärnutzung überhaupt noch als Erfüllung einer gesetzlichen Aufgabe verstanden werden kann. In diesem Sinne äusserst sich auch das Bundesamt für Gesundheit (BAG) als Aufsichtsbehörde in dem jüngst aktualisierten Kreisschreiben Nr. 7.1[590]. So folgert das BAG aus dem Grundsatz der Zweckbindung und dem Legalitätsprinzip, dass Personendaten nur für die Erfüllung der Aufgaben genutzt werden, die im gleichen Zweckrahmen liegen, wie diejenigen Aufgaben, zu deren Erfüllung sie erhoben worden sind. Bei dieser Ausgangslage ist deshalb auch die Schlussfolgerung des BAG richtig.[591] So ist die Bearbeitung von Gesundheitsdaten und Persönlichkeitsprofilen der Versicherten zur Identifizierung von besonderen Zielgruppen für ein Empfehlungsschreiben für gesundheitsfördernde Massnahmen oder für Medikamente mit den erwähnten rechtlichen Grundlagen nicht vereinbar. Da es sich dabei nicht um eine nach dem KVG oder KVAG übertragene Durchführungsaufgabe des Versicherers handelt, ist eine gezielte gesundheits- oder krankheitsspezifische Empfehlung an selektionierte Versicherte nicht durch Art. 84 KVG abgedeckt. Namentlich kann auch nicht von einer blossen "Führung von Statistiken" ausgegangen werden, wenn Personen, allenfalls gestützt auf Erkenntnisse aus Statistiken, kontaktiert werden sollen. Insofern fehlt für eine solche Personendatenbearbeitung bereits die erforderliche gesetzliche Grundlage und würde auch einen Verstoss gegen das Zweckbindungsgebot darstellen. Die Datenbearbeitung ist demzufolge unzulässig und infolgedessen zu unterlassen.

Dass die Krankenversicherer selbst keine hinreichende Grundlage für Bearbeitungen haben, die nicht zur Aufgabenerfüllung dienen, bedeutet noch nicht zwingend, dass dies auch für andere Verantwortliche gilt. So enthält das KVG denn auch eine ausführliche Regelung dazu, unter welchen Voraussetzungen die Krankenversicherungen Personendaten Dritten bekanntgeben dürfen[592]. Aufgeführt werden dabei bspw. folgende Bekanntgaben an[593]:

- Organe der Bundesstatistik nach dem Bundesstatistikgesetz;
- Stellen, die mit der Führung von Statistiken zur Durchführung des KVG betraut sind, wenn die Daten für die Erfüllung dieser Aufgabe erforderlich sind und die Anonymität der Versicherten gewahrt bleibt;

590 Kreisschreiben des BAG Nr. 7.1, 20.12.2012, Aufsicht des BAG über datenschutzrelevante Bereiche gemäss KVAG 1, KVAV 2, KVG 3 und KVV.

591 Vgl. Kreisschreiben des BAG Nr. 7.1, Ziff. 5.1 S. 6 f.

592 Art. 84a KVG.

593 Vgl. Art. 84a Abs. 1 lit. d-f KVG.

- zuständige kantonale Behörden, wenn es sich um Daten nach Artikel 22*a* KVG handelt und diese für die Planung der Spitäler und Pflegeheime sowie für die Beurteilung der Tarife erforderlich sind.

Ferner sind folgende weiteren Ausnahmetatbestände vorgesehen:

- Veröffentlichung von Daten, die von allgemeinem Interesse sind und sich auf die Anwendung dieses Gesetzes beziehen, sofern die Anonymität der Versicherten gewahrt bleibt;[594]

- Bekanntgabe nicht personenbezogener Daten, sofern die Bekanntgabe einem überwiegenden Interesse entspricht;[595]

- Bekanntgabe von Personendaten, sofern die betroffene Person im Einzelfall schriftlich eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse der versicherten Person vorausgesetzt werden darf.[596]

Insbesondere der letztgenannte Grund kann für eine Vielzahl von Konstellationen der Fall sein, setzt jedoch grundsätzlich das Einholen einer Einwilligung voraus. Auch bei dieser Aufzählung werden mehrere Fälle aufgeführt, in welchen entweder von nicht-personenbezogenen Daten oder von Anonymität gesprochen wird. Dies wirft wiederum die bereits thematisierten Fragen zu den rechtlichen Anforderungen an die Anonymisierung und deren Umsetzbarkeit[597] auf und führt zu Unsicherheiten. In all diesen Fällen dürfen jeweils aber ohnehin nur die Daten bekannt gegeben werden, welche für den in Frage stehenden Zweck erforderlich sind.[598]

Bereits angesichts der Ausführlichkeit der Regelung stellt sich die Frage, inwieweit noch Raum für die ergänzende Anwendung des DSG besteht. Während die Datenbearbeitungsgrundsätze kaum vollumfänglich verdrängt werden, spricht jedoch namentlich in Bezug auf das Legalitätsprinzip Einiges für eine abschliessende Regelung. Hierzu zählt unter anderem auch die Bestimmung in Art. 6a Abs. 3 KVV, welche in Bezug auf Daten aus dem Beitrittsformular festhält, dass die Versicherer diese nur für die im Gesetz vorgesehenen Aufgaben bearbeiten dürfen. In diesem Sinne könnte auch die Erwägung des Bundesgerichts in seinem Leitentscheid verstanden werden, wonach bei Datenbearbeitungen, die nach Art. 42 Abs. 3 und 4 sowie Art. 84 und 84a KVG rechtmässig sind, kein Raum bestehe, sie gestützt auf das DSG als unrechtmässig zu erklären.[599]

Die Frage ist jedoch nach wie vor offen. So hat auch das Bundesverwaltungsgericht in seinem Helsana+-Urteil einen anderen Standpunkt zum Ausdruck gebracht, wenn auch ohne Begründung.[600] Für die nicht vollumfänglich abschliessende Regelung spricht zumindest ein systematischer Aspekt. Denn wenn im erwähnten sehr breit gefassten Art. 84a Abs. 5 lit. b KVG sogar die Bekanntgabe an jegliche Dritten losgelöst von bestimmten Zwecken erlaubt wird, ist unerklärlich, wieso nicht auch die Krankenversicherer selbst eine ge-

---

[594] Art. 84a Abs. 3 KVG.

[595] Art. 84a Abs. 5 lit. a KVG.

[596] Art. 84a Abs. 5 lit. b KVG.

[597] Vgl. oben Abschnitt 3.1.2c) und 3.2.6.oben Abschnitte 3.1.2c) und 3.2.6.

[598] Art. 84a Abs. 6 KVG.

[599] BGE 133 V 359, E. 6.4.

[600] Urteil des BVGer A-3548/2018 vom 19. März 2019, E. 4.8.2; ferner die Kritik bei BÜHLMANN/SCHÜEPP, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15. März 2021, Rz. 24.

wöhnliche Bearbeitung von Personendaten vornehmen dürfen sollen, wenn ihnen hierfür eine gültige Einwilligung erteilt wird. Insofern ist denkbar, dass auch weitere Ausnahmen und Sonderregelungen des DSG ergänzend greifen könnten.[601] Vor diesem Hintergrund wäre eine Berufung darauf für die Sekundärnutzung mit erheblichen Unsicherheiten verbunden.

4.4.4 Epidemiengesetz (EpG)

Das Epidemiengesetz (EpG) ist spätestens seit der COVID-19 Pandemie auch dem juristischen Laien ein Begriff. Die Erfassung von Erkrankten und das sogenannte Contact-Tracing waren wichtige Massnahmen zur Eindämmung der Pandemie, welche ohne die Bearbeitung von Personendaten nicht möglich gewesen wären. Dementsprechend enthält das Epidemiengesetz zahlreiche Bestimmungen zum Informationsaustausch und zur Bearbeitung von Personendaten.[602] Das datenschutzrechtliche Legalitätsprinzip gibt vor, dass Bundesorgane Personendaten nur bearbeiten dürfen, wenn hierfür eine gesetzliche Ermächtigung oder eine Ausnahme davon vorliegt.[603] Das EpG schafft für das Bundesamt für Gesundheit (BAG), die zuständigen kantonalen Behörden und die mit Aufgaben nach dem EpG betrauten öffentlichen und privaten Institutionen diese gesetzliche Grundlage in Bezug auf Datenbearbeitungen, die der Epidemienbekämpfung bzw. -prävention dienen.

So dürfen die genannten Stellen nach Art. 58 EpG Personendaten, inklusive Daten über die Gesundheit, bearbeiten (oder bearbeiten lassen), "soweit dies zur Identifizierung von kranken, krankheitsverdächtigen, angesteckten, ansteckungsverdächtigen und Krankheitserreger ausscheidenden Personen im Hinblick auf Massnahmen zum Schutz der öffentlichen Gesundheit, insbesondere zur Erkennung, Überwachung und Bekämpfung übertragbarer Krankheiten, erforderlich ist". Soweit Art. 58 EpG gewisse Teilbereiche nicht oder nicht abschliessend regelt, finden die allgemeinen Datenschutzbestimmungen des Bundes oder der Kantone Anwendung.[604] Damit sind namentlich die Datenbearbeitungsgrundsätze angesprochen, welche auch im Bereich der Epidemienbekämpfung zu beachten sind.

Die Datenbearbeitungen von Art. 58 EpG sollen insbesondere den folgenden zwei Zwecken dienen[605]:

i.) Identifizierung von Risikopersonen zur Epidemienüberwachung und -bekämpfung

Gemäss der Botschaft zu EpG sind gewisse Daten zur Identifizierung von verschiedenen Personen, wie z.B. Infizierten und anderen "Risikopersonen"[606] im Hinblick auf Massnahmen zum Schutz der öffentlichen Gesundheit notwendig.[607] In diesem Kontext müssen, neben krankheitsspezifischen Informationen – welche Rückschlüsse auf die Infektionsquelle und auf das Gefahrenpotenzial zulassen – personenidentifizierende Angaben wie der vollständige Name, das Geburtsdatum und die Wohnadresse der Betroffenen bearbeitet

---

601 Im Ergebnis ebenso, allerdings ohne Auseinandersetzung mit dem Verhältnis zwischen DSG und KVG, SZUCS /BRÄM, Gesundheitsforschung mit Versicherungsdaten, in: Jusletter 27. Januar 2020, Rz. 13, die Anwendbarkeit der Forschungsausnahme bejahend.

602 BAERISWYL, Datenschutz in der (Corona)-Krise, EuZ 2020, S. 168 ff., 171.

603 Vgl. zum Legalitätsprinzip oben Abschnitt 4.1.4b) sowie 4.3.3c). iii.).

604 Botschaft zum EpG, BBl 2011 S. 406.

605 Botschaft zur Revision des Bundesgesetzes über die Bekämpfung übertragbarer Krankheiten des Menschen, BBl 2011 S. 406.

606 Z.B. kranken, krankheitsverdächtigen, angesteckten, ansteckungsverdächtigen oder Krankheitserreger ausscheidenden Personen.

607 Botschaft zum EpG, BBl 2011 S. 406.

werden. Die entsprechenden Daten dienen der Abklärung und Kontrolle von Krankheitsausbrüchen und ermöglichen die Anordnung von personenbezogenen Massnahmen i.S.d. Art. 30 ff. EpG.[608] Dazu gehören insbesondere dringliche Rückfragen bei Ärztinnen und Ärzten sowie Laboratorien zur Diagnostik, die Suche, Befragung und Beratung von angesteckten und exponierten Einzelpersonen und Personengruppen, die dringliche Benachrichtigung von Gesundheitsbehörden zur internationalen Suche, die Benachrichtigung exponierter Personen und die Suche nach Personen mit einer früheren Exposition durch Blut, Blutprodukte und Organe.[609]

ii.) Früherkennung und Überwachung von übertragbaren Krankheiten

Neben dem oben genannten Zweck dürfen gewisse Daten auch zur Früherkennung und Überwachung von übertragbaren Krankheiten bearbeitet werden.[610] Dieser Bearbeitungszweck stellt insbesondere auf die Erstellung von Analysen der zeitlichen und räumlichen Entwicklung von alters- und verhaltensspezifischen Auftretenshäufigkeiten der jeweiligen Infektionskrankheit ab.[611] Für die Erstellung der genannten Analysen, die als Entscheidungsgrundlage für die zuständigen Behörden dienen sollen, ist die Erfassung und Aufbewahrung von Alters- und Wohnortsangaben zusammen mit krankheitsspezifischen Expositionsinformationen notwendig.[612] Art. 59 Abs. 2 zählt exemplarisch auf, welche Daten – einschliesslich Gesundheitsdaten – bekanntgegeben werden dürfen. Hierbei handelt es sich insbesondere um die Daten, die im Rahmen der Meldepflicht nach Artikel 12 EpG sowie der epidemiologischen Abklärungen nach Artikel 15 EpG erhoben werden. Schliesslich dürfen die Daten nur an eine konkret abgegrenzte Gruppe von Empfängern bekanntgegeben werden: Hierzu zählen mit der Behandlung übertragbarer Krankheiten beauftragte Ärztinnen, zuständige kantonale Behörden und zuständige Vollzugsbehörden des Bundes.[613] Daraus folgt, dass die Daten nicht an andere Akteure, wie z.B. Forschungseinrichtungen, weitergeben werden dürfen.

Die oben beschrieben Daten werden z.B. durch Meldungen von Ärztinnen, Spitälern und anderen öffentlichen und privaten Gesundheitseinrichtungen gewonnen. Diese sind gem. Art 12 Abs. 1 EpG dazu verpflichtet, Beobachtungen zu übertragbaren Krankheiten mit den Angaben, die zur Identifizierung der erkrankten, infizierten oder exponierten Personen sowie zur Feststellung des Übertragungswegs notwendig sind, zu melden. Die Ausführungsverordnungen regeln detailliert den konkreten Inhalt der Meldungen, nicht aber das Meldemittel.[614]

Mit anderen Worten wird hier die Bearbeitung von (besonders schützenswerten) Personendaten zum Zwecke der Epidemienbekämpfung gesetzlich angeordnet, obwohl diese Personendaten ursprünglich primär zu Behandlungszwecken erhoben wurden. Aufgrund der gesetzlichen Anordnung handelt es sich somit auch nicht um eine Zweckänderung im Sinne des Zweckbindungsgebots. Das EpG erlaubt es dem BAG ferner zur epidemiologischen Überwachung und zu Forschungszwecken mit Ärztinnen und Ärzten, Laboratorien, Spitälern und anderen öffentlichen und privaten Institutionen des Gesundheitswesens zu vereinbaren, dass sie

608 Botschaft zum EpG, BBl 2011 S. 406.

609 Botschaft zum EpG, BBl 2011 S. 406.

610 Botschaft zum EpG, BBl 2011 S. 406.

611 Botschaft zum EpG, BBl 2011 S. 407.

612 Botschaft zum EpG, BBl 2011 S. 407.

613 Art. 59 Abs 3 EpG.

614 Vgl. Art. 6 ff. Epidemienverordnung, EpV; Art. 1 ff. der Verordnung des EDI über die Meldung von Beobachtungen übertragbarer Krankheiten des Menschen, insb. Art. 15 Abs. 1 betr. Meldemittel.

