Klinische Register im 21. Jahrhundert

Ein Spagat zwischen Datenschutz und Machbarkeit?

C.-A. Behrendt, H. Pridöhl, K. Schaar, H. Federrath, E. S. Debus

erschienen in: Chirurg 88/11 (2017) 944-949

https://doi.org/10.1007/s00104-017-0542-9

Zusammenfassung

Verschiedene Formen von Registern gewinnen als eine Form der Big-Data-Anwendung in der Medizin in den letzten Jahren zunehmend an Bedeutung. Unter anderem aufgrund dieser Veränderungen, insbesondere im Bereich der digitalen Datenverarbeitung, findet bereits seit mehreren Jahren ein Reformprozess des EU-Datenschutzes

statt. Nach einer Übergangsfrist wird eine neue Datenschutzgrundverordnung in der Europäischen Union am 25.05.2018 in Kraft treten und dann das noch bestehende Bundesdatenschutzgesetz ablösen. Eine gewissenhafte Beschäftigung mit dem Thema Datenschutz und die konsequente Einhaltung der gesetzlichen Rahmenbedingungen stellen eine obligatorische Voraussetzung

für die erfolgreiche Durchführung von Registerprojekten in der medizinischen Forschung dar. Der technische Fortschritt und die zunehmende Menge an digital gespeicherten Daten machen belastbare technische Datenschutzlösungen erforderlich, um die Patientenrechte zu wahren. Dieser Artikel gibt einen Überblick über die Hintergründe, Entwicklungen und damit verbundene Maßnahmen im Zusammenhang mit medizinischen Registerprojekten.

Einleitung und Hintergrund

Die globale Vernetzung und moderne Computertechnik ist heute aus der medizinischen Versorgung und Forschung nicht mehr wegzudenken. Haben vor 20 Jahren noch ganze Gebäude den Aktenbestand einer mittelgroßen Klinik beherbergt, geht der Trend heute eindeutig zu einer vollständigen Digitalisierung der Behandlungs- und Abrechnungsdaten.

Auch auf dem Gebiet der Qualitätssicherung und Versorgungsforschung hat man sich dies zunutze gemacht und die papierbasierte Datenspeicherung gegen digitale Pendants ausgetauscht. „Big Data“ ist mittlerweile ein (uneinheitlich) definiertes Schlagwort für die rasante Entwicklung großer Datenmengen. Besonders groß sind die Daten im Hinblick auf die Menge („volume“), die Varianz unterschiedlicher Formate und Quellen („variety“), die Geschwindigkeit, mit der sie erzeugt werden können („velocity“), und ihre Unterschiedlichkeit und kontextuelle Qualität, da sie aus unterschiedlichen Quellen stammen („variability“; [1,2]). Daraus folgt eine besondere Herausforderung für ihre Verarbeitung, Speicherung und Analyse und insbesondere auch für Konzepte zur Anonymisierung.

Verschiedene Formen von Registern gewinnen dabei als eine Form der Big-Data-Anwendung in den letzten Jahren zunehmend an Bedeutung [3]. Im Unterschied zu den randomisierten klinischen Studien („randomized controlled trial“, RCT), die zweckgemäß nur eine zuvor exakt definierte Patientenkohorte einschließen können und damit nicht ohne weiteres für die Qualitätssicherung und Versorgungsforschung geeignet sind, ermöglichen entsprechende Registerprojekte die Abbildung einer möglichst großen Population und damit eine Annäherung an die inhomogene Versorgungsrealität. Bei der Planung eines Registers stellen sich grundsätzliche Fragen auch zur Datenverarbeitung und zum Datenschutz. Heute stehen auf dem Markt zahlreiche Lösungen zur Verfügung, die den Aufbau eines Registers und die Datenerhebung auch für Personen ohne entsprechende Fachkenntnisse der Informationstechnologie oder Softwareentwicklung ermöglichen. Mit diesen und weiteren

sog. „Cloud-basierten“ Lösungen (z. B. Surveymonkey [Surveymonkey Inc, San Mateo, CA, USA] oder iFormBuilder [Zerion Software Inc, Herndon, VA, USA]) lassen sich, ohne relevanten Programmieraufwand, umfassende Formulare nach dem WYSIWYG-Prinzip erstellen und hierüber Daten sammeln.

