Positionspapier zur Neugestaltung der datenschutzrechtlichen Regelungen bzgl. der Verarbeitung von personenbezogenen Daten in der Versorgung, Qualitätssicherung und Forschung im Gesundheitswesen

Eine Zusammenarbeit von

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Gesellschaft für Datenschutz und Datensicherheit e. V.

Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Autor(en)

Frank DaPont	B·A·D Gesundheitsvorsorge und Sicherheitstechnik GmbH
Christoph Isele	Cerner Deutschland GmbH
Thomas Jäschke	Datatree AG
Holger Koch	Fachberater für Datenschutz und Datensicherheit
David Koeppe	Vivantes - Netzwerk für Gesundheit GmbH
Pierre Kaufmann	Agfa HealthCare GmbH
Christoph Nahrstedt	MEDNOVO Medical Software Solutions GmbH
Rainer Röhrig	Carl von Ossietzky Universität Oldenburg, Abteilungen im Department für Versorgungsforschung
Ulrich Sax	Universitätsmedizin Göttingen, Abteilung Medizinische Informatik
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Jens Schwanke	Kairos GmbH
Gerald Spyra	Kanzlei Spyra

Stand: 15. August 2016

Inhaltsverzeichnis

Copyright

Zusammenfassung

Die Patientenversorgung erfolgt heute institutions- und bundeslandübergreifend. Daher sollte die durch die Einführung der europäischen Datenschutzgrundverordnung (DS-GVO) zu erfolgende Änderung der Gesundheitsdatenschutzgesetzgebung in Bund und Ländern dazu genutzt werden, diesem Umstand Rechnung zu tragen und die Gesetzgebung bzgl. des Gesundheitsdatenschutzes von Bund und Ländern harmonisieren.

Es ist zwingend notwendig, dass Erlaubnistatbestände zur Datenweitergabe an mitbehandelnde und/oder weiterbehandelnde Personen, die nicht zwangsläufig ärztliche Personen sein müssen, weiterhin gesetzlich geregelt bleiben. Dies schließt die derzeitigen gesetzlichen Regelungen der Sozialgesetzbücher ein, insbesondere auch die Regelungen bzgl. des MDK. Es ist wünschenswert, dass diese Erlaubnistatbestände nicht zwingend die Einwilligung des Patienten erfordern, wenngleich selbstverständlich die Transparenz gegenüber dem Patienten gewährleistet sein muss.

Die medizinische Forschung wird in der DS-GVO nur am Rande betrachtet. Vielmehr überlässt man die gesetzliche Ausgestaltung dieses Themas dem nationalen Gesetzgeber. Damit der medizinische Forschungsstandort Deutschland nicht den Anschluss an die internationale medizinische Forschung verliert, benötigt Deutschland klare Regeln bzgl. des Umgangs mit Daten der besonderen Kategorien zu Forschungszwecken. Insbesondere werden gesetzliche Erlaubnistatbestände bzgl. des Umgangs mit Biomaterial benötigt, aber auch Regelungen für einrichtungsübergreifende Forschung und Qualitätssicherung mit den Daten der Patientenversorgung.

Neben der Forschung ist die Qualitätssicherung der medizinischen Versorgung unabdingbar. Auch hier müssen mindestens die aktuellen Regelungen beibehalten werden, welche die Nutzung von Daten der Routineversorgung zu Zwecken der Qualitätssicherung erlauben. Nicht staatlich geforderte Register sind für die Weiterentwicklung der Versorgung unverzichtbar, diese brauchen gesetzliche Erlaubnistatbestände.

In der heutigen Zeit ist die elektronische Datenverarbeitung derart komplex geworden, dass innerhalb einer verantwortlichen Stelle - wie einem Krankenhaus oder einer Arztpraxis - das dort beschäftigte Personal ohne externe Unterstützung die EDV-Prozesse nicht managen kann. Die Gesetzgebung sollte dem Rechnung tragen und ermöglichen, dass Daten außerhalb eines Krankenhauses verarbeitet werden dürfen und den Daten dort derselbe gesetzliche Schutz wie in der versorgenden Einheit gewährt wird.