Beobachtungen, die nicht der Meldepflicht unterstehen, einer vom BAG bezeichneten Stelle melden.[615] Solche Meldungen haben allerdings, anders als die Inhalte der Meldepflicht, anonymisiert zu erfolgen.[616]

Über die Regelungen zu Meldungen und Meldepflichten hinaus enthält das EpG auch Vorschriften, die den Informationsaustausch unter den für den Vollzug dieses Gesetzes zuständigen Stellen des Bundes und der Kantone und damit eine gegenseitige Bekanntgabe von Personendaten erlauben. Hierfür enthält das EpG in Art. 59 zusätzlich zur Regelung der Meldepflichten eine gesonderte Grundlage. Damit werden die Vollzugsbehörden ermächtigt, sich gegenseitig Personendaten, einschliesslich Daten über die Gesundheit, bekannt zu geben, die sie zur Erfüllung der ihnen durch das EpG zugewiesenen Aufgaben benötigen. Darüber hinaus können das BAG und die für den Vollzug dieses Gesetzes zuständigen kantonalen Behörden Personendaten, einschliesslich Daten über die Gesundheit, die erforderlich sind, um die Verbreitung einer übertragbaren Krankheit zu verhindern, den folgenden Personen und Behörden bekannt geben: den mit der Behandlung übertragbarer Krankheiten beauftragten Ärztinnen und Ärzten, den kantonalen Behörden, die Aufgaben im Bereich der Erkennung, Überwachung, Verhütung und Bekämpfung von übertragbaren Krankheiten wahrnehmen, sowie anderen Bundesbehörden, sofern dies für den Vollzug der von diesen Behörden anzuwendenden Erlasse notwendig ist.

Das BAG betreibt ferner ein Informationssystem, in das Daten über die Risikopersonen aufgenommen werden.[617] In der Epidemienverordnung (EpV) wird geregelt, welche Personendaten in dem Register zu erfassen sind, wer Zugriff auch die entsprechenden Daten hat und welche technischen und organisatorischen Massnahmen das BAG ergreifen muss, um das Informationssystem vor unberechtigtem Zugriff zu schützen.[618]

Darüber hinaus ist aus datenschutzrechtlicher Sicht noch das sogenannte Proximity-Tracing System (PT-System) zu nennen, dessen Rechtsgrundlage im Rahmen der COVID-Pandemiebekämpfung geschaffen wurde.[619] Das PT-System wurde durch die sogenannte Tracing App umgesetzt, welche (freiwilligen) Teilnehmern auf dem Smartphone meldete, wenn sie sich eine gewisse Zeit in der Nähe eines infizierten oder unter Infektionsverdacht stehenden Teilnehmers aufgehalten haben. Das System wurde durch technische und organisatorische Massnahmen weitgehend datenschutzfreundlich gestaltet,[620] jedoch blieb der praktische Erfolg zur Pandemiebekämpfung bescheiden.

Insgesamt enthält das EpG damit relativ breit gefasste gesetzliche Ermächtigungsgrundlagen für umfassende Datenbearbeitungen und Bekanntgaben durch die Vielzahl von Behörden und Institutionen, die mit dem Vollzug des EpG betraut sind. Davon erfasst sind namentlich auch umfassende Sekundärnutzungen von Gesundheitsdaten, allerdings beschränkt auf die Zwecke der Epidemienbekämpfung bzw. -prävention. Ein grosses Hindernis für die effiziente Nutzung der grossen Zahl an Daten für die gesetzlichen Zwecke be-

615 Art. 14 Abs. 1 EpG.

616 Art. 14 Abs. 2 EpG.

617 Art. 60 EpG.

618 Art. 89 ff. EpG.

619 Art. 60a EpG.

620 Art. 60a Abs. 5 EpG.

steht jedoch darin, dass für die Meldepflichten keine bestimmten (elektronischen) Meldemittel vorgeschrieben sind, die Daten daher auch mittels schriftlicher Formulare per Post, Kurier oder Fax übermittelt werden können.[621]

4.4.5 Regelungen für klinische Versuche

Das Schweizer Recht kennt eine Vielzahl von Sondervorschriften für sog. klinische Versuche. Grundlage dieser Regelungen sind die Vorschriften im Heilmittelgesetz (HMG). Dieses erklärt in Art. 53 HMG für klinische Versuche mit Heilmitteln zusätzlich zu den Sondervorschriften des HMG und der Ausführungsverordnungen die Vorschriften des Humanforschungsgesetzes für anwendbar, was allerdings rein deklaratorisch ist, da klinische Versuche im nachfolgend erläuterten Sinne ohnehin in den oben erläuterten Geltungsbereich des HFG fallen.[622]

Darüber hinaus wurden namentlich zwei Ausführungsverordnungen mit umfangreichen Vorgaben erlassen:

- Verordnung über klinische Versuche (KlinV);[623]
- Verordnung über klinische Versuche mit Medizinprodukten (KlinV-Mep).[624]

Der Begriff des klinischen Versuchs wird in der KlinV[625] wie folgt definiert:

> Forschungsprojekt mit Personen, das diese prospektiv einer gesundheitsbezogenen Intervention zuordnet, um deren Wirkungen auf die Gesundheit oder auf den Aufbau und die Funktion des menschlichen Körpers zu untersuchen.

In Bezug auf Medizinprodukte wird demgegenüber in der KlinV-Mep[626] von folgendem Begriffsverständnis des klinischen Versuchs ausgegangen:

> Systematische Untersuchung eines Produkts, bei der eine oder mehrere Personen einbezogen sind und die zwecks Bewertung der Sicherheit oder Leistung des Produkts durchgeführt wird.

Im Unterschied zu nicht-klinischen Studien (auch als beobachtende Studien bezeichnet) enthalten die beiden Erscheinungsformen der Humanforschung somit eine gesundheitsbezogene Intervention (z.B. ein Arzneimittel oder Medizinprodukt), deren Wirkung auf die Teilnehmenden untersucht wird.[627] Im Einzelfall kann die Abgrenzung[628] und die Einschätzung der einschlägigen Sondervorschriften in der Praxis Schwierigkeiten

---

621 Art. 15 der Verordnung des EDI über die Meldung von Beobachtungen übertragbarer Krankheiten des Menschen.

622 Botschaft zum HFG, BBl 2009 S. 8150.

623 Verordnung über klinische Versuche mit Ausnahme klinischer Versuche mit Medizinprodukten (Verordnung über klinische Versuche, KlinV) vom 20. September 2013), SR 810.305. (im Folgenden KlinV).

624 Verordnung über klinische Versuche mit Medizinprodukten (KlinV-Mep) vom 1. Juli 2020,), SR 810.306. (im Folgenden KlinV-Mep).

625 Art. 2 lit. a KlinV.

626 Art. 2 lit. a bzw. lit a^{bis} KlinV-Mep.

627 Vgl. Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 7.

628 Wertvolle Hilfestellungen bietet z.B. die Koordinationsstelle Forschung am Menschen (KOFAM) mit dem "Categoriser": https://www.kofam.ch/de/categoriser (zuletzt aufgerufen am: 24.5.20022).

bereiten. Für den vorliegenden Zusammenhang ist wichtig, dass für Weiterverwendungen bereits vorliegender Daten die Anforderungen der KlinV und die KlinV-Mep nicht gelten.[629] Vielmehr sind dafür die allgemeinen Vorschriften des HFG und der HFV massgebend. Nichtsdestotrotz sind umgekehrt aber die Daten, die im Rahmen solcher Versuche erhoben wurden, von erheblichem Wert und deshalb wichtig für die Sekundärnutzung. Indem die KlinV und die KlinV-Mep die Anforderungen für die (originäre) Datenerhebung festlegen, bestimmen sie auch massgeblich, inwieweit eine spätere Sekundärnutzung erfolgen darf. Denn wurden die Daten unrechtmässig erhoben, ist, wie in den Erläuterungen zum HFG erwähnt[630], auch ihre Weiterverwendung selbst unter Einhaltung der besonderen Anforderungen an die Weiterverwendung unzulässig.

In Bezug auf die klinischen Studien sind zudem die wissenschaftlichen Anforderungen besonders wichtig. Hierzu gehören die Anforderungen an die wissenschaftliche Qualität (Art. 10 Abs. 1 lit. b HFG), welche in den anerkannten internationalen Regeln der Guten Praxis über die Forschung am Menschen (Art. 10 Abs. 1 lit. c HFG) geregelt sind. Für den Bereich der klinischen Versuche verweist der Bundesrat insbesondere auf die in der ICH-Leitlinie von 1996 formulierten Regeln der Guten Klinischen Praxis (Art. 5 Abs. 1 i.V.m. Anhang I Ziff. 2 KlinV). Darin sind auch Vorgaben enthalten, die Einfluss auf den Umgang mit Daten und Dokumentationen[631] und damit auch auf die Sekundärnutzung von Gesundheitsdaten haben. Auf diese internationalen Standards wird in der vorliegenden Untersuchung mit Fokus auf das Schweizer Recht nicht näher eingegangen. Für Forschungsvorhaben im Anwendungsbereich der beiden Verordnungen zu klinischen Versuchen gilt schliesslich ebenfalls eine Bewilligungspflicht, wobei besondere Anforderungen und Zuständigkeiten zu beachten sind,[632] sowie eine Pflicht zur Registrierung[633] der Vorhaben.

Mit Blick auf die Sekundärnutzung ist jedenfalls auch für klinische Studien der verfassungsrechtlich verankerte Grundsatz gültig, wonach die Teilnahme an Humanforschungen eine aufgeklärte Einwilligung der Teilnehmenden voraussetzt.[634] Folgerichtig verweisen die Verordnungen[635] im Grundsatz für die Anforderungen an diese Einwilligungen auf die Vorschriften des HFG, die bereits weiter oben[636] erläutert wurden. Auch die Aufklärungsinhalte entsprechen weitgehend den Anforderungen, wie sie im HFG und der HFV enthalten sind.[637] Für den Fall, dass eine Weiterverwendung des im klinischen Versuch entnommenen biologischen Materials oder der im klinischen Versuch erhobenen gesundheitsbezogenen Personendaten für die Forschung beabsichtigt ist, so muss darüber hinaus auch über die Inhalte nach den Artikeln 28–32 der HFV aufgeklärt werden.[638]

Aus der Kombination dieser Vorschriften zur Aufklärung folgt letztlich eine grosse Zahl an Pflichtangaben. Dies erschwert die Anforderung, dass die Informationen dazu verständlich sein müssen, umso mehr als die

---

629 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 7.

630 Vgl. oben Abschnitt 4.2.4a).

631 Vgl. z.B. die Anforderung betreffend Dokumentation von unterschriebenen Einwilligungserklärungen, Ziff. 8.3.12.

632 Vgl. Art. 19 ff. KlinV; Art. 6 ff. KlinV-Mep.

633 Vgl. Art. Art. 64 KlinV.

634 Vgl. dazu oben Abschnitt 4.2.3b).

635 Art. 7 Abs. 1 und 2 KlinV; Art. 3 Abs. 1 lit. b KlinV-Mep i.V.m. Art. 7 Abs. 1 und 2 KlinV.

636 Vgl. dazu oben Abschnitt 4.2.3b).

637 Art. 7 Abs. 1 KlinV (s. aber immerhin den zusätzlichen lit. a); Art. 3 Abs. 1 lit. b KlinV-Mep i.V.m. Art. 7 Abs. 1 KlinV.

638 Art. 7 Abs. 1 und 2 KlinV; Art. 3 Abs. 1 lit. b KlinV-Mep i.V.m. Art. 7 Abs. 1 und 2 KlinV.

Komplexität der Versuche regelmässig hoch ist. Die Verantwortlichen müssen durch geeignete Massnahmen sicherstellen, dass die betroffene Person die wesentlichen Aufklärungsinhalte versteht.[639] Demnach ist die aufgeklärte Einwilligung auch hier nicht als pauschale Übermittlung von Information plus Einholung einer Unterschrift zu verstehen. Vielmehr handelt es sich nach den Vorstellungen des Verordnungsgebers um einen Prozess des textgestützten Gesprächs, der bei der für das Projekt angefragten Person zu einem wirklichen Verständnis über die Implikationen ihrer potentiellen Teilnahme führen soll.[640] Inwieweit aber diese Anforderung auch für die Datenbearbeitungen im Zusammenhang mit dem betreffenden klinischen Versuch gilt, ist auch hier nicht geklärt. Es stellt sich somit die Frage, ob auch diesbezüglich und anders als im DSG ein subjektiver Massstab gelten soll, was jedoch aus den besagten Gründen abzulehnen ist.[641] Darüber hinaus ist auch hier mangels vereinheitlichter Formulare die Nutzung der Daten mit unterschiedlich weit oder eng definierten Zwecken mit Unsicherheiten verbunden.

Ein weiteres Hindernis ist hier ebenfalls das grundsätzliche Erfordernis der Schriftlichkeit, weil gleichermassen davon ausgegangen wird, dass damit Einwilligungserklärungen nur gültig sind, wenn sie unterzeichnet sind.[642] Auch wenn wiederum nicht von vornherein ausgeschlossen ist, dass auch eine digitale Signatur, z.B. auf einem Touch-Screen, ausreichen könnte, besteht diesbezüglich Unsicherheit und dürfte zudem nicht der heutigen Praxis entsprechen. Immerhin sind in den Verordnungen über die klinischen Versuche aber auch Ausnahmen von der Schriftlichkeit definiert,[643] die jedoch wiederum nur unter strengen Voraussetzungen greifen.

Konkret mit Blick auf die Sekundärnutzung von Daten oder Material aus klinischen Versuchen sind auch hier die differenzierten Anforderungen des HFG für die unterschiedlichen Kategorien[644] anwendbar. Es kann insofern auch hier ein Generalkonsent genügen, sofern es um die unverschlüsselte Verwendung nichtgenetischer gesundheitsbezogener Personendaten oder die verschlüsselte Verwendung von biologischem Material und genetische Daten geht. Es kann deshalb auf die bisherigen Erläuterungen zum HFG verwiesen werden.

Hinzuweisen ist an dieser Stelle jedoch darauf, dass bei Daten aus klinischen Versuchen eine besondere Aufbewahrungspflicht gilt. Demnach müssen sämtliche für die Identifizierung und die Nachbetreuung der teilnehmenden Personen notwendigen Unterlagen sowie alle anderen Originaldaten während mindestens zehn Jahren nach Abschluss oder Abbruch des klinischen Versuchs aufbewahrt werden.[645] Mit dieser Pflicht soll sichergestellt werden, dass nach Abschluss des klinischen Versuchs allfällig auftretende Erkrankungen der Teilnehmenden ursächlich eingeordnet und behandelt werden können.[646] Soweit bestimmte Daten für die Nachbetreuung eines Teilnehmers erforderlich sein können, dürfen sie mit anderen Worten während dieser

639 Art. 7 Abs. 4 KlinV; Art. 3 Abs. 1 lit. b KlinV-Mep i.V.m. Art. 7 Abs. 1 KlinV.

640 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 18 f.

641 Vgl. oben Abschnitt 4.2.3b).

642 Vgl. Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 18.

643 Art. 8 KlinV; Art. 3 Abs. 1 lit. b KlinV-Mep i.V.m. Art. 8 KlinV.

644 Vgl. dazu oben Abschnitt 4.2.4.

645 Art. 45 Abs. 2 KlinV.

646 Erläuternder Bericht über die Verordnungen zum Humanforschungsgesetz (21. August 2013), S. 17.

Dauer grundsätzlich auch nicht gelöscht oder anonymisiert werden.[647] Es ist lediglich eine Verschlüsselung erlaubt, wobei hierfür wiederum die Anforderungen an die sichere und getrennte Aufbewahrung gelten.[648]

Insgesamt entsprechen die Regelungen der Verordnungen für klinische Versuche damit weitgehend denjenigen des HFG und der HFV. Es kommen allerdings gleichwohl weitere Anforderungen hinzu, was die praktische Handhabung in Anbetracht der ohnehin hohen Komplexität der Versuche zusätzlich erschwert und Abgrenzungsfragen aufwirft.