Neben den möglichen Vorteilen ist jedoch zu bedenken, dass das nötige Datenschutzniveau bzw. die Datenschutzfunktionalität für die Verarbeitung medizinischer Daten nicht erreicht wird. So hat z. B. die Datenübermittlung an ausländische Serverstandorte (z. B. USA oder Indien) eine besondere Relevanz für die Datenschutzansprüche und Persönlichkeitsrechte der betroffenen Patienten. Eine übergeordnete Bedeutung hat in diesem Kontext der juristische Rahmen, der die Datensammlung und Verarbeitung innerhalb deutscher und europäischer Grenzen regelt. Auf Europaebene findet gegenwärtig eine notwendige Überarbeitung des EU-Datenschutzrechts statt, die den geänderten Anforderungen gerecht werden soll. Dieser Übersichtsartikel beschäftigt sich mit den Auswirkungen der EU-Datenschutzreform auf medizinische Registerprojekte in Deutschland.

Datenschutz in Deutschland und Europa

In der Bundesrepublik Deutschland stellt bisher unter anderem das Bundesdatenschutzgesetz (BDSG) die nationale Umsetzung der europäischen EU-Datenschutzrichtlinie 95/46/EG und des EU-Rahmenbeschlusses 2008/977/JI dar. Darüber hinaus regeln zahlreiche Datenschutzbestimmungen in den Landesdatenschutzgesetzen sowie in Fachgesetzen den Umgang mit schutzbedürftigen Daten in Deutschland. Ergänzend können Ländergesetzgebungen (z. B. Hamburgisches Krankenhausgesetz, HmbKHG) oder das Berufsrecht (z. B. (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, MBO-Ä) die Thematik substanziell tangieren. Unter anderem aufgrund der Veränderungen, insbesondere im Bereich der digitalen Datenverarbeitung, findet bereits seit mehreren Jahren ein Reformprozess des EU-Datenschutzes statt.

Am 25.05.2016 wurde auf europäischer Ebene die seit 2012 diskutierte Reform des europäischen Datenschutzrechts mit der Verabschiedung der Europäischen Datenschutz-Grundverordnung (DS-GVO; [4]) abgeschlossen. In 99 Artikeln und 173 zusätzlichen Erwägungsgründen soll das europäische Datenschutzrecht harmonisiert werden. Anders als die Richtlinie gilt die Verordnung unmittelbar in allen 28 Mitgliedsstaaten. Das heißt, mit ihr gibt es laut dem Vertrag über die Arbeitsweise der EU (AEUV) keine nationalstaatliche Gesetzgebung mehr (Anwendungsvorrang der Grundverordnung, Art. 288 Abs. 2). Die Mitgliedsstaaten haben jedoch die Möglichkeit, nationale Spezifizierungen für ausgewiesene Bereiche für die sog. Öffnungsklauseln vorzunehmen. Für Deutschland wurden diese Anpassungen bereits durch die am 30.06.2017 erfolgte Verabschiedung des Datenschutz Anpassungs- und Umsetzungsgesetzes (DSAnpUG/BDSG-neu; [5]) vorgenommen. Nach einer zweijährigen Übergangsfrist wird dieses Gesetz als Ergänzung der DS-GVO am 25.05.2018 in Kraft treten und dann das noch bestehende BDSG ablösen. Ab diesem Zeitpunkt ist die neue Datenschutzgesetzgebung durch die zuständigen Datenschutzaufsichtsbehörden und Gerichte überprüfbar. Während dieser Übergangsfrist ist es erforderlich, die bisherigen Dokumentationen, Datenschutzerklärungen sowie -prozesse, die Umsetzung von Widerspruchserklärungen und die Verfahren zur Risikobewertung in diesem Zeitraum anzupassen.