Hinsichtlich der Bestellpflicht eines Datenschutzbeauftragten ist es wünschenswert, dass einerseits die bestehenden Regelungen in Deutschland beibehalten werden. Die Betroffenenrechte sind in der DS-GVO sehr umfangreich ausgestaltet, was angesichts der immer stärkeren digitalen Vernetzung verständlich und begrüßenswert ist. Dennoch sollte der Gesetzgeber einige wenige dieser Rechte (siehe z. B. Kapitel 4.2.2) einschränken, bis nationale Umsetzungsvorgaben (z.B. im Rahmen des Rechts auf Datenübertragbarkeit) eine nutzbare Gestaltung dieser Betroffenenrechte erlauben.

Art. 9 Abs. 3 DS-GVO fordert eine Geheimhaltungspflicht für Personen, welche besondere Kategorien personenbezogener Daten gemäß Art. 9. Abs. 2 lit. h DS-GVO verarbeiten. In verschiedenen juristischen Kommentaren werden verschiedene Kategorien von Personen[1] genannt, die nicht unter den

[1] Z.B. beschränkt sich im Krankenhaus nach Cierniak/Pohlit, Münchener Kommentar zum StGB, Bd. 4, 2. Auflage 2012, § 203 Rn. 122 der Kreis der ärztlichen Gehilfen auf die für das Behandlungsgeschehen sowie dessen Abrechnung und Kontrolle zuständigen Personen, hingegen gehören Verwaltungsbedienstete und Verwaltungsleiter danach nicht zum Kreis der ärztlichen Gehilfen

Schutzbereich des § 203 StGB fallen, sodass hier eine Regelung analog § 17 UWG oder eine Änderung des §203 StGB selbst zur Herstellung einer Rechtssicherheit wünschenswert erscheint.

1. Einführung

Die europäische Datenschutz-Grundverordnung (DS-GVO) wurde am 14. April vom europäischen Parlament verabschiedet, am 4. Mai 2016 im Amtsblatt der Europäischen Union[2] veröffentlicht und wird ab dem 25. Mai 2018 in ganz Europa direkt gelten und gleichgeregeltes deutsches Recht ersetzen; es gilt der Grundsatz des Anwendungsvorrangs des EU-Rechts. Dies wird dazu führen, dass nahezu alle deutschen Datenschutzregeln angepasst werden müssen; auch und gerade die datenschutzrechtlichen Regelungen bzgl. der Verarbeitung von Gesundheitsdaten. Dies sollte als Chance aufgefasst werden, die derzeit bestehende Vielzahl an landesspezifischen Regelungen zu harmonisieren.

Im Folgenden wird in aller Kürze dargelegt, welche nationalen Regelungen aus Sicht einer bestmöglich unterstützten Patientenversorgung notwendig erscheinen. Dies beinhaltet u.a. die Lehre und Forschung, Qualitätssicherung und Fort- und Weiterentwicklung von medizinischen Produkten ohne die eine Weiterentwicklung und stetige Optimierung der Patientenversorgung nicht möglich ist.

2. Vereinheitlichung der datenschutzrechtlichen Regelungen

Gerade unter dem Gesichtspunkt, dass die Versorgung von Patienten heute nicht mehr ausschließlich von einer Institution - sei es Arztpraxis oder Krankenhaus - gewährleistet werden kann, ist eine institutions- und bundeslandübergreifende Versorgung heute nicht mehr die Ausnahme. Ein Austausch zur Versorgung zwingend benötigter Patientendaten bedarf daher datenschutzrechtlicher Regelungen, welche diesen Umstand berücksichtigen.