4.4.6 Krebsregistrierungsgesetz (KRG)

Von Bedeutung für die Sekundärnutzung ist auch die Regelung des Krebsregistrierungsgesetzes (KRG) des Bundes. Denn mit dem Gesetz wurden die nötigen Datengrundlagen geschaffen, um Präventions- und Früherkennungsmassnahmen zu erarbeiten, die Behandlungsqualität zu evaluieren und die Versorgungsplanung sowie die Forschung zu unterstützen.[649]

Zur Erreichung dieser Zwecke schreibt das KRG eine Meldepflicht vor für Ärztinnen und Ärzte, Spitäler und andere private oder öffentliche Institutionen des Gesundheitswesens, die eine Krebserkrankung diagnostizieren oder behandeln (meldepflichtige Personen und Institutionen).[650] Diese Meldepflichtigen müssen eine Vielzahl genau festgelegter Personendaten zu den Krebserkrankungen und den betroffenen Patientinnen und Patienten erheben und dem kantonalen Krebsregister und dem Kinderkrebsregister melden.[651]

Hierdurch wird also wiederum gesetzlich eine Verwendung von personenbezogenen Gesundheitsdaten aus dem Behandlungskontext für die Zwecke des Krebsregistrierungsgesetzes vorgeschrieben. Aufgrund der gesetzlichen Anordnung handelt es sich somit allerdings nicht um eine Zweckänderung im Sinne des Zweckbindungsgebots. Als Ausgleich und zur Gewährleistung der Rechte der Patientinnen und Patienten sind jedoch zahlreiche besondere Regelungen zur Information und zum Widerspruchs- und Auskunftsrecht der Patientinnen und Patienten vorgesehen.[652] Unklar bleibt auch hier das Verhältnis zu den allgemeinen Vorschriften der sektorübergreifenden Datenschutzvorschriften, also insbesondere, ob gleichwohl weitere Informationen zu erteilen und weitere Rechte zu beachten sind. Auch unter dem KRG muss davon ausgegangen werden, dass dies der Fall ist, die allgemeinen Vorschriften also nicht vollumfänglich verdrängt werden. Die Einzelheiten sind jedoch ungeklärt und es hat für jede Bestimmung eine gesonderte Prüfung im Einzelfall zu erfolgen.

Den kantonalen Krebsregistern kommt, wie es der Name sagt, die Aufgabe der Registrierung der gemeldeten Daten zu.[653] Sie haben die gemeldeten Daten auf Plausibilität zu prüfen, zu ergänzen, zu berichtigen und zu aktualisieren durch Nachfragen bei den Meldepflichtigen und durch einen Abgleich mit anderen Daten von

---

647 Vgl. für den Fall des Widerrufs einer Einwilligung ferner aber Art. 9 KlinV; dazu ferner VAN SPYK, in: RÜTSCHE (Hrsg.), SHK-HFG, 2015, Art. 7 N 46.

648 Vgl. Art. 18 KlinV; ferner Art. 8.3.21 GCP E6(R2), der eine Aufbewahrung des Schlüssels während der Durchführung des Versuchs verlangt.

649 Vgl. Art. 2 KRG.

650 Art. 3 Abs. 1 KRG.

651 Vgl. Art. 3 und 4 KRG und Art. 1 ff. KRV.

652 Art. 5-7 KRG.

653 Art. 8 Abs. 1 KRG.

anderen Stellen, wie den kantonalen und kommunalen Einwohnerregistern und oder der Todesursachenstatistik.[654] Die Krebsregister registrieren und kodieren die Daten nach den Vorgaben der nationalen Krebsregistrierungsstelle.[655] Sie weisen jeder Krebserkrankung eine Fallnummer zu und stellen sicher, dass die personenidentifizierenden Daten von den übrigen Daten getrennt bearbeitet werden.[656] Die kantonalen Krebsregister leiten ihrerseits die registrierten Daten und die Fallnummer regelmässig an die nationale Krebsregistrierungsstelle weiter. Das Geburts- und das Todesdatum umfassen dabei nur Monat und Jahr. Nicht weitergeleitet werden Name und Vorname, Wohnadresse und Versichertennummer der Patientin oder des Patienten und in Bezug auf die Versichertennummer erfolgt durch einen eingeschalteten Dienst eine Pseudonymisierung. Der Dienst leitet die Fallnummer und die pseudonymisierte Versichertennummer ebenfalls an die nationale Krebsregistrierungsstelle weiter.[657] Die nationale Krebsregistrierungsstelle überprüft und erfasst sodann ihrerseits die Daten, welche die kantonalen Krebsregister ihr weitergeleitet haben. Die bereinigten Daten bereitet sie auf für statistische Auswertungen, Auswertungen im Rahmen der Gesundheitsberichterstattung, Auswertungen zur Evaluation der Diagnose- und Behandlungsqualität und für die Weiterverwendung zu Forschungszwecken.

Aus diesen Elementen resultiert in der Summe ein komplexes System, das durch umfangreiche Ausführungsvorschriften in der Krebsregistrierungsverordnung weiter spezifiziert wird. Die involvierten Krebsregister und die Krebsregistrierungsstelle übernehmen dabei eine wichtige Rolle, verfügen sie doch über eine Vielzahl von sensitiven und für die Weiterverwendung wertvollen Daten. Entsprechend detailliert sind deshalb nicht nur die Ermächtigungsgrundlagen zur Bearbeitung und Bekanntgabe der Daten, sondern auch die Auflagen an den Umgang mit den Daten[658] und die Sicherstellung der Umsetzung der Patientenrechte[659]. Ihre Tätigkeiten und auch diejenigen der anderen involvierten Akteure erfolgen stets im Zusammenhang mit der Erzielung von Fortschritten bei der Prävention, der Früherkennung und der Behandlung von Krebserkrankungen.

Es stellt sich deshalb die Frage nach dem Verhältnis der Vorschriften des KRG zu denjenigen des HFG. In dieser Hinsicht stellt Artikel 28 KRG klar, dass der Kern der mit dem KRG geregelten Datenbearbeitungen nicht dem HFG unterstellt ist. Das KRG gilt in diesem Sinn als Spezialgesetz im Verhältnis zum HFG.[660] Es geht also namentlich um die Erhebung und Meldung der Daten durch die meldepflichtigen Personen, die Aufbereitung, Registrierung und Weiterleitung der Daten durch die kantonalen Krebsregister sowie die Aufbereitung, Verwaltung und Weitergabe von Daten durch die Krebsregistrierungsstelle. Diese Tätigkeiten sind nicht vom HFG erfasst. Gleiches gilt für die ausdrücklich erlaubte Weitergabe ihrer Daten zu Forschungszwecken in anonymisierter Form,[661] wobei dies ohnehin nicht vom Anwendungsbereich des HFG erfasst wäre. Für die Anforderungen an die Anonymisierung sind sodann wieder vergleichbare Regelungen wie in

654 Art. 9 KRG.

655 Art. 10 Abs. 1 KRG.

656 Art. 10 Abs. 2 und 3 KRG.

657 Art. 12 KRG.

658 Vgl. z.B. Art. 25 ff. KRG und Art. 28-30 KRV.

659 Vgl. z.B. Art. 5-7 KRG und Art. 13-16 KRV.

660 Vgl. Botschaft zum KRG, BBl 2014 S. 8797.

661 Art. 23 Abs. 2 KRG.

der HFV enthalten,[662] was ebenfalls die dort erwähnten Unsicherheiten mit sich bringt.[663] Für all diese Tätigkeiten ist keine Bewilligung einer kantonalen Ethikkommission erforderlich.[664]

Zu beachten ist jedoch, dass es den Krebsregistern und der Krebsregistrierungsstelle auch gestattet ist, ihre Daten zu Forschungszwecken zu bearbeiten und sie mit zusätzlich durch sie erhobenen Daten zusammenführen.[665] In dieser Hinsicht stellt Art. 24 Abs. 4 KRG klar, dass für die Forschung mit registrierten Daten und die Erhebung von zusätzlichen gesundheitsbezogenen Personendaten sowie für deren Weiterverwendung oder deren anderweitige Bearbeitung zu Forschungszwecken die Bestimmungen des HFG gelten.[666] Die Vorgaben des HFG sind ebenfalls zu beachten, wenn die gemeldeten Daten in nicht anonymisierter Form zur Weiterverwendung zu Forschungszwecken an Dritte bekanntgegeben werden. Hierfür ist grundsätzlich der Generalkonsent der betroffenen Person im Sinne von Artikel 33 Absatz 1 HFG erforderlich.[667]

Die Unterscheidung der beiden Anwendungsbereiche ist insofern wichtig und fällt in der Praxis nicht immer leicht. Dabei ist auch sicherzustellen, dass die jeweiligen Verwendungszwecke und Rechte auch aus Sicht der Patientinnen und Patienten verständlich sind. Denn im Bereich der dem KRG unterstellten Tätigkeit tritt an die Stelle der grundsätzlich im HFG verlangten aufgeklärten Einwilligung ein blosses Widerspruchsrecht gegen die Registrierung nach hinreichender Information.[668] Gerade für Patientinnen und Patienten in einer ohnehin bereits gesundheitlich anspruchsvollen Situation dürfte die Erfassung der beiden Aspekte sowie das Fällen einer Entscheidung dazu jedenfalls nicht immer leichtfallen. Insgesamt wird die Summe an Pflichtangaben[669] somit weiter erhöht, was der Verständlichkeit abträglich ist. Auch auf Seiten der Meldepflichtigen führt dies zu hohen Anforderungen an die Umsetzung. Hinzu kommt, dass jeweils das Datum der Informationserteilung zu erfassen ist,[670] was regelmässig zu Schwierigkeiten geführt hat, durch eine kürzlich erst erfolgte Totalrevision aber etwas verbessert wurde[671].

Praktische Schwierigkeiten bestehen nicht nur bei der Umsetzung der Patientenrechte, sondern auch in Bezug auf das Format der zu meldenden Daten. So ist es zwar das erklärte Ziel, elektronische Datenübermittlungen gestützt auf Austauschformate, wie im Kontext des elektronischen Patientendossiers (ePD), zu etablieren. Verbindlich ist die Nutzung von Austauschformaten bei der Datenübermittlung an die Krebsregister

662 Art. 30 KRV; s. demgegenüber die Sonderregelungen zur Pseudonymisierung der Versichertennummer u.a. Art. 23 KRV.

663 Vgl. dazu vorstehend Abschnitte 3.1.2c) und 3.2.6.

664 Vgl. zum Ganzen Botschaft zum KRG, BBl 2014 S. 8797.

665 Art. 23 Abs. 3 KRG.

666 Vgl. auch Botschaft zum KRG, BBl 2014 S. 8794.

667 BBl 2014 8727 ff., S. 8795.

668 Vgl. zum Ganzen Botschaft zum KRG, BBl 2014 S. 8797.

669 Vgl. die Liste in Art. 13 KRV.

670 Vgl. Art. 1 Abs. 1 lit. d und Art. 2 Abs. 1 lit. d KRV.

671 Insbesondere können die Daten auch bei der Nichterfassung des Datums verwertet werden, weil die Karenzfrist für die Erhebung des Widerspruchs in Art. 17 Abs. 1 KRV seit dem 1.1.2022 neu ab dem Eingang der ersten Meldung einer Krebserkrankung läuft und nicht mehr ab dem Datum der Patienteninformation; vgl. Erläuterungen zur Revision der Verordnung über die Registrierung von Krebserkrankungen (Krebsregistrierungsverordnung, KRV), April 2021.

gleichwohl nicht.[672] So hält die KRV lediglich fest, dass die Meldungen elektronisch oder in Papierform erfolgen können. Erfahrungen aus der Praxis zeigen, dass dies nicht nur auf Seiten der Meldepflichtigen, sondern auch der Register zu erheblichen Schwierigkeiten und Ineffizienzen führt. Dies erschwert letztlich auch die mit dem KRG angestrebten Ziele und die Sekundärnutzung der hier betroffenen, wertvollen Gesundheitsdaten.

5. Analyse der Use Cases unter Berücksichtigung der aufgezeigten rechtlichen Hindernisse

Die vorangehende Untersuchung hat eine grosse Zahl von grundlegenden Hindernissen für die Sekundärnutzung identifiziert. Die zentralen Erkenntnisse daraus lassen sich anhand der Analyse der nachfolgenden Use-Cases darstellen und zusammenfassen.

5.1 Use Case I: Sekundärnutzung im Behandlungs-, Vorsorge- und Früherkennungskontext

5.1.1 Use Case

Ein Softwareunternehmen entwickelte gemeinsam mit einem Team aus Ärzten und Wissenschaftlern eine Anwendung zur frühzeitigen Erkennung von Autoimmunerkrankungen (z.B. Multiple Sklerose) und zur Bestimmung von Risikopatienten. Diese Anwendung wird von Ärzten im Rahmen der Behandlung eingesetzt und greift dabei zur Erkennung von Mustern auf pseudonymisierte (oder anonymisierte) Patientendaten verschiedener Spitäler zu. Darüber hinaus wird das Patientendossier der betroffenen Person in die Anwendung eingelesen, um Rückschlüsse auf etwaige Vorerkrankungen und Risikofaktoren zu erhalten. Der Patient hat zusätzlich die Möglichkeit, Daten, die über eine Smartwatch erhoben werden (Puls, Bewegungsmuster und weitere Daten zur körperlichen Verfassung) zur Verfügung zu stellen. Um Rückschlüsse auf familiäre Risikofaktoren zu erhalten, sollen Patientendossiers von verstorbenen und lebenden Angehörigen zur Verfügung gestellt werden. Die Anwendung errechnet das individuelle MS-Risiko des Patienten und gibt eine Handlungsempfehlung ab, wie oft sich die betroffene Person einer Kontrolluntersuchung unterziehen soll.

5.1.2 Analyse

a) Anwendbare Vorschriften

Der vorliegende Use Case hat die Datennutzung im Kontext der Behandlung zum Gegenstand. Im Fokus steht dabei die Datennutzung durch Ärztinnen und Ärzte zum Zweck der Behandlung ihrer Patientinnen und Patienten.

In einem ersten Schritt ist zu prüfen, welche rechtlichen Vorschriften für die Datenbearbeitungen durch die behandelnden Ärzte zur Anwendung gelangen. Ausserhalb des Forschungskontexts und der Vorschriften des HFG sind hier primär die sektorübergreifenden Datenschutzgesetze anwendbar. Es stellt sich allerdings die Frage, ob die Vorschriften des DSG oder diejenigen einer der kantonalen Datenschutzgesetzgebungen anwendbar sind.

Entscheidend ist dabei, ob der jeweilige Arzt eine Datenbearbeitung in Erfüllung öffentlicher Aufgaben (des Bundes oder eines Kantons) vornimmt. Hierfür muss geklärt werden, welcher Arzt konkret die Behandlung

[672] Vgl. zum Ganzen BAG/Nationale Krebsregistrierungsstelle, Dokumentation Austauschformat KRG, Version 8.1.2020, S. 7.

durchführt. Wird der behandelnde Arzt, z.B. an einem Kantonsspital, hier im Rahmen eines krankenversicherungsrechtlichen oder eines kantonalen Leistungsauftrags tätig, ist von einem Handeln als öffentliches kantonales Organ auszugehen. Handelt es sich demgegenüber um selbständige Zusatzleistungen, die nicht mit Grundversicherungsleistungen verbunden sind, liegt eine private Tätigkeit vor und die damit verbundenen Datenbearbeitungen sind den Vorschriften für private Verantwortliche unterstellt. Es ist somit eine Beurteilung der jeweiligen Leistungsaufträge und krankenversicherungsrechtlichen Vorschriften zur Kostentragung vorzunehmen. Bei neueren Behandlungsformen oder Leistungen, die auch der Prävention von Krankheiten dienen, oder unter Einsatz von digitalen Anwendungen erbracht werden, ist diese Beurteilung jedoch nicht immer leicht vorzunehmen.