Die DS-GVO ist grundsätzlich im öffentlichen sowie im nichtöffentlichen Bereich anwendbar. Sie macht dabei nicht nur Vorgaben, die rein europäische Projekte betreffen, sondern regelt auch Fragen, die den außereuropäischen Rechtsraum tangieren. Kernaspekt der internationalen Diskussionen ist dabei auch die grenzüberschreitende Weitergabe und Verarbeitung der Daten. Sofern Daten an ein Drittland außerhalb der Europäischen Union oder eine internationale Organisation übermittelt werden, muss der Verantwortliche oder ein Auftragsverarbeiter dabei sicherstellen, dass dort geeignete Garantien für die Rechte betroffener Personen gegeben sind (vgl. Artikel 44, 45, 46 DS-GVO) und ein vergleichbares Schutzniveau garantiert werden kann (DS-GVO Erwägungsgrund 101).

Die Kommission kann hierbei bestimmte Länder definieren, in denen von einem vergleichbaren Datenschutzstandard ausgegangen werden kann (DS-GVO Erwägungsgrund 103).

Safe-Harbour-Urteil und das Privacy-Shield-Übereinkommen

In einem weitreichenden Urteil des Europäischen Gerichtshofs (EuGH) vom 06.10.2015 wurde die als „Safe-Harbor“ bezeichnete Entscheidung der Europäischen Kommission, die lange Zeit den Rechtsrahmen für die Übermittlung personenbezogener Daten in die USA darstellte, für ungültig erklärt. Um weiterhin rechtmäßig Daten übermitteln zu können, hat die EU-Kommission mit den USA ein neues Übereinkommen verhandelt, das sog. „Privacy Shield“. Dieses beinhaltet strengere Datenschutzregelungen und räumt EU-Bürgern erstmals Ansprüche gegen US-Unternehmen ein. Es umfasst allerdings nicht allgemein den Datenverkehr in die USA, sondern beschränkt sich auf gelistete Firmen bzw. Organisationen, die definierte Datenschutzanforderungen erfüllen [6].

Kritiker bemängeln jedoch, dass auch das Privacy-Shield-Übereinkommen nicht dem Datenschutzniveau der EU entspreche [7]. Hinsichtlich des Datenaustauschs in der transnationalen Medizin, z. B. durch die Nutzung von Cloud-Diensten unter dem Privacy Shield, kommt eine Prüfung der im Privacy Shield gegebenen Gewährleistungen zu dem Schluss, dass ein angemessenes und vergleichbares Schutzniveau für die Rechte von Betroffenen bislang nicht besteht [8].

Wichtige Neuerungen der DS-GVO

Während zahlreiche Regelungen der DS-GVO bereits durch das BDSG in seiner alten Fassung hinreichend geregelt wurden, wird es auch Änderungen mit Relevanz für die Forschung geben [9]. So ist durch die Erhöhung der möglichen Bußgelder auf bis zu 20 Mio. EUR bzw. bis zu 4 % des globalen Jahresumsatzes von Unternehmen das Risiko für die Verantwortlichen signifikant erhöht worden (Art 83 Abs. 4 und 5). Auch bei der Festlegung der Zuständigkeiten und Verantwortlichkeiten finden sich relevante Neuerungen: So sind die Aufgaben und Zuständigkeiten der bestellten Datenschutzbeauftragten von Forschungseinrichtungen umfassend erweitert worden, was eine frühere und konsequentere Einbindung dieser Stellen bereits bei der Planung bzw. bei der Beantragung von Forschungsprojekten erforderlich machen könnte (Art. 37 und Art. 39 DS-GVO). Weitere Neuerungen betreffen primär die Patientenrechte. Während die Regelungen zur informierten Patienteneinwilligung, bis auf den stärkeren Schutz Minderjähriger unter 16 Jahren, weitestgehend gleichgeblieben sind, regeln die Artikel 12 und 13 der DS-GVO beispielsweise die faire und transparente Verarbeitung der Daten.