Die DS-GVO sieht an einer ganzen Reihe zentraler Regelungspunkte die Möglichkeit vor, durch nationale Gesetzgebung den nationalen Besonderheiten bei der Verarbeitung personenbezogener Daten Rechnung zu tragen. Somit bietet die europäische Datenschutz-Grundverordnung (DS-GVO) Deutschland die Chance, die entsprechenden datenschutzrechtlichen Regelungen zu modernisieren und eine Abstimmung zwischen den einzelnen Bundesländern vorausgesetzt, zu harmonisieren.

Wegen der im Grundgesetz existierenden Gesetzgebungskompetenz ist im Bereich des Gesundheitswesens eine länderspezifische Gesetzgebung nicht zu umgehen. Wünschenswert wäre daher, wenn der Bundesgesetzgeber in Einvernehmen mit den Landesgesetzgebern eine Rahmengesetzgebung bzgl. des Gesundheitsdatenschutzes erlässt, an welcher sich die jeweiligen Landesgesetzgeber orientieren.

3. Rechtssicherheit bzgl. Gesetzgebung in den Mitgliedstaaten

An vielen Punkten der DS-GVO heißt es „Unionsrechts oder des Rechts eines Mitgliedstaats“, ohne dass zum Ausdruck gebracht wird, dass damit der für den Verantwortlichen zuständige Mitgliedstaat gemeint ist.

Letztlich führt dies dazu, dass jede Versorgungseinheit in Deutschland, wie beispielsweise eine Arztpraxis oder ein Krankenhaus in der ein Patient behandelt wird, die jeweilige für den Patienten geltende nationale Gesetzgebung seines Mitgliedstaates berücksichtigen muss, wenn die

[2] Amtsblatt der Europäischen Union. Online, zitiert am 2016-05-24]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1462345886854&uri=OJ:JOL_2016_119_R_0001

Versorgungseinheit aus diesem Land Anfragen wie beispielsweise die Übermittlung von Daten an ein nationales Krankheitsregister erhält. Denn ggfs. ist in diesem Mitgliedstaat eine (bußgeld- oder strafbewehrte) Pflicht verankert, dass bei der Behandlung Patientendaten an eine staatliche Stelle in dem betroffenen Mitgliedstaat übermittelt werden müssen.

Es ist den Leistungserbringern in Deutschland nicht zumutbar, in allen europäischen Ländern die Gesetzgebung zu verfolgen. Daher muss für Deutschland geregelt werden, ob nationale Regelungen aus den europäischen Mitgliedsländern von den versorgenden Stellen zu beachten sind. Hier wäre die Schaffung einer zentralen Informationsstelle wünschenswert, ähnlich wie sie das DIMDI in Bezug auf Medizinprodukte darstellt.

4. Erforderliche nationale Regelungen

4.1. Bestellung eines Datenschutzbeauftragten

Die in Deutschland bestehenden Regelungen zur Bestellung eines betrieblichen und behördlichen Datenschutzbeauftragten haben sich bewährt und sollten beibehalten werden, eine dem heutigen §4f Abs. 1 BDSG entsprechende nationale Regelung gemäß Art. 37 Abs. 4 DS-GVO ist daher zu begrüßen.

4.2. Beschränkung der Rechte von Patienten

Entsprechend Art. 23 Abs. 1 lit. e DS-GVO können die Betroffenenrechte von Art. 12 bis 22 beschränkt werden, sofern eine solche Beschränkung eine „notwendige und verhältnismäßige Maßnahme“ darstellt, welche

a) den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und
b) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit dient.

Grundsätzlich ist die Beschränkung der Grundrechte Betroffener nicht wünschenswert und sollte daher in nationalen Regelungen nur maßvoll Anwendung finden.

4.2.1. Beschränkung des Informationsrechts des Patienten

Ein Export aller Daten in elektronischer Form für Zwecke des Betroffenen ist zu gewährleisten. Dies beruht auf den gesetzlichen Regelungen in § 630 g Abs. 2 BGB. Demgegenüber können die aus der DS-GVO geltenden Rechte beschränkt werden.