Für die Zwecke der vorliegenden Analyse wird unterstellt, dass die öffentlich-rechtlichen Vorschriften des Datenschutzrechts des Kantons Zürich, d.h. des Gesetzes über die Information und den Datenschutz des Kantons Zürich (IDG-ZH), auf die von den Ärzten vorgenommenen Datenbearbeitungen zur Behandlung der Patientinnen und Patienten zur Anwendung gelangen.

b) Datenkategorien und datenschutzrechtliche Rollen

Aus Sicht der Ärzte ist dabei zunächst fraglich, wie die Daten der anderen Spitäler zu qualifizieren sind, auf welche die Software zugreift. Im vorliegenden Beispiel liegt der Schluss nahe, dass es sich zu einem wesentlichen Teil um Gesundheitsdaten handelt. Denn es dürften regelmässig die Daten derjenigen Personen interessieren, bei welchen eine entsprechende Autoimmunerkrankung diagnostiziert wurde. Es wird sich somit um Gesundheitsdaten und damit besonders schützenswerte Daten bzw. (in der Terminologie des IDG-ZH) um besondere Personendaten handeln und dies unabhängig davon, ob man von einem weiteren Begriffsverständnis als auf Bundesebene ausgehen würde.

Allerdings stellt sich in einem nächsten Schritt die Frage, ob die Gesundheitsdaten einer bestimmbaren Person zugeordnet werden können und damit überhaupt von Personendaten auszugehen ist. Es ist somit zu beurteilen, ob die bei den anderen Spitälern ausgelesenen Daten tatsächlich anonymisiert sind oder ob pseudonymisierte oder gar gewöhnliche personenbezogene Gesundheitsdaten vorliegen. Die Beurteilungskriterien hierfür sind im Anwendungsbereich des DSG Gegenstand von zahlreichen Stellungnahmen in Lehre und Rechtsprechung. Gleichwohl besteht Uneinigkeit und letztlich eine erhebliche Unsicherheit darüber, aus wessen Perspektive zu beurteilen ist, ob die Information, hier die medizinischen Daten und Befunde, einer konkreten Patientin oder einem konkreten Patienten zugeordnet werden können.[673]

Diese Fragestellung lässt sich nur dann sinnvoll beantworten, wenn auf die datenschutzrechtlichen Rollen abgestellt wird, also wer der für eine Datenbearbeitung Verantwortliche ist. Aus dessen Perspektive ist die Frage zu entscheiden und auch eine plausible Abgrenzung zwischen Anonymisierung und Pseudonymisierung vorzunehmen.

Im vorliegenden Use Case ist unter genauer Analyse der Funktionsweise der Software, den damit verbunden Datenbearbeitungen und faktischen Einflussnahmemöglichkeiten zu beurteilen, wer Verantwortlicher ist. Denkbar ist, dass die Ärzte in Bezug auf die Bearbeitungen zum Zweck der Behandlung als Verantwortliche qualifiziert werden müssen. Somit wäre aus der Sicht der Ärzte zu beurteilen, ob sie gestützt auf die ihnen vorliegenden Mittel und Informationen mit verhältnismässigem Aufwand die Informationen einzelnen Patientinnen oder Patienten zuordnen können. Ist dies nicht der Fall bedeutet dies aber noch nicht, dass anonymisierte Daten vorliegen. Denn den Ärzten zuzurechnende Auftragsbearbeiter oder Co-Verantwortliche sind

673 Vgl. zur Anonymisierung Abschnitt 3.1.2 c) und d).

ebenfalls zu berücksichtigen. Ist es auch diesen nicht möglich, die dahinterstehenden Patientinnen oder Patienten ohne unverhältnismässigen Aufwand zu identifizierten, ist von anonymisierten Personendaten auszugehen. Die Beurteilung ist deshalb aber ungewiss und von vielen Faktoren abhängig. Mit Blick auf die Rechtslage im Kanton Zürich kommt hinzu, dass unklar ist, welche Perspektive konkret massgeblich sein soll. Denn es fehlt eine Anknüpfung an den Begriff des Verantwortlichen, was zu zusätzlicher Rechtsunsicherheit führt. Schliesslich ist auch die unnötige Auseinandersetzung mit der Frage erforderlich, inwieweit auch die Daten der hier involvierten juristischen Personen (bspw. der anderen Spitäler oder des Software-Herstellers) bearbeitet werden dürfen.

Wie oft in der Praxis wird damit eine grundlegende Frage kaum mit hinreichender Gewissheit beantwortet werden können. Die Ärzte werden sich bis zu einem gewissen Grad auf Zusicherungen des Softwareherstellers verlassen müssen. Die Frage, ob tatsächlich eine Anonymisierung vorliegt, entscheidet aber massgeblich darüber, ob der Einsatz der Anwendung und die Sekundärnutzung der Daten Dritter im Behandlungskontext zulässig ist. Denkbar ist jedenfalls, dass aus Sicht der behandelnden Ärzte tatsächlich anonymisierte Daten vorliegen, also bspw. nur die anderen Spitäler eine Identifikation mit verhältnismässigen Mitteln vornehmen können, weil nur sie, nicht aber der Softwarehersteller, Zugang zum Zuordnungs-Schlüssel haben. Aus Sicht des Softwareherstellers ist dann zwar von pseudonymisierten Daten auszugehen, aus Sicht der behandelnden Ärzte liegen aber anonymisierte Daten vor.

c) Berufsgeheimnis, Zweckbindung und Legalitätsprinzip

In diesem Use Case wird die Bereitstellung der (pseudonymisierten bzw. anonymisierten) Daten durch die anderen Spitäler, zumindest nach der hier vertretenen Meinung, grundsätzlich auch ohne Einverständnis der Patientinnen und Patienten bzw. Entbindung keinen Verstoss gegen die beruflichen Schweigepflichten, namentlich das Arztgeheimnis, darstellen. Die Einzelheiten dazu sind jedoch umstritten, namentlich auch, wenn es um den Einbezug von Software-Herstellern mit US-Bezug geht. Die technischen Aspekte der hinreichenden Verschlüsselung sind im Detail zu prüfen und es sind die je nach Kanton unterschiedlich strengen Haltungen der Aufsichtsbehörden zu berücksichtigen. Ferner müsste muss die hinreichende Verschlüsselung von den beteiligten Akteuren, zumindest einigen Gerichtsurteilen zufolge, auch bewiesen werden können.[674] Scheitert der Nachweis, ist die Übermittlung der pseudonymisierten Daten gleichwohl nur unter Einholung einer informierten Einverständniserklärung bzw. Entbindung vom Berufsgeheimnis zulässig.

Solange aus Sicht der behandelnden Ärzte nicht mit Gewissheit von anonymisierten Daten ausgegangen werden kann, ist für sie zentral, unter welchen Umständen die Daten der anderen Spitäler beschafft und bereitgestellt werden. Kann das Vorliegen von personenbezogenen Daten und damit die Anwendbarkeit der Datenschutzgesetze – hier des IDG-ZH – demnach nicht ausgeschlossen werden, hängt hiervon massgeblich auch die Zulässigkeit der Weiterbearbeitung ab. War nämlich für die Patientinnen und Patienten der anderen Spitäler nicht erkennbar, dass ihre Daten auch zur Behandlung anderer Patientinnen oder Patienten durch andere Ärzte genutzt werden, liegt ein Verstoss gegen das Zweckbindungsgebot vor. Selbst wenn man dies verneinen würde, ist fraglich, inwiefern sich die Spitäler und behandelnden Ärzte auf eine hinreichende gesetzliche Grundlage für die Bearbeitung der Gesundheitsdaten als besonders schützenswerte bzw. besondere Personendaten berufen könnten. Hierfür muss zumindest feststehen, dass die Datenbearbeitung für die Erfüllung der gesetzlichen Aufgaben, bspw. die Gesundheitsversorgung, erforderlich ist, also keine milderen Mittel vorliegen und die Bearbeitung für die betroffenen Personen zumutbar sind.

Zur Absicherung ist deshalb das Einholen einer Einwilligung eine Option. Diese muss durch die anderen Spitäler bei der Erhebung der Daten ihrer Patientinnen und Patienten oder zumindest vor der Übermittlung an

674 Vgl. Abschnitt 3.1.2 d).

den Software-Hersteller eingeholt werden. Geht man davon aus, dass die Spitäler für die hier interessierenden Datenbearbeitungen ebenfalls dem IDG-ZH unterstellt sind, bleibt jedoch unklar, inwieweit die Einwilligung tatsächlich als Absicherung dienen kann. Denn im IDG-ZH ist, anders als im DSG, nicht gesetzlich geregelt, ob und inwieweit die Einwilligung eine fehlende gesetzliche Grundlage ersetzen kann. Ferner müssen auch die Anforderungen an die hinreichende Information (inkl. Kategorien von Empfängern der Daten) und an die Freiwilligkeit erfüllt sein, was weitere Unsicherheiten mit sich bringt, umso mehr, weil die behandelnden Ärzte sich hier auf Zusicherungen der Spitäler verlassen müssen.

Insgesamt bleiben somit wichtige Fragen rund um den zulässigen Einsatz der Software offen, solange nicht auf die wirksame Anonymisierung der Daten vertraut werden kann. Die Unsicherheiten in Bezug auf den Einsatz von Anbietern mit US-Bezug sowie betreffend gesetzlicher Grundlage oder Einwilligung bleiben bestehen.

d) Weitere Elemente des Use Cases

Ähnliche Fragen stellen sich auch für eventuelle Übermittlungen von Daten an den Software-Hersteller durch den behandelnden Arzt, der die Software bei der Behandlung seiner Patientinnen und Patienten einsetzt. Entsprechend den Angaben im Use Case handelt es sich dabei potentiell um die Angaben im Patientendossier sowie die Information aus der Smartwatch. In Bezug auf die Smartwatch-Daten wird zu beurteilen sein, ob der Arzt die Daten in die Software einspielt oder ob es die Patientinnen und Patienten sind, welche die Daten selber übermitteln. Je nach dem hat der Arzt bereits für die Zulässigkeit der Übermittlung als solche zu sorgen oder erst bei der Weiterverarbeitung der Daten in Kombination mit den anderen Daten im Rahmen der Anwendung der Software. Angesichts der fehlenden wissenschaftlichen Aufarbeitung und Rechtsprechung im Kanton Zürich bleibt dabei auch unklar, inwieweit die Daten aus der Smartwatch bereits als Gesundheitsdaten zu betrachten sind, für die ein strengerer Beurteilungsmassstab gilt.

Entscheidend für die Beurteilung der Zulässigkeit der Weiterbearbeitung sind auch dabei wiederum die Rollen der involvierten Akteure. Ist der Software-Hersteller nur als Auftragsbearbeiter der behandelnden Ärzte als Verantwortlicher zu sehen, kann angenommen werden, dass die Übermittlung gar nicht erst eine Bekanntgabe im datenschutzrechtlichen Sinne oder eine Offenbarung eines Berufsgeheimnisses darstellt. Gerade bei Anbietern mit US-Bezug ist auch dies mit Unsicherheiten behaftet.

Ähnliche Unsicherheiten bestehen auch bei der Berufung auf den Standpunkt, dass bloss pseudonymisierte Daten übermittelt werden, ist doch in diesem Fall auch damit zu rechnen, die hinreichende Pseudonymisierung beweisen zu müssen. Aufgrund der erwähnten Unsicherheiten in Bezug auf die Einwilligung bleibt wiederum die Frage der Anonymisierung, die für die Zulässigkeit des Software-Einsatzes entscheidend ist. Inwieweit die Anonymisierung gegeben ist, ist auch für diese Daten unklar. Im Übrigen dürfte in Bezug auf den vorliegenden Use Case ferner eine sinnvolle Anbindung der Software an das elektronische Patientendossiers nach aktuellem Stand bereits daran scheitern, dass darin noch keine strukturierten Daten vorhanden sind. Ferner würde die Anbindung voraussetzen, dass die Patientinnen und Patienten bereits über ein elektronisches Patientendossier verfügen und der betreffende (bspw. der nachbehandelnde und der zuweisende) Arzt bereits angebunden ist. Zudem wird auch die Sicherstellung der hinreichenden Information für eine gültige Einwilligung schwierig und im Falle von öffentlichen Organen die gesetzliche Grundlage fraglich sein.

In Bezug auf die Daten der Angehörigen, die im Use Case auch noch erwähnt werden, ist darauf hinzuweisen, dass die Nutzung von deren Gesundheitsdaten potentiell eine Zweckänderung darstellt und im Falle der Offenbarung durch den Arzt für den aktuell behandelten Patienten potentiell eine Verletzung des Arztgeheimnisses ist. Ohne Einwilligung der Angehörigen wird somit der Einbezug ihrer Daten in die Behandlung des Patienten nicht erfolgen dürfen.

e) Fazit

Bei diesem Use Case zeigen sich die folgenden vier Aspekte, die bereits in der vorangehenden Untersuchung als wesentliche Hindernisse identifiziert wurden.

1. Unsicherheiten, ob die Vorschriften des Bundes oder der Kantone anzuwenden sind und inwieweit die kantonalen Vorschriften im Einklang mit (den besser aufbearbeiteten) Vorgaben des nDSG stehen.

2. Unklarheiten in Bezug auf die Anonymisierung und die damit verbundene Frage nach den datenschutzrechtlichen Rollen.

3. Unklarheiten in Bezug auf die möglichen alternativen Absicherungen einer Datenbearbeitung in Form einer Einwilligung oder anderen Ermächtigungsgrundlage.

4. Ungenügende Nutzbarkeit des elektronischen Patientendossiers.

5.2 Use Case II: Sekundärnutzung im Forschungskontext

Im Rahmen eines Forschungsprojekts sollen mithilfe von künstlicher Intelligenz (KI) fortschrittliche Modelle entwickelt werden, um eine effektivere Behandlung einer bestimmten Krebsart (z.B. Prostatakrebs) zu ermöglichen. Insbesondere soll das Forschungsprojekt zu einer Verbesserung der Diagnose, der Erkennung von Metastasen und der Vorhersage des Ansprechens auf die Behandlung führen.

Um diese Ziele zu erreichen, benötigt das Forschungsteam grosse Mengen an Gesundheitsdaten. Einerseits wollen die Forscher eine Datenbank, bestehend aus pseudonymisierten (oder anonymisierten) Prostata-MRI-Scans und den dazugehörigen Patientendaten, welche im Rahmen der Krebstherapie angefertigt wurden, erstellen. Mithilfe dieser Scans soll eine KI-Anwendung trainiert werden, welche zu einer verbesserten Diagnose beiträgt. Zusätzlich sollen genetische Daten und Blutproben gesammelt werden, um die Diagnosefähigkeiten der KI-Anwendung zu verbessern. Die Daten sollen aus verschiedenen Schweizer Spitälern und onkologischen Arztpraxen sowie aus anderen Forschungsprojekten stammen. Mit prospektiven Studien soll der Nutzen für den Patienten bestimmt werden und die Wirksamkeit von verschiedenen (z.B. medikamentösen) Behandlungsmethoden mit Hilfe dieser Anwendung getestet werden. Dafür ist ein Zugriff auf die Primärsysteme der Spitäler oder die elektronischen Patientendossiers der Probanden notwendig.