Unter Art. 35 der DS-GVO wird außerdem ein wichtiges neues Instrument des Datenschutzes beschrieben: die Datenschutz-Folgenabschätzung (DSFA; [10]). Diese entspricht im Wesentlichen der bereits bekannten Prüfung vor Beginn der Verarbeitung (Vorabkontrolle) in § 4 Abs. 5 des BDSG und entspricht somit letztlich einer Prüfung und Risikoabschätzung von Datenverarbeitungsvorgängen durch den für die Datenverarbeitung Verantwortlichen. Durchzuführen ist eine DSFA nach der DS-GVO immer dann, wenn die Verarbeitung der Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge hat. Dies gilt nach Art. 35 Abs. 1 insbesondere auch bei der Verwendung neuer Technologien sowie immer bei der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (DS-GVO Art. 35 Abs. 2 lit. b), zu denen beispielsweise auch Gesundheitsdaten oder genetische Daten zählen (DS-GVO Art. 9 Abs. 1). Nach den Mindestanforderungen der DS-GVO (Art. 35 Abs. 7) muss die DSFA zu den geplanten Datenverarbeitungsvorgängen mindestens eine systematische Beschreibung und den Zweck der Verarbeitung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit, eine Risikobewertung für die Rechte und Freiheiten der Betroffenen sowie die geplanten Abhilfemaßnahmen einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren beinhalten. Für mehrere Verarbeitungsvorgänge

mit ähnlich hohem Risiko kann dabei eine einzige Abschätzung vorgenommen werden (DS-GVO Art. 35 Abs. 1 und DSAnpUG/BDSG-neu § 67, Abs. 2).

Für die Forschung sieht die DS-GVO unter bestimmten Bedingungen Ausnahmen vor, z. B. für Betroffenenrechte (DS-GO Art. 89). Weitere Ausnahmen betreffen die Zweckbindung und eine längere Speicherdauer (DS-GVO Art. 5 Abs. 1 lit b, e) sowie Informationspflichten (Art. 14 Abs. 5 lit b) im Rahmen der Weiterverarbeitung von Forschungsdaten.

Die Verarbeitung personenbezogener Daten in Registern wird in der DS-GVO positiv hervorgehoben, denn „... durch die Verknüpfung von Informationen aus Registern können Forscher neue Erkenntnisse von großem Wert in Bezug auf weit verbreitete Krankheiten wie Herz-Kreislauf-Erkrankungen, Krebs und Depression erhalten. Durch die Verwendung von Registern können bessere Forschungsergebnisse erzielt werden, da sie auf einen größeren Bevölkerungsanteil gestützt sind." (DS-GVO Erwägungsgrund 157)

Voraussetzung hierfür ist jedoch, dass Garantien für die Rechte und Freiheiten betroffener Personen vorhanden sind (DS-GVO Erwägungsgrund 157 und Art. 9 Abs. 2 lit. j) und – insbesondere bei der Verarbeitung von Gesundheitsdaten – die betroffenen Personen ihre informierte Einwilligung in die Verarbeitung gegeben haben (DS-GVO Art. 9 Abs. 2 lit.a). Die Mitgliedsstaaten der Europäischen Union können jedoch für wissenschaftliche Zwecke hier Ausnahmen vorsehen, sofern die Grundrechte und Interessen der betroffenen Person gewahrt bleiben (DS-GVO Art. 9 Abs. 2 lit. j).