Patienten, die an klinischen Forschungen z.B. im Rahmen einer Arzneimittelstudie teilnehmen, sollte das Recht auf Einsichtnahme gemäß Art. 15 Abs. 1 DS-GVO in Informationen, deren Preisgabe das Forschungsergebnis beeinflussen oder das Erreichen des Forschungszieles verhindern, bis zur Beendigung der Forschung beschränkt werden, sodass dieses Recht nur aus wichtigen Gründen (z.B. Verdacht auf Beeinträchtigung der eigenen Gesundheit durch die Forschung) wahrgenommen werden kann. Die Information, in welcher Gruppe ein Patient im Rahmen einer Doppelblindstudie teilnimmt, kann im schlimmsten Fall die Aussagekraft der gesamte Studie beeinträchtigen, sodass in derartigen Fällen eine Interessensabwägung (analog Art. 21 Abs. 1 Satz 2 DS-GVO) statthaft sein muss.

Die Regelung könnte anlog zu Art. 15 Abs. 4 DS-GVO getroffen werden, die das Recht auf eine Kopie der Daten gemäß Art. 15 Abs. 3 DS-GVO beschränkt.

Wenn ein Verarbeiter dem Recht auf Auskunft aufgrund einer entsprechenden Interessensabwägung nicht nachkommt, müssen die Gründe dem Patienten verbunden mit dem Hinweis mitgeteilt werden, dass sich die Person an die zuständige Aufsichtsbehörde zur Überprüfung des Sachverhaltes wenden kann.

4.2.2. Beschränkung des Rechts auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit ist eine große Errungenschaft der DS-GVO, welche dem Bereich eHealth in Deutschland neue Impulse geben kann. Allerdings muss der nationale Gesetzgeber hier zuvor Bedingungen schaffen, welche eine sinnvolle Umsetzung erst ermöglichen. Alternativ kann der Weg über Artikel 40 DS-GVO eingeschlagen werden und der nationalen Aufsichtsbehörde eine Verbandsregelung entsprechend Art 40 Abs. 2 DS-GVO vorlegen. Eine Verbandsregelung kann beispielsweise durch eine Zusammenarbeit von Bundesärztekammer, Krankenhausgesellschaft, bvitg, GDD und GMDS erstellt werden.

Art. 20 Abs. 1 DS-GVO gibt einem Patienten das Recht, seine Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“. Die technische Umsetzung ist trivial und schnell zu erfüllen, jeder Export der Daten in eine XML-Datei erfüllt die gesetzlichen Bedingungen. Allerdings werden diese Daten von keiner anderen datenverarbeitenden Stelle einlesbar sein. Damit diese rechtliche Vorgabe sinnvoll umgesetzt werden kann, muss der nationale Gesetzgeber festlegen

a) welche Daten eines Patienten sollen exportiert werden
b) welches Format soll genutzt werden.

Zu a): Während einer Patientenversorgung fallen viele administrative Daten an wie z.B. Abrechnungsdaten in der niedergelassenen Praxis oder dem Krankenhaus oder Verlegungsdaten in einem Hospital, welche für die weitere Patientenbehandlung irrelevant sind. Ein unbeschränkter Datenexport wird dazu führen, dass die nach- oder weiterbehandelnde Stelle in der Menge der Daten die relevanten Patienteninformationen ggf. nicht findet. Daher muss hier eine rechtliche Regelung erfolgen, welche den Datenexport zum Zwecke der Weitergabe an eine nach- oder weiterbehandelnde Stelle auf diagnose- und behandlungsrelevante Daten beschränkt. Die Vorgaben, welche medizinischen Daten ausgetauscht werden sollten, könnte von einem entsprechenden Arbeitskreis des wissenschaftlichen Beirats der Bundesärztekammer erarbeitet werden.