5.2.1 Anwendbarkeit HFG

Als Vorfrage bei diesem Use Case mit Fokus auf die Forschung ist zu klären, ob das HFG als Spezialgesetz anwendbar ist. Das HFG gilt grundsätzlich für die Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers. Diese Forschung wird u.a. mit biologischem Material bzw. gesundheitsbezogenen Personendaten durchgeführt. Die Forschung ist als "methodengeleitete Suche nach verallgemeinerbaren Erkenntnissen" zu verstehen, wobei keine Einschränkung auf institutionelle Forschungseinrichtungen (z.B. Universitäten) vorgenommen wird. Als methodengeleitet wird die Anwendung von wissenschaftlich anerkannten Vorgehensweisen zur Erkenntnisgewinnung angesehen. Der Methodenbegriff ist jedoch gegenüber neuartigen Methoden offen (wie z.B. dem Einsatz von KI zur Krebsdiagnose), sofern die

Abweichungen vom geltenden Wissenschaftsstandard begründbar sind und die Anforderungen an die wissenschaftliche Qualität eingehalten werden.[675] Ausgehend davon muss jeweils im Einzelfall die konkrete Methodik beurteilt werden. Es müssten für eine abschliessende Beurteilung des Use Cases somit nähere Angaben bekannt sein.

Allerdings werden im vorliegenden Use Case bspw. die gewonnen Erkenntnisse durch eine prospektive Studie verifiziert, was auf eine wissenschaftliche Vorgehensweise hinweist. Ferner müssen die zu gewinnenden Erkenntnisse verallgemeinerbar sein, d.h. sie müssen auch über den Kontext des Forschungsprojekts hinaus Gültigkeit besitzen und dürfen nicht einen nur individuellen Bezug aufweisen. Dies ist in diesem Use Case gegeben, weil durch das Trainieren eines KI-Systems anhand einer grossen Datenmenge verallgemeinerbare Schlüsse abgleitet werden sollen (bspw. welche Merkmale deuten in einer überwiegenden Anzahl an Fällen auf einen Tumor hin). Generell ist der Forschungsbegriff des HFG weit zu verstehen, da sich der Geltungsbereich primär nach dem Ziel und nicht direkt nach der Art bzw. Konzeption der Forschungstätigkeit richtet. Es kann vorliegend somit eine Forschungstätigkeit i.S.d HFG angenommen werden, die als Krankheit Krebs zum Gegenstand hat.

5.2.2 Gesundheitsbezogene Personendaten und biologisches Material

Für die Anwendbarkeit des HFG ist zusätzlich die Frage zu beantworten, ob biologisches Material oder gesundheitsbezogene Personendaten bearbeitet werden.

a) MRI-Scans

Die Forschung soll im Use Case anhand von pseudonymisierten (oder anonymisierten) MRI-Scans und Patientendaten erfolgen. Es ist deshalb zu klären, ob es sich bei diesen Daten um gesundheitsbezogene Personendaten handelt. MRI-Scans bestehen zumeist – z.B. nach dem DICOM-Standard[676] – aus Bildmaterial und verschiedenen Metadaten. Als Gesundheitsdaten i.S.d. HFG gelten "diejenigen Informationen über eine Person zu verstehen, die einen Bezug zu einer physischen oder psychischen Krankheit aufweisen oder über Aufbau und Funktion des Körpers der betreffenden Person".[677] Das Bildmaterial ist geeignet, Aufschluss über eine Krankheit bzw. den Aufbau und Funktion des Körpers zu geben.

Fraglich ist, ob das Bildmaterial für sich schon als Personendatum zu qualifizieren ist. Hierbei ist entscheidend, ob die Abbildung einen solchen Individualisierungsgrad aufweist, dass sie einer bestimmten Person zugeordnet werden kann. In diesem Zusammenhang ist relevant, ob bspw. ein Prostatascan – ähnlich wie ein Fingerabdruck – eindeutig einer Person zugeordnet werden kann. Je individueller ein abgebildetes Merkmal einer Person ist, desto höher ist die Wahrscheinlichkeit, dass die Abbildung selbst bereits ein Personendatum ist. Sofern die betroffene Person aber nur anhand von Referenzdaten (bspw. vergleichbares Bildmaterial inkl. Metadaten, welche die Person identifizieren) bestimmt werden kann und diese Referenzdaten für den Datenbearbeiter nicht mit verhältnismässigen Mitteln beschafft werden können, gelten die Daten als pseudonymisiert oder anonymisiert, je nachdem in welchem Verhältnis der Dateninhaber zu der Person oder Organisation steht (bspw. Spital), welche über die Referenzdaten verfügt.[678] Da die Auffassungen über die für die Beurteilung massgeblichen Perspektiven auseinandergehen, ist die Einschätzung mit Unsicherheiten

[675] VAN SPYK, in: RÜTSCHE (Hrsg.), SHK-HFG, 2015, Art. 3 Rz. 4; Art. 10 HFG.

[676] Website DICOM: https://www.dicomstandard.org/about (zuletzt aufgerufen am 19.05.2022).

[677] Botschaft zum HFG, BBl 2009 S. 8095.

[678] Vgl. Abschnitte 3.1.2d), 3.2.6 und 3.2.7.

behaftet. So wäre mitunter auch zu klären, wer die für die Datenbearbeitungen im Forschungsprojekt Verantwortlichen sind und welche datenschutzrechtlichen Rollen den involvierten Beteiligten zukommt. Für diese Beurteilung müssten jedoch nähere Angaben zur Aufgabenverteilung und dem Verhältnis untereinander bekannt sein.

Hinzu kommt, dass die Evaluierung, ob eine Person bestimmbar ist, jeweils von den nicht immer eindeutigen Umständen des Einzelfalls abhängt. Sind an einer Datenbearbeitung, was bei Forschungsvorhaben regelmässig der Fall ist, eine Vielzahl von Beteiligten involviert, ist in die Beurteilung auch eine Vielzahl von zusätzlichen Aspekten (Rollen, Wissen etc.) einzubeziehen. Diese Beurteilung fiele zumindest dann weniger schwer, wenn es von vornherein um das gesamte (unverschlüsselte) DICOM-file ginge. Da dieses File sowohl die Informationen über die Gesundheit (das Bildmaterial), als auch die Metadaten enthält, die einen Patienten identifizieren können (Patientenname, Patienten ID, Geschlecht), muss von personenbezogenen Gesundheitsdaten ausgegangen werden.[679] Entsprechend den Angaben im Sachverhalt soll aber zumindest von pseudonymisierten bzw. verschlüsselten Scans und Gesundheitsdaten ausgegangen werden. Die Beurteilung, ob tatsächlich eine hinreichende Verschlüsselung im Sinne der rechtlichen Anforderungen vorliegt, ist mit den gleichen Unsicherheiten verbunden, wie sie sich bei der Frage der Anonymisierung ergeben. Denn die Verschlüsselung im HFG setzt voraus, dass die Daten für eine Person, die keinen Zugang zum Schlüssel hat, als anonymisiert zu betrachten sind. Diese Beurteilung hat im Einzelfall zu erfolgen und ist mit Unsicherheiten verbunden. Da Scans keine Information über das Erbgut enthalten, handelt es sich zumindest nicht um genetische Gesundheitsdaten.

Für die nachfolgende Beurteilung des Use Cases wird demnach unterstellt, dass die Scans und weiteren Patientendaten verschlüsselte nichtgenetische Gesundheitsdaten darstellen.

b) Genetische Daten und Blutproben

Gemäss Sachverhalt sollen, zusätzlich zu den MRI-Scans, genetische Daten und Blutproben entnommen werden, um die Diagnosefähigkeit des KI-Systems zu verbessern. Laut Legaldefinition sind unter biologischem Material jegliche Körpersubstanzen, die von lebenden Personen stammen, zu verstehen. Unter diese Begriffsdefinition fallen auch die Blutproben und das Forschungsprojekt zielt somit auf die Verwendung von biologischem Material ab. Bei genetischen Daten wird von einem weiten Begriffsverständnis ausgegangen, sodass nicht nur die Sequenzierungen spezifischer Genome davon erfasst ist, sondern auch die Informationen, die gewonnen werden, wenn bspw. bei einer onkologischen Untersuchungsmethode mit Genmarkern gearbeitet wird.

Der Use Case spricht sodann nicht von anonymisierten oder verschlüsselten Daten oder Material. Es wäre dabei aber ohnehin nicht unumstritten, ob eine Anonymisierung aus rechtlicher Sicht tatsächlich korrekt erfolgt ist.

[679] DICOM Standards Committee, Working Group 14 Security, 'Digital Imaging and Communications in Medicine (DICOM) - Supplement 55: Attribute Level Confidentiality (Including De-Identification)', https://www.dicomstandard.org/News-dir/ftsup/docs/sups/sup55.pdf (zuletzt aufgerufen am 19.05.2022).

5.2.3 Zwischenfazit

Für die Beurteilung des Use Cases wird somit unterstellt, dass der Geltungsbereich des HFG bejaht werden kann, da unverschlüsselte genetische Daten und biologisches Material sowie verschlüsselte nicht-genetische Gesundheitsdaten zu Forschungszwecken (weiter-)verwendet werden, um Fragen zu Krankheiten des Menschen nachzugehen.

5.2.4 Verwendung der Gesundheitsdaten im Forschungsprojekt

Damit das Forschungsprojekt rechtskonform durchgeführt werden kann, braucht es eine Bewilligung der zuständigen Ethikkommission. Gegenstand der Prüfung ist der vorgesehene Ablauf des Projekts und die Unterlagen zur Einholung der Einwilligungen. Denn sowohl für die Teilnahme an Forschungsprojekten und der damit verbundenen Beschaffung von Daten, als auch für die Weiterverwendung von bereits erhobenen Daten, ist grundsätzlich eine Einwilligung der betroffenen Personen erforderlich. Im Use Case, wo auch von der Durchführung prospektiver Studien die Rede ist, sind beide Elemente enthalten, wobei die Weiterverwendung im Fokus steht.

Die Einwilligung ist von den betroffenen Personen einzuholen. Die Anforderungen an die Einwilligung (wie eingehend erläutert wurde, gibt es zwei Arten von Einwilligungen gemäss den Vorgaben des HFG) sind bis zu einem gewissen Grad identisch, unterscheiden sich aber in den Details. Zentral ist bei allen die Aufklärung und damit die hinreichende Information, die einer gültigen Einwilligung der betroffenen Personen vorausgehen muss. Es handelt sich dabei um eine Anforderung, die sowohl im HFG als auch in den sektorübergreifenden Datenschutzgesetzen (Bund und Kantone) vorgesehen ist. Für die Ausgestaltung der Informations- und Einwilligungsunterlagen im Use Case stellt sich somit die Frage, welche Vorgaben massgeblich sind. Es besteht Einigkeit, dass die Regeln des HFG als Spezialregelung für die Humanforschung den Vorschriften in den allgemeinen Datenschutzgesetzen vorgehen. Weitgehend ungeklärt ist jedoch die Frage, inwieweit die Vorschriften der Datenschutzgesetze auch ergänzend zur Anwendung gelangen können.[680] Dies wird jedenfalls dort bejaht werden müssen, wo eine Regelung des HFG nicht als abschliessend betrachtet werden kann. Für welche Regelungen dies zutrifft, ist wiederum teilweise ungeklärt. Es muss für den Use Case genauso wie bei anderen Forschungsprojekten damit gerechnet werden, dass für die Aufklärung und Einwilligung auch gewisse zusätzliche Anforderungen der Datenschutzgesetze beachtet werden müssen, welche nicht explizit im HFG und der Ausführungsverordnung (HFV) aufgeführt sind.

Aufbauend darauf ist für den Use Case zu klären, welche der sektorübergreifenden Gesetze konkret ergänzend zu berücksichtigen sein könnten. Es stellt sich also die Frage, ob das DSG oder eines oder mehrere der kantonalen Gesetze massgeblich sind. Die massgeblichen Kriterien für diese Prüfung sind nicht alle klar, wobei bei einer Tätigkeit, die im Rahmen eines öffentlich-rechtlichen Forschungsauftrags durchgeführt wird, bspw. von einem Kantonsspital, von der Anwendbarkeit der kantonalen Vorschriften des jeweiligen Spitals auszugehen sein dürfte. Nicht ausgeschlossen ist jedoch auch das Handeln eines Spitals als Privater. Dies führt letztlich dazu, dass nicht nur die Vorschriften mehrerer Staaten (die DSGVO und nationale Vorschriften von EU-Mitgliedstaaten), sondern auch Vorschriften innerhalb der Schweiz, zusätzlich zum HFG, also eine Vielzahl nicht vollständig harmonisierter Datenschutzgesetze zu berücksichtigen ist. Dies sorgt nicht nur für einen grossen Aufwand, sondern auch zu Rechtsunsicherheit.

Rechtsunsicherheit entsteht dabei bspw. in einem zentralen Aspekt zur Frage, was konkret alles Gegenstand der Aufklärung und Information der betroffenen Personen sein muss. In den Spezialregelungen zur Humanforschung wird nur in den besonderen Vorschriften für die klinischen Versuche verlangt, dass der Sponsor

[680] Vgl. Abschnitt 4.2.2.

angegeben wird. Im nDSG ist jedoch die Angabe des oder der für die Datenbearbeitungen Verantwortlichen eine der zentralen Pflichtangaben. Es ist deshalb damit zu rechnen, dass eine solche Angabe auch bei Einwilligungen für die Humanforschung erforderlich ist. Dies gilt allerdings wiederum nur im Anwendungsbereich des nDSG. Auf kantonaler Ebene fehlt zumindest teilweise eine explizite Regelung dazu. Ob die Angabe deshalb aber unter den jeweiligen kantonalen Vorschriften tatsächlich nicht erforderlich ist, bleibt offen. Hinzu kommt, dass die Kantone teilweise auch von einem unterschiedlichen Verständnis des Begriffs der Verantwortlichen ausgehen.

Im HFG selbst und der HFV sind sodann eine Vielzahl von Pflichtangaben explizit aufgeführt. Die erforderlichen Angaben unterscheiden sich nach der Art der Einwilligung. Im vorliegenden Use Case interessiert die (Weiter-)Verwendung von bereits bei Schweizer Spitälern, onkologischen Arztpraxen sowie anderen Forschungsprojekten beschaffte personenbezogene Daten. Für die Weiterverwendung solcher Daten sind die besonderen Regelungen in Art. 32 ff. HFG zu beachten, welche je nach Kategorie der betroffenen Daten unterschiedliche Anforderungen stellen.

Im vorliegenden Use Case gelten die höchsten Anforderungen für die geplante Verwendung von unverschlüsseltem biologischem Material und genetischen Daten. Für die Weiterverwendung dieser Datenkategorien sind keine Erleichterungen im Vergleich zu einer gewöhnlichen Einwilligung vorgesehen. Die Einwilligung kann daher nur für das spezifische Forschungsprojekt eingeholt werden und nichtgenerell für beliebige noch nicht näher definierbare weitere Forschungsprojekte. Es braucht mit anderen Worten eine hinreichende Umschreibung des Forschungsprojekts, inklusive Art, Zweck, Dauer und Verlauf, sowie zahlreiche weitere Pflichtangaben. Ein sogenannter Generalkonsent, d.h. eine sehr breit gefasste Einwilligung für die Weiterverwendung von Gesundheitsdaten zu Forschungszwecken, also beliebigen noch unbestimmten Forschungsvorhaben, ist in diesem Fall somit unzureichend.

Für die im Use Case ebenfalls geplante Verwendung von verschlüsselten nicht-genetischen Gesundheitsdaten genügt demgegenüber die Information und das Ausbleiben des Widerspruchs der betroffenen Personen. Aus praktischen Überlegungen und mit Blick auf die erforderliche Nachweisbarkeit bringt dies im Vergleich zum Generalkonsent aber kaum Vorteile, weshalb sich oftmals gleichwohl die Aushändigung und Unterzeichnung des jeweiligen Formulars für den Generalkonsent aufdrängen wird. Sowohl in Bezug auf die Aufklärung für das Widerspruchsrecht als auch den Generalkonsent stellen sich Fragen zu den ergänzenden Anforderungen der sektorübergreifenden Datenschutzgesetze.