Das DSAnpUG/BDSG-neu macht von dieser Möglichkeit Gebrauch und sieht eine Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Zwecken auch ohne Einwilligung vor, wenn sie erforderlich ist und die Interessen des Verantwortlichen die Interessen der betroffenen Person erheblich überwiegen (DSAnpUG/BDSG-neu § 27 Abs. 1). Bereits jetzt werden hierfür Verfahren vorgeschlagen, die eine Prüfung der Interessenabwägung zwischen den Betroffenen und einem zulässigen Forschungsinteresse vorsehen. So ist eine Prüfung durch Ethikkommissionen und das Vorliegen strenger technischer und organisatorischer Maßnahmen [11] ebenso im Gespräch, wie die Etablierung eines unabhängigen bundesweit zuständigen Gremiums, bei dem Projekte, die Daten ohne die Einwilligung von Betroffenen verarbeiten, gemeldet werden und geprüft werden können [12]. Gegen das DSAnpUG/BDSG-neu wird allerdings Kritik vorgebracht, da die Einschränkung von Betroffenenrechten als zu weitreichend und nicht europarechtskonform eingeschätzt wird. Insofern besteht in diesem Bereich – auch für die Weiterverarbeitung von Gesundheitsdaten in Registern – weiterhin Rechtsunsicherheit.

Begrifflichkeiten

Die Begrifflichkeiten der alten und neuen Gesetzgebungen stellen mitunter eine Herausforderung für Nicht-Juristen dar. In der DS-GVO werden alle Informationen als besonders schutzbedürftige „personenbezogene Daten" definiert, die sich auf eine identifizierte oder identifizierbare natürliche (nicht juristische) Person beziehen. Nach dem Erwägungsgrund 26 sollten dabei alle Daten als personenbeziehbar betrachtet werden, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten.

Außerdem wurde auch die bisherige (96/46/EG Artikel 2) begriffliche Trennung in anonymisierte vs. pseudonymisierte Daten verlassen. So wird die „Pseudonymisierung" sinngemäß als Verarbeitung personenbezogener Daten in einer Weise bezeichnet, dass die Zuordnung zu einer spezifischen identifizierten oder identifizierbaren natürlichen Person – ohne Hinzuziehung zusätzlicher Informationen – nicht mehr möglich ist. Die entsprechenden zusätzlichen Informationen sind zudem gesondert aufzubewahren.

Begriffsbestimmungen zur „Anonymisierung" sind dagegen nicht mehr explizit enthalten. Werden die Daten derart verändert, dass die Personenbezogenheit nicht mehr oder nur noch mit einem unverhältnismäßig großen Aufwand hergestellt werden kann, sprach der Gesetzgeber dagegen

bisher von einer Anonymisierung. Angaben zur Körpergröße, zu Geschlecht und Augenfarbe ließen demnach ohne weitere Angaben keinen direkten Personenbezug zu. In der neuen DS-GVO gelten diese Daten grundsätzlich als personenbeziehbar und damit schutzbedürftig. Als Maß für die Anonymisierung gilt dabei im technischen Kontext die sog. k-Anonymität (Sweeney et al. [13]), die weiter unten erläutert wird.

Die drei in diesem Abschnitt beschriebenen Begriffe (Anonymisierung, Pseudonymisierung, k-Anonymität) werden nicht selten kontrovers diskutiert, da die Möglichkeit der Reidentifizierung grundsätzlich von verschiedenen externen Faktoren abhängen kann und sich im Laufe der Zeit auch ändern kann (z. B. durch Anhäufung und Verknüpfung neuer Datenbanken). Die DS-GVO sieht zudem nach Artikel 9 eine besonders strenge Regelung für die Verarbeitung „besonders sensibler Daten“ vor. Hierunter fallen neben genetischen und biometrischen Daten zur eindeutigen Identifizierung auch Daten über die Gesundheit. Die explizite Erwähnung genetischer Daten ist dabei eine Neuheit gegenüber dem BDSG.

Anonymisierung von Patientendaten

Zur Anonymisierung von Patientendaten stehen verschiedenen Methoden zur Verfügung. Deren Anwendbarkeit hängt jedoch stark von den zugrunde liegenden Daten sowie von der Verarbeitung dieser Daten ab. Folglich definiert der Gesetzgeber auch nicht, wie Daten zu anonymisieren sind, sondern beschreibt unbestimmt, wann sie als anonymisiert gelten.