Zu b): Die Extensible Markup Language (XML) hat sich derzeit bzgl. eines Austausches strukturierter Daten etabliert. Zudem gibt es eine Vielzahl von XML-Prozessoren (sogenannte „Parser“) für diverse Programmiersprachen wie C++, Java C#, sodass die Einbindung von XML-Strukturen in vorhandene Softwarelösungen unkompliziert implementiert werden kann. Allerdings muss bei XML die grundlegende Struktur vorgegeben werden, ansonsten ist ein Datenaustausch mittels XML nicht möglich. HL7 CDA - die Clinical Document Architecture - basiert auf der Extensible Markup Language (XML) und ist speziell für die Übermittlung von medizinischen Daten in einem Patientenkontext entwickelt worden, sodass unter Nutzung der Vorteile der XML-Spezifikation ein standardisierter Datenaustausch für Gesundheitsdaten ermöglicht und stark vereinfacht wird. HL7 Deutschland könnte damit beauftragt werden, die Spezifikation eines entsprechenden

CDA-Datenaustauschformats für das Gesundheitswesen zu erstellen, basierend auf den oben beschriebenen inhaltlichen Vorgaben.

4.3. Geheimhaltungspflicht für Auftragsverarbeiter

Art. 9 Abs. 3 DS-GVO fordert eine Geheimhaltungspflicht für Personen, welche besondere Kategorien personenbezogener Daten gemäß Art. 9. Abs. 2 lit. h DS-GVO verarbeiten. Mit § 203 StGB existiert in Deutschland eine entsprechende Regelung. In der juristischen Literatur wird jedoch unterschiedlich diskutiert, ob Auftragsverarbeiter unter § 203 StGB im Rahmen einer Gehilfenregelung fallen oder nicht.

Um den Anforderungen der DS-GVO zu genügen und hier zugleich Rechtssicherheit zu schaffen, wäre daher eine Regelung analog § 17 UWG dringend erforderlich, wonach Auftragsverarbeiter einer gesetzlichen Schweigepflicht unterliegen. Dabei muss diese Regelung statt auf „Geschäfts- oder Betriebsgeheimnis“ wie bei § 17 UWG auf die „Verarbeitung besonderer Kategorien personenbezogener Daten“ zielen und die Pflicht zur Geheimniswahrung auch nach Beendigung der Tätigkeit fortbestehen.

4.4. Patientenversorgung

4.4.1. Datenweitergabe an mitbehandelnde/weiterbehandelnde Personen

Es ist zwingend notwendig, dass Erlaubnistatbestände zur Datenweitergabe an mitbehandelnde und/oder weiterbehandelnde Personen, die nicht zwangsläufig ärztliche Personen sein müssen, weiterhin gesetzlich geregelt bleiben. Dies schließt die derzeitigen gesetzlichen Regelungen der Sozialgesetzbücher ein, insbesondere auch die Regelungen bzgl. des MDK.

Es ist wünschenswert, dass die Erlaubnistatbestände nicht zwingend die Einwilligung des Patienten erfordern, wenngleich selbstverständlich die Transparenz gewährleistet sein muss. Bei der Behandlung eines Patienten erscheint es zweifelhaft, inwieweit ein Patient im Rahmen seiner Behandlung eine Einwilligung unter Berücksichtigung der Vorgaben der DS-GVO geben kann, und ob z. B. unter dem Eindruck der eigenen Erkrankung noch von einer „Freiwilligkeit“ bei der Zustimmung ausgegangen werden kann. Um hier Rechtsunsicherheiten zu vermeiden, sollte der nationale Gesetzgeber klare Erlaubnistatbestände schaffen, in denen geregelt wird, dass zur Mit- und Weiterbehandlung zwingend benötigte Informationen zwischen den behandelnden Personen ausgetauscht werden dürfen, wobei der aus Art. 14 DS-GVO resultierenden Informationspflicht gegenüber dem Patienten genügt werden muss.

4.5. Medizinische Forschung und Lehre

Die medizinische Forschung wird in der DS-GVO nur am Rande betrachtet. Vielmehr überlässt man die gesetzliche Ausgestaltung dieses Themas dem nationalen Gesetzgeber.