Ausgehend davon ist die Beurteilung der Anforderungen an die Aufklärung und Einwilligung nicht bei allen im Use Case betroffenen Datenkategorien gleich. Auch für den Fall, dass diese Anforderungen eingehalten und Einwilligungen wirksam eingeholt werden, ist die Reichweite bei der gewöhnlichen Einwilligung und dem Generalkonsent nicht dieselbe. Dies gilt umso mehr als die Einwilligungserklärungen von unterschiedlichen Stellen ausformuliert sind und sich auch hieraus unterschiedliche Reichweiten ergeben können. Daraus resultiert weitere Unsicherheit, weil sich die an einem Forschungsprojekt Beteiligten darauf verlassen können müssen, dass die Einwilligungen an den jeweiligen Datenerhebungspunkten hinreichend weit und wirksam eingeholt wurden und dies im Streitfall auch bewiesen werden muss, also eine entsprechende Dokumentation vorhanden ist. Insbesondere bei Daten, die wie im Use Case vorgesehen, aus anderen Forschungsprojekten und Datenbanken stammen, kann dies erhebliche Unsicherheiten mit sich bringen. In diesem Zusammenhang muss angenommen werden, dass der datenschutzrechtliche Rechtmässigkeitsgrundsatz gilt, wonach die Weiterbearbeitung von unrechtmässig erhobenen Daten unzulässig ist. Daraus kann sich eine weitere Quelle von Unsicherheiten ergeben.

Hindernisse für die Einholung gültiger Einwilligungen stellen ferner auch die Anforderungen an die Verständlichkeit und die Schriftlichkeit dar. Auch wenn Argumentationsspielraum für die Zulässigkeit digitaler Lösungen besteht, wird jedenfalls in der Praxis zur Vermeidung von Risiken eine handschriftliche Unterzeichnung auf einer Erklärung in Papierform eingeholt. Dies erschwert die Einholung und Verwaltung erheblich. Weiter ist gemäss der Anforderung der Verständlichkeit mit geeigneten Massnahmen sicherzustellen, dass die konkret betroffene Person die wesentlichen Punkte der Aufklärung auch (subjektiv) verstanden hat.

Nur wenn all diese hohen Voraussetzung erfüllt werden können, ist die Weiterverwendung der Daten gemäss Use Case erlaubt. Alternativ sind die Anforderungen der sog. escape clause zu erfüllen und es ist eine Ausnahmebewilligung einzuholen. Die Hürden dafür sind hoch.

Im vorliegenden Use Case gilt es in Bezug auf die prospektiven Studien zu beachten, dass es selbst mit gültiger Einwilligung der Teilnehmenden unwahrscheinlich erscheint, direkten Zugriff auf das Primärsystem der Spitäler (Klinikinformationssystem, in dem die Patientendaten gespeichert sind) zu erhalten; dies bereits aus Sicherheitsgründen. Darüber hinaus wird nach aktuellem Stand auch der direkte Zugriff auf das elektronische Patientendossier gemäss dem Gesetz über das elektronische Patientendossier durch die Forschenden bereits deshalb wenig sinnvoll sein, weil darin im jetzigen Zeitpunkt keine strukturierten Daten vorhanden sind und die Patienten vielfach noch gar nicht über ein elektronisches Patientendossier verfügen. Zudem wird auch die Sicherstellung der hinreichenden Information für eine gültige Einwilligung schwierig und im Falle von öffentlichen Organen die gesetzliche Grundlage fraglich sein. Zu berücksichtigen ist ferner, dass sich die Schwierigkeiten weiter erhöhen, wenn im Rahmen des Use Cases ein Zugriff aus den USA oder eine andere Form der Bekanntgaben von Daten oder eine Ausfuhr in die USA erfolgen soll. Denn die USA gelten, wie viele andere Länder ausserhalb des EWR auch, als Land ohne angemessenes Datenschutzniveau und eine einfache, rechtssichere Lösung zur Sicherstellung rechtmässiger Datentransfers in Länder wie die USA ist derzeit nicht in Sicht. Denkbar sind einzig Verschlüsselungslösungen, wobei dann wiederum hohe technische Anforderungen zu berücksichtigen sind, deren Einhaltung im Streitfall unter Umständen auch nachgewiesen werden müssen.

5.2.5 Fazit

Die Analyse des Use Cases verdeutlicht deshalb insbesondere die nachfolgenden Hindernisse:

- Unklarheiten in Bezug auf die Anonymisierung, Pseudonymisierung/Verschlüsselung und die damit verbundene Frage nach den datenschutzrechtlichen Rollen;

- Unsicherheiten zum Verhältnis zwischen den Vorschriften des HFG und der Datenschutzgesetze des Bundes und der Kantone;

- Hohe und unklare Anforderungen an die wirksame Einwilligung in die Sekundärnutzung (insb. Schriftformerfordernis);

- Ungenügende Nutzbarkeit des elektronischen Patientendossiers.

5.3 Use Case III: Sekundärnutzung für gesundheitspolitische Zwecke

5.3.1 Use Case

In der Schweiz grassiert eine Pandemie, zu deren Bekämpfung politische Entscheidungsträger schnell über eine umfassende und aktuelle Faktenlage verfügen müssen. Die zuständigen Gesundheitsbehörden benötigen dazu einen Zugriff auf tagesaktuelle Gesundheitsdaten der Erkrankten. Die Verknüpfung dieser Daten mit der AHV-Nummer der Erkrankten ermöglicht die kontinuierliche Überwachung der Infektionen und des Expositionsrisikos gefährdeter Personen, sollte die Pandemie für eine bestimmte Altersgruppe ein erhöhtes Risiko darstellen. Hiervon versprechen sich die Entscheidungsträger der öffentlichen Hand unter anderem genaue Modellvorhersagen über den künftigen Bedarf an Spitalressourcen (ärztliches und nicht-ärztliches Gesundheitspersonal, Betten, medizinische Hilfsmittel).

5.3.2 Analyse

Im Fokus dieses Use Cases steht die Datenbearbeitung der in den Vollzug des Bundes-Epidemiengesetzes (EpG) involvierten Stellen in Bund und Kantonen. Bei diesen Stellen handelt es sich um das Bundesamt für Gesundheit (BAG), die kantonalen Gesundheitsdirektionen und die weiteren öffentlichen und privaten Institutionen des Gesundheitswesens, wie z.B. Ärztinnen und Ärzte, Spitäler und Laboratorien.[681] Für die Analyse des Use Cases ist zu prüfen, welche datenschutzrechtlichen Vorschriften auf die Datenbearbeitungen dieser Stellen zur Anwendung gelangen.

Offensichtlich ist die Anwendbarkeit der im Epidemiengesetz vorgesehenen besonderen Datenbearbeitungsregeln. Es handelt sich hier wiederum um ein Spezialgesetz, das in seinem Geltungs- und Regelungsbereich den sektorübergreifenden Vorschriften der Datenschutzgesetze des Bundes und der Kantone vorgeht. Im Übrigen bleiben die Datenschutzgesetze weiterhin anwendbar. Zu beurteilen ist jedoch, ob das DSG oder kantonale Datenschutzgesetze greifen.

Die Kriterien für diese Beurteilung sind jedoch nicht klar. Unproblematisch dürfte dabei zwar bspw. die Beurteilung in Bezug auf das Bundesamt für Gesundheit oder die kantonalen Gesundheitsdirektionen sein. Diese sind jeweils klar der Verwaltung des Bundes bzw. des jeweiligen Kantons zugerechnet, erfüllen eine öffentliche Aufgabe und handeln dabei grundsätzlich nicht privatrechtlich. In Bezug auf die Gesundheitsdirektionen könnte sich zwar die Frage stellen, ob es im Zusammenhang mit dem Epidemiengesetz nicht eine öffentliche Aufgabe des Bundes ist, die sie erfüllen. Allerdings steht fest, dass der Kantonsverwaltung zuzurechnende Rechtseinheiten, wie es die kantonalen Gesundheitsdirektionen regelmässig sind, nicht zu Bundesorganen werden, nur weil sie Bundesgesetze, wie hier das Epidemiengesetz, vollziehen. Deutlich schwieriger wird jedoch die Beurteilung von anderen im Use Case angesprochenen Institutionen des Gesundheitswesens, wie z.B. Spitälern, die in der kantonalen Gesetzgebung nicht der Kantonsverwaltung zugerechnet werden. Bei diesen ist nicht ausgeschlossen, dass sie, je nach konkreter Datenbearbeitung, als Organ eines Kantons oder des Bundes zu beurteilen sind. Sie könnten also für unterschiedliche Datenbearbeitungen unterschiedlichen Datenschutzgesetzen unterstellt sein. Ähnlich schwierige Fragen und Abgrenzungen stellen sich auch für privatrechtlich handelnde öffentlich-rechtliche Organisationen oder für private Unternehmen, die im Gesundheitswesen tätig sind, wie bspw. Hausärzte. So ist nicht von vornherein klar, inwieweit diese bei der Erhebung von Daten eines Infizierten und der Übermittlung der Daten an die zuständigen Behörden in Erfüllung ihrer Meldepflicht den datenschutzrechtlichen Vorschriften für Private unterstehen oder nicht.

[681] Vgl. Art. 102 Abs. 3, Art. 105 Epidemienverordnung (EpV) und Art. 12 EpG.

Für einen wesentlichen Teil der datenschutzrechtlichen Fragen wird die abschliessende Klärung der Unterstellung nicht erforderlich sein. Gleichwohl besteht in diesem grundlegenden Punkt Unklarheit und es ist schwer abschätzbar, wie die Gerichte in einem Streitfall entscheiden würden. Mit Blick auf die im Use Case anvisierten Datenübermittlungen steht zumindest fest, dass das Epidemiengesetz selbst eine rechtliche Grundlage vorsieht, welche die Datenbearbeitungen und -bekanntgaben der hier betroffenen Gesundheitsdaten erlauben. Den im Use Case interessierenden Institutionen des Gesundheitswesens sind daher Übermittlungen der tagesaktuellen Gesundheitsdaten der Erkrankten erlaubt und es ist grundsätzlich von der Rechtmässigkeit der Erhebung und Übermittlung auszugehen. Das Epidemiengesetz, das die Meldepflichten vorsieht, ist nicht nur in Bezug auf Bundesorgane, sondern auch im Rahmen der kantonalen Datenschutzgesetze als hinreichende Grundlage im Sinne des Legalitätsprinzips zu betrachten, was eigentlich selbstverständlich erschiene, wenn nicht gewisse kantonale Gesetze ausdrücklich ein anderes (falsches) Verständnis der erforderlichen Grundlagen definiert hätten. Für die im Use Case gegebenenfalls privatrechtlich handelnden Beteiligten stellt die Meldepflicht ferner ein Rechtfertigungsgrund dar.

Ausgehend davon handelt es sich im Use Case bei der Nutzung der Daten aus dem Behandlungskontext zum Zweck der Pandemien-/Epidemiebenkämpfung im Übrigen auch um keine Zweckänderung und keinen Verstoss gegen das Zweckbindungsgebot. Denn die Erstellung von Modellvorhersagen über den künftigen Bedarf an Spitalressourcen, gestützt auf die gemeldeten Gesundheitsdaten, ist als Datenbearbeitung zum gesetzlich festgehaltenen Zweck des Schutzes der öffentlichen Gesundheit zu sehen. Die Einzelheiten dürften demgegenüber wiederum weniger klar sein. Dies gilt namentlich für das Prinzip der Verhältnismässigkeit der Datenbearbeitung bzw. der Datensparsamkeit und Speicherbegrenzung. Deren Einhaltung hat bei öffentlichen Organen des Bundes und der Kantone unmittelbar Einfluss auf die Zulässigkeit der Bearbeitung, lassen sich doch Verstösse dagegen nicht rechtfertigen. Aber auch bei Privaten, wo ein Verstoss theoretisch gerechtfertigt werden könnte, gilt dies indes nur beschränkt. Soll die Rechtfertigung, wie hier in der gesetzlichen Grundlage des Epidemiengesetzes gesehen werden, greift die Rechtfertigung nur so weit, wie auch die Grundlage reicht. Werden also z.B. mehr Daten bearbeitet als zur Erfüllung der gesetzlichen Zwecke, was für den Schutz der öffentlichen Gesundheit und der Planung der Spitalressourcen erforderlich ist, liegt gleichwohl eine widerrechtliche Datenbearbeitung vor.

Trotz der weitreichenden gesetzlichen Grundlagen und Verpflichtungen von Daten in grossem Umfang muss somit für jede Datenbearbeitung im Einzelnen geprüft werden, inwieweit diese zur Erfüllung der gesetzlichen Zwecke tatsächlich erforderlich und zumutbar ist. In Bezug auf die im Use Case vorgesehen Auswertungen stellt sich die Frage, inwieweit überhaupt die Identität der betroffenen Personen eine Rolle spielt und folglich auch eine Anonymisierung oder Pseudonymisierung denkbar wäre. Auch wenn die Übermittlung von Gesundheitsdaten mitsamt den Detailangaben zur Identität der Person im Gesetz grundsätzlich vorgesehen ist, bedeutet dies noch nicht, dass auch jede Weiterbearbeitung der Daten verhältnismässig und damit zulässig ist. Ähnliche Fragen zur Verhältnismässigkeit stellen sich in Bezug auf die Verwendung der AHV-Nummer. Diese wird von sehr vielen öffentlichen Stellen verwendet und ermöglicht daher eine Verknüpfung mit einer Vielzahl von Daten und birgt damit auch ein gewisses Missbrauchs-/Sicherheits-Risiko. Ähnliches gilt in Bezug auf einen im Use Case angedeuteten direkten Zugriff von Behörden auf Primärsysteme der Institutionen im Gesundheitswesen. Auch dies birgt ein Sicherheitsrisiko und ist ein Aspekt, der in die mitunter schwierige Einzelfallbeurteilung des Verhältnismässigkeitsgrundsatzes einzubeziehen ist. Inwieweit das erstrebte Ziel der Auswertungen auch mit anderen Daten oder Pseudonymen oder durch andere Datenübermittlungsformen erreicht werden kann, muss im Einzelfall unter Einbezug der relevanten technischen und wirtschaftlichen Gegebenheiten beurteilt werden.

Es besteht dabei jedenfalls ein grosser Argumentationsspielraum sowohl in Bezug auf die Erforderlichkeit der Bearbeitung gewisser Daten als auch im Rahmen der Abwägung der verschiedenen Interessen bei der Prüfung der Zumutbarkeit einer Datenbearbeitung. Damit verbunden ist auch eine Rechtsunsicherheit, die

für die Sekundärnutzung der Daten hinderlich sein kann. Ein weiteres Hindernis für die effiziente Nutzung der Daten ist die fehlende Vorgabe an das Format der Datenübermittlungen, also des Meldemittels. Bekanntlich können die Institutionen des Gesundheitswesens ihrer Meldepflicht auch durch Übermittlungen per Briefpost oder Fax nachkommen und es ist (leider) keine elektronische Übermittlung vorgeschrieben.

5.3.3 Fazit

Die Analyse des Use Cases verdeutlicht insbesondere die nachfolgenden Hindernisse:

- Unklarheiten bei der Abgrenzung zwischen kantonalen Datenschutzgesetzen und dem Datenschutzgesetz des Bundes;

- Unklarheiten bei gesetzlich an sich erlaubten Datenbearbeitungen infolge offener Anforderungen aus den Datenbearbeitungsgrundsätzen (insb. Verhältnismässigkeitsgrundsatz);

- Ungenügende Rahmenbedingungen zur elektronischen Datenübermittlung.