Das Entfernen der unmittelbar personenidentifizierenden Daten (z. B. Name, Anschrift) ist dabei in der Regel nicht ausreichend, wie das folgende Beispiel [13] zeigt: In Massachusetts (USA) ist die Group Insurance Commission (GIC) für die Krankenversicherung von Staatsbediensteten zuständig. Die GIC sammelte die Gesundheitsdaten von 135.000 Staatsbediensteten sowie ihrer Familien. Zusätzlich wurden Postleitzahl, Geburtsdatum und Geschlecht erfasst. Die Daten wurden durch das Entfernen des Namens und der Anschrift „anonymisiert“ und an Forscher weitergegeben. Es erfolgte außerdem ein Verkauf der Daten an die Industrie. Durch Kombination mit den für 20 US-Dollar zu erwerbenden Wählerverzeichnissen, die neben dem Namen auch Postleitzahl, Geburtsdatum und Geschlecht enthalten, gelang es Sweeney, den Gouverneur von Massachusetts, William Weld, in den „anonymisierten“ Datensätzen zu reidentifizieren.

Dies brachte Sweeney zur Definition der k-Anonymität, die heute als ein verbreitetes Maß für die Anonymität eines Datensatzes gilt. Die k-Anonymität stellt sicher, dass beim Hinzuziehen externer Informationen, beispielsweise aus den Wählerverzeichnissen, immer mindestens k-Personen nicht zu unterscheiden sind und somit keine eindeutige Reidentifizierung stattfinden kann. Um k-Anonymität zu erreichen, können Einträge hinzugefügt bzw. entfernt werden oder Attribute weggelassen oder vergröbert werden, also z. B. die Postleitzahl entfernt und das Geburtsdatum zum Geburtsjahr reduziert (aggregiert) werden.

Die k-Anonymität weist jedoch Schwächen auf, wie ein Beispiel illustriert: In einem Register sind Patienten mit Ortsangabe, Geburtsdatum und Diagnose gespeichert. Alle 10 Patienten aus Hamburg leiden unter Herzrhythmusstörungen. Ist nun bekannt, dass eine bestimmte Person aus Hamburg am Register teilnimmt, kann inferiert werden, dass diese unter Herzrhythmusstörungen leidet – es wurde ein sog. Homogenitätsangriff durchgeführt. Die Bedingung der k-Anonymität ist nicht verletzt, da nicht bekannt ist, welcher der 10 Hamburger in dem Register die bestimmte Person darstellt. Die k-Anonymität kann noch erweitert werden, beispielsweise um l-Diversity, die den Homogenitätsangriff verhindert oder um t-Closeness, die noch die statistische Verteilung von Werten betrachtet.

Die vorgenannten Beispiele zeigen deutlich, dass wenn Daten eines Registers anonymisiert werden sollen, immer der zugrunde liegende Datensatz zu betrachten und eine geeignete Methode zu wählen ist. Dies kann vom einfachen Vergröbern von Werten bis hin zu Verfahren aktueller Forschung, beispielsweise epsilon-Differential-Privacy, gehen. Allerdings gehen die vorgenannten Konzepte von

einer statischen Datenmenge aus. Big-Data-Datenbanken wachsen jedoch stetig an, Datensätze zu einzelnen Individuen können erweitert und neue Auswertungsverfahren angewandt werden. Insofern ist zu empfehlen, die angewandten Anonymisierungsverfahren regelmäßig auf ihre Wirksamkeit und Angemessenheit hin zu überprüfen [1].

Technische Lösungen des Datenschutzes in Registern

Um Datenschutz und die dafür benötigte IT-Sicherheit in Registern zu gewährleisten, bedarf es speziell darauf ausgelegte Softwarelösungen. Da bei einem Register unterschiedliche Personen mit unterschiedlichen Rollen auf die Daten zugreifen und diese verarbeiten, ist ein umfangreiches Rechtemanagement erforderlich, das den Zugriff auf die für die Rolle benötigten Daten bzw. Arten der Verarbeitung einschränkt.