4.5.1. Datenverarbeitung für wissenschaftliche Zwecke

Art. 9 Abs. 2 lit. j DS-GVO schreibt:

> „die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.“

Damit Daten für wissenschaftliche oder historische Forschungszwecke genutzt werden können, muss also zuvor ein Erlaubnistatbestand in Form des Unionsrechts oder des Rechts eines Mitgliedstaats existieren.

Dieses Recht muss den Anforderungen von Art. 9 Abs. 2 lit. j DS-GVO genügen:

- Berücksichtigung eines angemessenen Verhältnisses zu dem verfolgten Ziel
- Das Recht auf den „Wesensgehalt des Rechts auf Datenschutz“ muss gewahrt werden, d.h. insbesondere Berücksichtigung von Art. 5 DS-GVO
    - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a DS-GVO)
    - Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)
    - Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)
    - Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)
    - Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO)
    - Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)
    - Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO)

  und Art. 6 bzw. Art. 9 DS-GVO.

- Das Recht muss „spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorsehen.

Hier wäre ein gesetzlicher Erlaubnistatbestand analog § 28 Abs. 6 Nr. 4 BDSG wünschenswert, in dem die Nutzung personenbezogener Daten der besonderen Art (§3 Abs. 9 BDSG) für Forschungszwecke bei Unabdingbarkeit und Verhältnismäßigkeit unter den Voraussetzungen von § 40 BDSG (Zweckbindung auf Forschung, frühestmögliche Pseudonymisierung/Anonymisierung, Veröffentlichung nur mit Einwilligung bzw. bei Personen der Zeitgeschichte und vorhandenem öffentlichem Interesse) und den Vorgaben aus Art. 5 DS-GVO gestattet wird.

4.5.2. Daten, die eine „breite Einwilligung“ benötigen

Art. 9 Abs. 2 lit. j DS-GVO beinhaltet einerseits die Zweckbindung wie auch das Gebot der Datenminimierung. Für die Nutzung von personenbezogenen Daten besonderer Kategorien gemäß Art. 9 Abs. 1 DS-GVO in Krankheitsregistern und bei Biodatenbanken kann daher dieser Artikel nicht herangezogen werden.

Art. 9 Abs. 2 lit. h DS-GVO lautet:

> „die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich“

D.h. Art. 9 Abs. 2 lit. h DS-GVO gestattet einem Mitgliedstaat eine nationale Gesetzgebung

- für Zwecke der Gesundheitsvorsorge
- für Zwecke der Arbeitsmedizin
- für die Beurteilung der Arbeitsfähigkeit des Beschäftigten
- für die medizinische Diagnostik
- für die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich
- für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich

unter Berücksichtigung von Art. 9 Abs. 3 DS-GVO. Dieser verlangt, dass

- diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und
- dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt

oder

- wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

Somit ist es einem Mitgliedstaat gestattet, eine nationale Regelung zu erlassen, welche die Nutzung besonderer Kategorien personenbezogener Daten für Forschung im Bereich der medizinischen Diagnostik, Versorgung oder Behandlung gestattet, wenn diese nationale Regelung zugleich dafür Sorge trägt, dass die Verarbeitung nur durch Fachpersonal erfolgt und dieses einer Geheimhaltungspflicht entsprechend Art. 9 Abs. 3 DS-GVO unterliegt. Bzgl. der Geheimhaltungspflicht wurde in Kapitel 4.3 ein Vorschlag beschrieben.

Eine nationale Regelung gemäß Art. 9 Abs. 2 lit. h DS-GVO könnte jedoch die Vorgaben bzgl. Verwendungszweck und Datenminimierung weniger streng fordern (analog Erwägungsgrund 33) und auch die Informationspflichten bei zweckändernder Datenverwendung (analog Erwägungsgrund 62) moderater gestalten.