6. Entwicklungen in der EU

Wie bei der Analyse der rechtlichen Rahmenbedingungen und den obigen Use Cases verdeutlicht wurde, besteht in der Schweiz dringender Handlungsbedarf im Bereich der Sekundärnutzung von Gesundheitsdaten. Die aktuelle Rechtslage birgt zudem die Gefahr, Innovationen im wichtigen Life-Science-Bereich zu bremsen und eines Wettbewerbsnachteils im internationalen Vergleich. Die Europäische Kommission hat erkannt, dass auch in der EU zahlreiche rechtliche Hürden und Unsicherheiten bei der Weiterverwendung von Gesundheitsdaten bestehen. Als Reaktion darauf hat die Kommission im Mai 2022 den Verordnungsentwurf für den European Health Data Space (EHDS) präsentiert.[682] Im Folgenden werden die wesentlichen Eckpunkte des Entwurfs erläutert, um aufbauend darauf, sowie auf den Erkenntnissen der vorangehenden Untersuchung, Massnahmen zur Anpassung der Gesetzgebung in der Schweiz vorzuschlagen.

6.1 Überblick European Health Data Space (EHDS)

Durch den EHDS soll ein gemeinsamer Datenraum geschaffen werden, welcher Betroffenen mehr Verfügungsmacht über ihre elektronischen Gesundheitsdaten verleiht. Gleichzeitig soll der EHDS Forschern, Innovatoren und politischen Entscheidungsträgern ermöglichen, diese elektronischen Gesundheitsdaten in einer datenschutzfreundlichen und sicheren Weise zu bearbeiten.[683]

Wie bereits erwähnt, erschwert nach Ansicht der EU-Kommission die aktuelle Rechtslage die Erreichung der ambitionierten Ziele der EU in den Bereichen Medizin, Forschung und Innovation. Zwar sorgt die Datenschutz-Grundverordnung (DSGVO) für eine – grösstenteils – einheitliche Rechtslage im Bereich der Bearbeitung von personenbezogenen Daten, jedoch führt der mitgliedsstaatliche Regelungsspielraum im Bereich der Bearbeitung von sensitiven Daten zu Forschungs-, Archiv- und statistischen Zwecken zu Problemen; insbesondere in internationalen Forschungsprojekten. So können nach der einschlägigen Regelung der

[682] Proposal for the Regulation on the European Health Data Space, COM(2022) 197 final.

[683] Proposal for the Regulation on the European Health Data Space, COM(2022) 197 final.

DSGVO[684] "besondere Kategorien von personenbezogenen Daten" – wie bspw. Gesundheitsdaten – auch ohne Einwilligung für im öffentlichen Interesse liegende Zwecke – wie bspw. medizinische Forschung – verarbeitet werden. Die Vorschrift verweist jedoch auf eine sog. Öffnungsklausel,[685] welche es den Mitgliedstaaten ermöglicht, diese Verarbeitungstätigkeit eigens auf nationaler Ebene zu regeln. Die durch die Inanspruchnahme der Öffnungsklausel entstandene uneinheitliche europäische Rechtslage erschwert nun die Zusammenarbeit in europäischen Forschungsprojekten, wie bspw. im Rahmen von Horizon 2020 oder dem europäischen "Beating Cancer Plan".[686]

Darüber hinaus hat die Covid-19 Pandemie nach Ansicht der EU-Kommission eindrücklich gezeigt, wie wichtig der unbürokratische und schnelle Zugriff auf qualitativ hochwertige und repräsentative Gesundheitsdaten sein kann. Daten zu aktuellen Ansteckungszahlen, der Schwere der Krankheitsverläufe und der Wirksamkeit von Massnahmen stellten eine essenzielle Entscheidungsgrundlage für die Wissenschaft und Politik im Umgang mit der Pandemie dar. Ferner hat die Pandemie in den Augen der EU-Kommission verdeutlicht, dass uneinheitliche Datenformate und Standards die Zusammenarbeit innerhalb der Union erheblich erschwert.[687]

6.2 Zusammenspiel mit anderen EU-Rechtsakten

Die Kommission betont im Entwurf der Verordnung für den EHDS, dass die damit verfolgten Ziele im Einklang mit den Zielen der Agenda für einen digitalen Binnenmarkt[688], der Europäischen Gesundheitsunion[689] und der Europäischen Datenstrategie stehen.[690] In diesem Zusammenhang sind insbesondere die folgenden (geplanten) Rechtsakte von Bedeutung.

6.2.1 CBHC-Richtlinie (2011/24/EU)

Der grenzüberschreitende Austausch von Gesundheitsdaten war bereits bisher – zumindest zum Teil – in der Richtlinie 2011/24/EU über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (CBHC-RL) geregelt. Der Art. 14 CBHC-RL sieht die Einführung eines eHealth-Netzwerks vor, welches sich aus Experten auf dem Gebiet der elektronischen Gesundheitsdienste zusammensetzt und sich für die Förderung von Interoperabilität, die Erstellung von Richtlinien und technischen Standards von Gesundheitsdaten einsetzen soll. Aufgrund des freiwilligen Charakters der erarbeiteten Richtlinien hatte das genannte eHealth-Netzwerk einen geringen Einfluss auf die Ausübung von Zugriffs- und Kontrollrechten der betroffenen Patientinnen und Patienten auf ihre Gesundheitsdaten. Durch den EHDS sollen die Vorschriften

684 Art. 9 Abs. 2 lit. j DSGVO.

685 Art. 89 Abs. 2 DSGVO.

686 European's Beating Cancer Plan: https://ec.europa.eu/health/system/files/2022-02/eu_cancer-plan_en_0.pdf (zuletzt aufgerufen am 26.05.2022).

687 Proposal for the Regulation on the European Health Data Space, COM(2022) 197 final.

688 European's Beating Cancer Plan: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_de (zuletzt aufgerufen am 26.05.2022).

689 European's Beating Cancer Plan: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_de (zuletzt aufgerufen am 26.05.2022).

690 Proposal for the Regulation on the European Health Data Space, COM(2022) 197 final, S. 3; European's Beating Cancer Plan: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de (zuletzt aufgerufen am 26.05.2022).

der CBHC-RL abgelöst und dadurch die Patientenrechte gestärkt und verbindliche Standards für Gesundheitsdaten eingeführt werden.

6.2.2 DSGVO (Verordnung 2016//679/EU)

Sofern personenbezogene Gesundheitsdaten bearbeitet werden, gilt es in der EU die Vorgaben der Datenschutzgrundverordnung (DSGVO) zu beachten. Grundsätzlich lässt der Entwurf der EHDS-Verordnung die Anwendbarkeit der DSGVO unberührt, jedoch sollen gewisse Rechte in Bezug auf Gesundheitsdaten, welche besonderen Schutz geniessen, gestärkt werden. Hierbei wird insbesondere auf die Stärkung der Verfügungsmacht der Patientinnen und Patienten über ihre Gesundheitsdaten abgezielt. Konkret soll durch den EHDS das in Art. 20 DSGVO verankerte Recht auf Portabilität und Interoperabilität in Bezug auf Gesundheitsdaten ausgebaut werden.

Neben der Stärkung der Patientenrechte soll der Zugriff auf Gesundheitsdaten für legitime Zwecke erleichtert werden. Die eingangs erwähnte Öffnungsklausel in der DSGVO eröffnet nicht nur den Mitgliedsstaaten einen Regelungsspielraum für Datenverarbeitungen im Forschungskontext, sondern erlaubt auch spezialgesetzliche EU-Bestimmungen. Durch die Verordnung zum EHDS soll dieser Regelungsspielraum in Anspruch genommen werden und wird – aufgrund der Höherrangigkeit von EU-Recht in dessen Kompetenzbereich – widersprechende nationale Bestimmungen verdrängen.

6.2.3 Data Governance Act und (Draft) Data Act

Bei der Schaffung eines Rahmens für die Sekundärnutzung elektronischer Gesundheitsdaten baut der EHDS auf zwei weiteren kürzlich vorgeschlagenen Regelwerken auf: dem Data Governance Act (DGA)[691] und dem Data Act (DA)[692]. Als horizontaler Rechtsrahmen legt der DGA nur allgemeine Bedingungen für die Weiterverwendung von Daten des öffentlichen Sektors fest, ohne ein echtes Recht auf Weiterverwendung solcher Daten zu schaffen. Der vorgeschlagene DA verbessert die Übertragbarkeit bestimmter nutzergenerierter Daten, zu denen auch Gesundheitsdaten gehören können, enthält aber keine Vorschriften für alle Gesundheitsdaten.

Daher ergänzt der EHDS diese vorgeschlagenen Rechtsakte und enthält spezifischere Vorschriften für den Gesundheitssektor, bspw. in Bezug auf den Austausch elektronischer Gesundheitsdaten, das standardisierte Format für Gesundheitsdaten und die Voraussetzungen für den Datenzugriff. Folglich enthält der EHDS Spezialvorschriften für die Sekundärnutzung von Gesundheitsdaten, die Vorrang gegenüber dem DGA und DA enthalten. Sofern der EHDS in gewissen Bereichen aber keine abschliessende Regelung vornimmt, kommen die genannten Rechtsakte zur Anwendung.

6.3 Ausgewählte Regelungsbereiche des EHDS

Wie bereits angesprochen, bezweckt die EU-Kommission mit dem vorliegenden Verordnungsentwurf einen europäischen Gesundheitsdatenraum ("E-EHDS") zu schaffen, indem Regeln, gemeinsame Standards und

691 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), COM(2020) 767 final.

692 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final.

Verfahren, Infrastrukturen und ein Rechtsrahmen für die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten festgelegt werden.[693] Im Folgenden werden einige wesentliche Regelungsvorschläge aufgegriffen, die für die vorliegend untersuchten Fragestellungen relevant sind.

6.3.1 Interoperabilität von Gesundheitsdaten

In der Praxis stellen häufig uneinheitliche Standards und Datenformate eine Hürde für die Weiterverwendung von Daten aus verschiedenen Quellen dar. Um den Austausch von elektronischen Gesundheitsdaten und deren Nutzung zu erleichtern, will die EU einheitliche Datenstandards normieren. So schafft z.B. Art. 6 E-EHDS die Grundlage für die Einführung eines "European electronic health record exchange format"[694] Laut Legaldefinition ist darunter ein strukturiertes, allgemein verwendetes und maschinenlesbares Format, das die Übertragung personenbezogener elektronischer Gesundheitsdaten zwischen verschiedenen Softwareanwendungen, Geräten und Gesundheitsdienstleistern ermöglicht, zu verstehen.[695] Die genauen technischen Spezifikationen sollen hierbei in gesonderten Rechtsakten festgelegt werden.[696] Diese Massnahme soll sowohl die grenzüberscheitende Erbringung von Gesundheitsdienstleistungen (bspw. ärztliche Behandlung) als auch die Weiterverwendung der Daten zu anderen Zwecken erleichtern.

Neben dieser allgemeinen technischen Standardisierung von elektronischen Gesundheitsdaten, sollen auch einheitliche rechtliche und technische Standards für die Verwaltung von elektronischen Patientendossiers (EHR-Systeme) geschaffen werden.[697] Das EHR-System ist hierbei wie folgt definiert: "eine Sammlung elektronischer Gesundheitsdaten, die sich auf eine natürliche Person beziehen und im Gesundheitssystem gesammelt und für Zwecke der Gesundheitsversorgung verarbeitet werden". Folglich sollen diese Systeme primär für die medizinische Versorgung eingesetzt werden, jedoch soll eine Sekundärnutzung der darin beinhalteten elektronischen Gesundheitsdaten (electronic health record "EHR") ermöglicht werden.[698]

Darüber hinaus ist im EHDS vorgesehen, dass Daten aus sogenannten "Wellness Applications" (WA) mit EHR-Systemen verknüpft werden können.[699] Unter einer WA ist jedes Gerät oder jede Software zu verstehen, das oder die vom Hersteller dazu bestimmt ist, von einer natürlichen Person für die Verarbeitung elektronischer Gesundheitsdaten zu anderen Zwecken als der Gesundheitsfürsorge verwendet zu werden, bspw. für das Wohlbefinden und eine gesunde Lebensweise. Hiermit sind u.a. Smartwatches, Wearables und Gesundheitsapps gemeint. Sofern der Hersteller einer WA angibt, dass sein Produkt mit EHR-Systemen kompatibel ist, muss er sich an die für EHR-Systeme geltenden Spezifikationen und Standards halten.[700]

---

693 Art. 1 Abs. 1 Vorschlag für eine Verordnung über den Europäischen Gesundheitsdatenraum (EHDS).

694 Hier wird auf die englischen Formulierungen zurückgegriffen, um Unschärfen bei der Übersetzung zu vermeiden; bisher liegt noch keine offizielle deutsche Sprachfassung des Verordnungsentwurfs vor.

695 Art. 2 Abs. 2 lit. g E-EHDS.

696 Art. 6 Abs. 1 E-EHDS.

697 Art. 17 ff. E-EHDS.

698 Vgl. Art 33 ff. E-EHDS.

699 Art. 31 ff. E-EHDS.

700 Art. 31 Abs. 1 ff. E-EHDS.

Neben dem oberhalb beschrieben standardisierten Datenformat, legt der Verordnungsentwurf in Art. 55 ff. Standards für die Datenqualität der elektronischen Gesundheitsdaten fest.

6.3.2 Sekundärnutzung

Der Verordnungsentwurf des EHDS sieht in Kapitel IV umfassende Rahmenbedingungen für die Sekundärnutzung von elektronischen Gesundheitsdaten vor. Gemäss Art. 33 E-EHDS müssen Dateninhaber ("data holders") eine umfangreiche Liste[701] an verschiedenen elektronischen Gesundheitsdaten für die Sekundärnutzung zur Verfügung stellen. Die Definition des Dateninhabers ist sehr weit gefasst und umfasst praktisch alle Gesundheits-, Pflege- und Forschungseinrichtungen (die im Gesundheitssektor forschen) sowie Unionsorgane, die berechtigt sind, elektronische Gesundheitsdaten zu teilen.[702] Zu den Daten, die zur Verfügung gestellt werden müssen, zählt auch das elektronische Patientendossier (EHR).

Der Zugang zu den zur Verfügung gestellten elektronischen Gesundheitsdaten ist von der Zustimmung der nationalen Stelle abhängig, die für den Zugang zu Gesundheitsdaten zuständig ist ("health data access body").[703] Der Antragssteller, der die Daten weiterverwenden will, erhält nur Zugriff auf Daten des EHDS sofern er mit der Bearbeitung einen der in Art. 34 Abs. 1(abschliessend) aufgezählten Zwecke verfolgt. Hierzu zählt bspw.: die Forschung im Gesundheitssektor; die Entwicklung von innovativen Produkten oder Dienstleistungen, die der öffentlichen Gesundheit dienen; für das Training und Testen von AI Algorithmen, die der öffentlichen Gesundheit dienen; oder für die personalisierte Gesundheitsversorgung. Obwohl die aufgezählten Bereiche einen gewissen Interpretationsspielraum bieten, sorgt die Liste an erlaubten Bearbeitungszwecken für Klarheit inwiefern die elektronischen Gesundheitsdaten des EHDS grundsätzlich verwendet werden dürfen. Ferner verdeutlicht Art. 35 E-EHDS, welche Bearbeitungsaktivitäten definitiv verboten sind.

Grundsätzlich soll im Rahmen des EHDS nur Zugang zu anonymisierten elektronischen Gesundheitsdaten gewährt werden.[704] Kann der Zweck der Bearbeitung durch den Datennutzer nicht mit anonymisierten Daten erreicht werden, gewähren die zuständigen Stellen Zugang zu elektronischen Gesundheitsdaten in pseudonymisierter Form.[705] Für die Rechtsunsicherheit, die mit der potentiellen Entschlüsselung von pseudonymisiert Daten einhergeht, wählte die Kommission in ihrem Verordnungsentwurf einen relativ pragmatischen Ansatz. Dem Datennutzer ist es demzufolge – unter Androhung einer Strafe – verboten, die bereitgestellten Daten zu re-identifizieren.[706] Darüber hinaus erhält der Datennutzer nur im Rahmen eines "Secure Processing Environments" Zugang zu den (anonymisierten oder pseudonymisierten) elektronischen Gesundheitsdaten.[707] Dies gewährt einerseits, dass nur Berechtigte Zugriff zu den Daten haben und andererseits ermöglicht es den Behörden zu überprüfen, ob der Datennutzer die Daten lediglich zu den genehmigten Zwecken bearbeitet.