Um die im Register gespeicherten Daten vor einem Angreifer zusätzlich zu sichern, werden diese verschlüsselt. Verschlüsseln bezeichnet in diesem Kontext die Unkenntlichmachung von Daten mithilfe eines Schlüssels. Nur wer den Schlüssel besitzt, kann die Daten wieder in eine lesbare Form bringen. Dabei treten verschiedene Probleme auf: Der Schlüssel darf nicht zusammen mit den Daten aufbewahrt werden, da ein Angreifer, der Zugriff auf die Daten bekommt, automatisch auch Zugriff auf den Schlüssel hat und damit die Daten entschlüsseln kann. Das Ausführen von Berechnungen oder das Durchsuchen verschlüsselter Daten ist ein aktuelles Forschungsgebiet der Kryptografie, daher stehen nur sehr eingeschränkt effiziente Lösungen zu Verfügung, die nicht erst alle Daten entschlüsseln müssen. Mit Inkrafttreten der DS-GVO und des daraus resultierenden neuen BDSG wird das Verschlüsseln bei personenbezogenen Daten besonderer Art, zu denen medizinische Daten gehören, Pflicht.

Tragen mehrere Institutionen Daten zum Register bei, sollte eine entsprechende technische Lösung sicherstellen, dass diese getrennt voneinander verarbeitet und gespeichert werden können und nur bei Bedarf zusammengeführt werden. Dies stellt sicher, dass bei einem erfolgreichen Angriff auf eine Institution nur ein Teil der Registerdaten betroffen ist und nicht das gesamte Register. Moderne Betriebssysteme und Datenbankmanagementsysteme stellen hier verschiedene Isolationsmechanismen bereit, die von einer Registersoftware genutzt werden kann.

Zum Datenschutz gehört auch, kontrollieren zu können, wer welche Daten in welcher Form hinzugefügt, bearbeitet, gelöscht – oder kurz: verarbeitet hat. Dazu müssen die Benutzeraktionen protokolliert werden und das Protokoll revisionssicher sein. Revisionssicherheit bedeutet, dass sichergestellt ist, dass die Protokolldateien nicht manipuliert wurden. Dies kann z. B. durch einen Zeitstempelserver erfolgen, der einen Beweis ausgibt, dass eine Protokolldatei zu einem bestimmten Zeitpunkt einen bestimmten Inhalt hat, ohne dabei selbst Kenntnis vom Inhalt zu nehmen. Dieser Beweis kann jederzeit überprüft werden.

Es ist ersichtlich, dass generische Softwarelösungen, wie beispielsweise Surveymonkey oder eine Excel-Tabelle [Microsoft Corp., Redmond, WA, USA] auf einem gemeinsamen Speicher, nicht den Anforderungen genügen. Daher sind beim Aufbau eines Registers die Anforderungen sorgfältig zu ermitteln und eine geeignete Registersoftware zu wählen, die diesen genügt.

Zusammenfassung und Ausblick

Eine gewissenhafte Beschäftigung mit dem Thema Datenschutz und die konsequente Einhaltung der gesetzlichen Rahmenbedingungen stellen eine obligatorische Voraussetzung für die erfolgreiche Durchführung von Registerprojekten in der medizinischen Forschung dar. Der technische Fortschritt und die zunehmende Menge an digital gespeicherten Daten machen belastbare technische Datenschutzlösungen erforderlich, um die Patientenrechte zu wahren. Die DS-GVO setzt dabei eine Reihe notwendiger Reformen um, damit die Gesetzgebung an diese Anforderungen angepasst und damit

eine verbindliche Rechtsgrundlage für die Verarbeitung dieser schutzbedürftigen Daten geschaffen wird. Alle zur medizinischen Forschung genutzten Softwarelösungen, auch die sog. Cloud-basierten Alternativen, sollten regelmäßig hinsichtlich ihrer Datenschutzkonformität geprüft werden, um unüberschaubaren haftungsrechtlichen Konsequenzen für die verantwortlichen Forschenden zu entgehen.