---

701 Art. 33 Abs. 1 E-EHDS.

702 Art. 2 Abs. 2 lit. y E-EHDS; Kleinstunternehmen sind gemäss Art. 33 Abs. 2 V_EHDS von dieser Pflicht befreit.

703 Art. 44 Abs. 1 E-EHDS.

704 Art. 44 Abs. 2 E-EHDS.

705 Art. 44 Abs. 3 E-EHDS.

706 Art. 44 Abs. 3 E-EHDS.

707 Art. 50 Abs. 1 E-EHDS.

6.3.3 Fazit

Der EHDS ist ein entschlossener Vorstoss der EU-Kommission für die Schaffung einer umfassenden Gesundheitsdatenpolitik. Die Ermöglichung weitreichender Zugriffsrechte von Wissenschaftlern und Innovatoren auf (anonymisierte bzw. pseudonymisierte) Gesundheitsdaten – in einem einheitlichen Format und einer entsprechenden Qualität – ist jedenfalls geeignet, die Innovation im Gesundheitssektor zu fördern. Gleichzeitig sollen die Rechte der Betroffenen durch mehr Verfügungsmacht über die eigenen Gesundheitsdaten gestärkt werden. Zusätzlich sollen durch die De-Identifizierung der Daten, eine behördliche Zugriffskontrolle (Genehmigungsverfahren) und entsprechende technische und organisatorische Massnahmen (Secure Processing Environment) die sensitiven Daten der betroffenen Personen geschützt werden.

Zusammenfassend sind die Vorschläge der EU-Kommission grundsätzlich zu begrüssen, obwohl die konkrete Umsetzung sehr aufwändig und bürokratisch organisiert ist. Dies kann zwar mit der Sensitivität der betroffenen Daten begründet werden, jedoch ist fraglich, wie effizient die praktische Umsetzung des EHDS sein wird. Die Festlegung von standardisierten Datenformaten und Qualitätsanforderungen ist besonders hervorzuheben, ist diese doch dringend notwendig, um das Potential von verfügbaren Gesundheitsdaten auszuschöpfen. Schliesslich löst der EDHS die Unklarheiten bei der praktischen Umsetzung der Anonymisierung und Pseudonymisierung zwar nicht auf, jedoch wird durch die behördliche Genehmigung und Kontrolle des Datenzugriffs Rechtsicherheit für den Datennutzer geschaffen.

7. Vorschlag für eine Anpassung der Schweizer Gesetzgebung

Die vorliegende Untersuchung hat veranschaulicht, dass die Schweizer Gesetzgebung zur Sekundärnutzung von Gesundheitsdaten komplex ist. Um das grosse Potential der Sekundärnutzung nutzen zu können, braucht es allerdings möglichst klare rechtliche Rahmenbedingungen für die Involvierten. Dem Gesetzgeber obliegt dabei die schwierige Aufgabe, eine sorgfältige Abwägung zwischen den wirtschaftlichen und gesundheitspolitischen Interessen sowie den Interessen der betroffenen Personen vorzunehmen. Vor diesem Hintergrund ist auch nicht erstaunlich, dass die Regelungen für die Sekundärnutzung eine gewisse Komplexität aufweisen. Der Gesundheitssektor hat bekanntlich auch in Bezug auf andere Aspekte als den Umgang mit Personendaten eine sehr hohe Regelungsdichte. Ebenso wenig ist überraschend, dass hohe Anforderungen an gewisse Sekundärnutzungen gestellt werden, geht es doch regelmässig um die Bearbeitung besonders schützenswerter Daten.

Gleichwohl zeigt die vorliegende Untersuchung, dass die Regelungen sehr oft unnötigerweise, d.h. ohne erkennbaren Nutzen, die Sekundärnutzung von Gesundheitsdaten geradezu behindern. Auf der Basis sämtlicher der Erkenntnisse aus diesem Gutachten erscheinen uns die folgenden Vorschläge am ehesten geeignet, solche Regelungen – unter Berücksichtigung der Entwicklungen auf EU-Ebene – zu beseitigen:

7.1 Vereinheitlichung der anwendbaren Vorschriften

In einem ersten Schritt ist eine Vereinheitlichung der auf die Sekundärnutzung anwendbaren datenschutzrechtlichen Vorschriften angezeigt. Der aktuelle Rechtsrahmen gleicht einem Flickenteppich, der bereits bei der grundlegenden Frage, welchen Regelwerken eine Bearbeitung von Gesundheitsdaten überhaupt untersteht, zu unnötiger Unsicherheit führt.

Es braucht deshalb ein einheitliches Gesetz, das für alle Beteiligten, seien sie kantonale öffentlich-rechtliche Organe, Bundesorgane oder rein privatrechtlich handelnde Rechtseinheiten, gilt. Dabei ist zwar denkbar,

weiterhin gewisse unterschiedliche Vorgaben für die verschiedenen Akteure vorzusehen. In diesem Fall sind diese aber aufeinander abzustimmen. Zwingend zu beseitigen sind aber bspw. Vorschriften, wonach bestimmte kantonale Akteure nicht nur Daten von natürlichen Personen, sondern auch diejenigen von juristischen Personen als Personendaten im Sinne des Datenschutzrechts zu behandeln haben. Solche Sonderwege, wie sie einzelne Kantone auch nach Inkrafttreten des nDSG noch vorsehen werden, gilt es in jedem Fall zu vermeiden. Darüber hinaus müsste auch das Verhältnis zu weiteren Vorschriften ausserhalb eines solchen einheitlichen Erlasses klargestellt werden. Es ist zu vermeiden, dass bei einer Sekundärnutzung die Ungewissheit besteht, ob und inwieweit neben dem (vorgeschlagenen) besonderen Gesetz allgemeinere Vorschriften zusätzlich zur Anwendung kommen.

Eine solche Vereinheitlichung der relevanten Vorschriften ist vor allem deshalb wichtig, weil die Sekundärnutzung von Gesundheitsdaten mehrheitlich unter Beteiligung von Akteuren des Bundes, der Kantone sowie der Privatwirtschaft erfolgt. Da dabei regelmässig auch grenzüberschreitende Kooperationen stattfinden, versteht sich von selbst, dass die Regelungen auch auf die Entwicklungen auf EU-Ebene abzustimmen sind. Es ist jedoch fraglich, inwiefern eine enge Abstimmung mit der EU oder sogar die Schaffung eines gemeinsamen Gesundheitsdatenraumes aufgrund der aktuellen politischen Rahmenbedingungen (Insta-Verhandlungsabbruch) realistisch ist.

7.2 Konkretisierung der Anforderungen an hinreichende Anonymisierung und Klarstellung der datenschutzrechtlichen Verantwortlichkeit

Eine grosse Schwierigkeit, die in der vorliegenden Untersuchung in vielerlei Hinsicht thematisiert wird, sind die Unsicherheiten rund um die Anforderungen an die Anonymisierung von Daten. In vielen Fällen wäre die Anonymisierung das geeignete und einzige Mittel, um die strengen datenschutzrechtlichen Vorgaben und die damit verbundenen Unsicherheiten und Sanktionsrisiken zu vermeiden. Bedauerlicherweise sind die konkreten Anforderungen trotz höchstrichterlicher Leitentscheidungen und vergleichsweise breiter wissenschaftlicher Auseinandersetzungen nach wie vor unklar oder zumindest umstritten. Bereits eine gesetzgeberische Klarstellung, aus welcher Perspektive die Beurteilung vorgenommen werden muss, wäre dabei wertvoll für die Praxis. Mit anderen Worten ist der sogenannte relative Ansatz zu verankern und dabei die Perspektive des datenschutzrechtlich Verantwortlichen für massgeblich zu erklären. Damit verbunden ist zugleich aber auch die wünschenswerte Klarstellung, wer in Bezug auf konkrete Sekundärnutzungen von Gesundheitsdaten als Verantwortlicher zu betrachten ist.

Mit diesen Anpassungen wären bereits wesentliche Ursachen für Unsicherheiten beseitigt. Es bleiben aber nach wie vor Ungewissheiten, da für die Beurteilung der Anonymisierung auf unbestimmte Kriterien, wie den verhältnismässigen Aufwand für die Identifizierung, abgestellt wird. In dieser Hinsicht wäre zu begrüssen, wenn für bestimmte Datensätze konkret definiert wird, welche Attribute zu entfernen sind, damit die Anonymisierung gegeben ist. Alternativ wäre denkbar, zumindest Vermutungstatbestände zu schaffen, also festzulegen, bei der Entfernung welcher Attribute die Anonymisierung vermutet, und damit der Beweis für die fehlende Anonymisierung den betroffenen Personen bzw. Behörden auferlegt wird.

7.3 Festlegung konkreter Erlaubnistatbestände

Neben der Anonymisierung können auch klar festgelegte Erlaubnistatbestände die nötige Absicherung von Sekundärnutzungen bringen. Im Schweizer Datenschutzrecht sind zwar bereits vergleichbare Tatbestände definiert. Bei den Vorgaben für Private handelt es sich dabei um die sogenannten Rechtfertigungsgründe. In Bezug auf die Vorgaben für öffentliche Organe sind es primär besondere gesetzliche Grundlagen, welche eine Ermächtigung zur Vornahme einer Datenbearbeitung enthalten.

Die Untersuchung hat jedoch deutlich gemacht, dass die meisten dieser Erlaubnistatbestände nicht die erforderliche Absicherung bringen. Vielmehr ist eine Datenbearbeitung selbst bei der Einhaltung der darin vorgesehenen Voraussetzungen noch nicht rechtmässig. Dies gilt in besonderem Ausmass für die sog. Forschungsausnahme, welche für die Sekundärnutzung von Gesundheitsdaten eine wichtige Absicherung darstellen könnte. Diese enthält Anforderungen, die unbestimmt sind, wie z.B. das Erfordernis der Anonymisierung, sobald es der Zweck erlaubt. Zudem greift sie aber, selbst wenn man annimmt, dass diese Voraussetzungen erfüllt sind, bspw. bei Privaten, nicht zwingend. Vielmehr kommt eine Rechtfertigung durch die Forschungsausnahme von Gesetzes wegen nur in Betracht und es ist deshalb gleichwohl eine mit weiteren Unsicherheiten verbundene Einzelfallprüfung vorzunehmen. Dies gilt es zu vermeiden.

Förderlich für die Rechtssicherheit wäre in diesem Zusammenhang auch die institutionalisierte Möglichkeit, in bestimmten Fällen die datenschutzrechtliche Genehmigung einer zuständigen Behörde für geplante Sekundärnutzungen einholen zu können. Für dieses behördliche Bewilligungsverfahren müsste die entsprechende gesetzliche Grundlage geschaffen und eine zuständige Behörde bestimmt werden. Um Komplexität abzubauen, wäre jedenfalls ein schweizweit einheitliches Verfahren zu befürworten. Zu diesem Zweck könnte entweder eine neue Behörde geschaffen werden, wie z.B. in Finnland die Findata[708], oder es könnten die Zuständigkeiten von bestehenden Behörden – wie z.B. der Datenschutzbehörden (EDÖB bzw. kantonale Datenschutzbeauftragte) – erweitert werden. Ein naheliegender Ansatz für den praktisch wichtigen Bereich der Sekundärnutzung zu Forschungszwecken im HFG könnte darin bestehen, die Bewilligung durch Ethikkommissionen auf die datenschutzrechtlichen Belange zu erstrecken. In diesem Zusammenhang überlasst es der E-EHDS den EU-Mitgliedsstaaten, eine (oder mehrere) "Zugangsstelle(n) für Gesundheitsdaten" zu benennen.[709] Das Bewilligungsverfahren sollte jedenfalls einfach, effizient und lösungsorientiert ausgestaltet werden, um tatsächlich eine Vereinfachung und nicht eine weitere bürokratische Hürde dazustellen.

In Bezug auf die Regelungen des HFG sind auch die Anforderungen an die informierte Einwilligung zu klären. Namentlich muss eine abschliessende Liste der für eine hinreichende Aufklärung erforderlichen Pflichtangaben definiert werden. Ferner ist das Schriftformerfordernis dahingehend klarzustellen, dass auch digitale Lösungen zur Einholung von Einwilligungen klar erlaubt sind. Schliesslich ist ein einheitliches Formular für den sogenannten Generalkonsent zu erstellen, das von den zuständigen Behörden genehmigt wird und von allen Akteuren rechtssicher verwendet werden kann.

7.4 Massnahmen zur Erleichterung des Datenaustauschs und gemeinsamer Datennutzung

Schliesslich sind neben den bereits genannten Punkten auch weitere Massnahmen zu ergreifen, die den für die Sekundärnutzung von Gesundheitsdaten erforderlichen Datenaustausch erleichtern. Hierzu sind zunächst Klarstellungen in Bezug auf die Regelungen zur Datenbekanntgabe notwendig. Es muss, auf der Basis der Regelungen zur Anonymisierung, klargestellt werden, wann von einer hinreichenden Pseudonymisierung auszugehen ist und dass die Zugänglichmachung von pseudonymisierten Daten keine Bekanntgabe im datenschutzrechtlichen Sinne darstellt. In diesem Zusammenhang gilt es vordringlich auch die Regelungen zur Datenbekanntgabe ins Ausland miteinzubeziehen und klarzustellen. Dabei muss namentlich ein rechtssicherer Einsatz von Diensten von Anbietern mit US-Bezug oder Bezug zu anderen Ländern sowie anderen wirtschaftlich bedeutenden Ländern ohne, aus europäischer Sicht, angemessenes Datenschutzniveau zeitnah ermöglicht werden.

---

[708] Bei dieser handelt es sich um eine eigens für die Genehmigung von Sekundärnutzung zuständige Behörde, welche im Rahmen des "Act on the Secondary Use of Health and Social Data" ins Leben gerufen wurde; vgl. dazu die Website der Behörde: https://findata.fi/en/about-findata/ (zuletzt aufgerufen am 26.07.2022).

[709] Art. 36 Abs. 1 E-EHDS.

Darüber hinaus muss der künftige rechtliche Rahmen auch den sog. FAIR-Grundsatz sicherstellen: Gesundheitsdaten müssen auffindbar, zugänglich, interoperabel und wiederverwendbar sein (FAIR: Findable, Accessible, Interoperable and Reusable).[710] Die Erfahrungen im Bereich des elektronischen Patientendossiers sowie dem Austausch von Daten im Rahmen der Pandemiebekämpfung haben in diesem Zusammenhang sehr grosse Defizite aufzeigt, welche, wie die vorliegende Untersuchung verdeutlicht hat, bis zu einem gewissen Grad auch auf Mängel in den rechtlichen Vorgaben zurückzuführen sind. Namentlich braucht es eine deutliche Verbreiterung der Einsatzfähigkeit des elektronischen Patientendossiers und eine Interoperabilität zwischen den verschiedenen Infrastrukturen und IT-Systemen der Institutionen des Gesundheitswesens.

***

Zürich, 26. Juli 2022

Lukas Bühlmann, LLM.

Dr. Ursula Widmer

[710] Vgl. dazu z.B. WILKINSON/DUMONTIER/AALBERSBERG, The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018 (2016); https://doi.org/10.1038/sdata.2016.18; FAIR Principles GO FAIR, https://www.go-fair.org/fair-principles/ (zuletzt aufgerufen am 12.07.2022).