Das vom Innovationsfond des Gemeinsamen Bundesausschusses (G-BA) mit insgesamt 3,57 Mio. Euro geförderte multimethodale und mehrstufige IDOMENEO-Projekt (www.idomeneo.de) verfolgt dabei das Ziel, Konzepte und technische Lösungen für eine datenschutzkonforme und datensichere Registerplattform GermanVasc zu entwickeln, die anschließend den Forschenden für eigene Projekte zur Verfügung gestellt werden kann. Während der dreijährigen Förderdauer werden unter anderem 10.000 Patientinnen und Patienten konsekutiv an 40 interdisziplinären Gefäßzentren eingeschlossen und über ein Jahr verlaufskontrolliert, die eine invasive stationäre Behandlung der symptomatischen peripheren arteriellen Verschlusskrankheit (PAVK) erhalten [14].

Literatur

1. Marnau N (2016) Anonymisierung, Pseudonymisierung und Transparenz für Big Data. Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung. Datenschutz Datensicherheit 7:428–433

2. US Department of Commerce (2015) NIST Big Data Interoperability Framework. Volume 1, Definitions: National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf Zugegriffen: 01.06.2017

3. Behrendt CA, Heidemann F, Riess HC, Stoberock K, Debus SE (2017) Registry and health insurance claims data in vascular research and quality improvement. VASA 46(1):11–15

4. Europäisches Parlament, Rat der Europäischen Union (2016) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung. http://eur-lex. europa.eu/legal-content/DE/TXT/?uri=OJ:JOL_2016_119_R_0001 (Erstellt: 4. Mai 2016) (DS-GVO, vom 2016/679, 27.04.2016. In: Amtsblatt der Europäischen Union (OJ L 119), S. 1–88) Zugegriffen: 01.06.2017

5. Bundestag, Bundesrat (2017) Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680. (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU). Artikel 1. Bundesdatenschutzgesetz (BDSG). (DSAnpUG-EU/ BDSG, vom 30.06.2017. In: Bundesgesetzblatt (44), S. 2097–2132.)

6. Privacy Shield Framework (2017) Privacy Shield List. https://www.privacyshield.gov/list Zugegriffen: 21.07.2017

7. Article 29 Data Protection Working Party: Opinion 01/2016 on the EU—U.S. Privacy Shield draft adequacy decision (WP, 238). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion- recommendation/files/2016/wp238_en.pdf Zugegriffen: 01.06.2017

8. Molnár-Gábor F, Kaffenberger L (2017) EU-US-Privacy-Shield – ein Schutzschild mit Löchern. Bedeutung des Austauschs von personenbezogenen Daten in der medizinischen Forschung. Z Datenschutz 1:18–24

9. Schaar K (2016) Was hat die Wissenschaft beim Datenschutz künftig zu beachten? Allgemeine und spezifische Änderungen beim Datenschutz im Wissenschaftsbereich durch die neue Europäische Datenschutzgrundverordnung. Berlin (RatSWD Working Paper, 257). http://www.ratswd.de/dl/RatSWD_WP_257.pdf Zugegriffen: 01.06.2017

10. Schmitz B, von Dall'Armi J (2017) Datenschutzfolgenabschätzung – verstehen und anwenden. Z Datenschutz 2:57–63

11. Pommerening K, Altmann U, Jöckel KH, Kieschke J, Müller TH, Pigeot-Kübler I, Schütze B (2017) Memorandum zum Datenschutz in der medizinischen Forschung aus Anlass der nationalen Umsetzung und Konkretisierung der EU-Datenschutz-Grundverordnung (DS-GVO). http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2017-0235&format=XML&language=EN Zugegriffen: 23.10.2017

12. Krawczak M, Weichert T (2017) Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland (Version 1.3). Manuskript, Kiel

13. Sweeney L (2002) k-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness Knowl Based Syst 10(5):557–570

14. Behrendt CA, Härter M, Kriston L et al (2017) Gefässchirurgie. https://doi.org/10.1007/s00772-016-0234-7 Zugegriffen: 21.07.2017