4.5.3. Spezialfall Big Data

Für den Begriff „Big Data“ existiert keine allgemein anerkannte Definition, es existieren lediglich verschiedene Beschreibungen, was jeweils unter Big Data verstanden wird. Die in Deutschland wohl am häufigsten verwendete Definition des Begriffs „Big Data“ stammt vom BITKOM e.V.[3]: Dabei wird Big Data als „die wirtschaftlich sinnvolle Gewinnung und Nutzung entscheidungsrelevanter Erkenntnisse aus qualitativ vielfältigen und unterschiedlich strukturierten Informationen, die einem schnellen Wandel unterliegen und in bisher ungekanntem Umfang zu Verfügung stehen“ definiert. Dabei werden im Big Data Umfeld ggfs. personenbezogene Daten verarbeitet, die ohne konkreten Verwendungszweck erhoben oder zum Erhebungszeitpunkt zu einem anderen Zweck gespeichert wurden. Dabei werden Daten genutzt, die bei zeitlich nach der Erhebung auftauchenden Fragestellungen deren Beantwortung erleichtern oder ermöglichen sollen. Somit stellt Big Data eine Vorratsdatenspeicherung dar, die speziell im Bereich der medizinischen Big Data Anwendungen besonders sensible Daten verarbeitet.

[3] BITKOM. (2015) Big Data und Geschäftsmodell - Innovationen in der Praxis: 40+ Beispiele. [Online, zitiert am 2016-05-26]; Verfügbar unter https://www.bitkom.org/Publikationen/2015/Leitfaden/Big-Data-und-Geschaeftsmodell-Innovationen/151229-Big-Data-und-GM-Innovationen.pdf

Der EuGH äußerte sich 2014 in seinem Urteil[4] zur Vorratsdatenspeicherung, dass diese als ein „Eingriff in die in Art. 7 und Art. 8 der Grundrechtecharta verankerten Grundrechte von großem Ausmaß und als besonders schwerwiegend anzusehen“ ist. Zugleich stellte der EuGH fest, dass eine Vorratsdatenspeicherung nicht den Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte verletzen muss und eine Vorratsdatenspeicherung ebenso den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten gewährleisten kann. Voraussetzung ist, dass

- die Vorratsdatenspeicherung eine dem Gemeinwohl dienende Zielsetzung verfolgt
- die Vorratsdatenspeicherung zur Erreichung des Zieles geeignet ist
- es kein milderes Mittel zur Erreichung des dem Gemeinwohl dienenden Zieles gibt
- klare und präzise Regeln müssen den Eingriff in die Grundrechte auf das „absolut Notwendige“ beschränken (Angabe von den zu speichernden Daten, Speicherzeitraum, Zugang zu den Daten)
- dem Betroffenen gegenüber ist eine Transparenz bzgl. der Verarbeitung seiner Daten zu gewähren ist, sofern dies mit der Erreichung des dem Gemeinwohl dienenden Zieles vereinbar ist
- technische und organisatorische Maßnahmen ausreichende Garantien für einen „wirksamen Schutz der personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung“ bieten.

Der EuGH erklärte mit seinem Urteil eine anlasslose Vorratsdatenspeicherung grundsätzlich für unzulässig: Die pauschale, unterschiedslose Datenspeicherung ist unvereinbar mit der gebotenen Beschränkung von Grundrechtseingriffen auf das „absolut Notwendige”.

Big Data besitzt das Potential die Gesundheitsversorgung der Menschen deutlich zu verbessern, z.B. [5,6,7,8]. Entsprechende medizinische Big Data Anwendungen verfolgen somit eine dem Gemeinwohl dienende Zielsetzung. Es müssen bei einer entsprechenden Gesetzgebung jedoch Grenzen festgelegt werden:

- Zu welchem Anlass erfolgt die Vorratsdatenspeicherung? Z.B. Big Data Analysen bzgl.
  - Erforschung des Auftretens und Verhinderns von Arzneimittelnebenwirkungen
  - Optimierung der Notfallversorgung
  - Erforschung von Herz-Kreislauf-Erkrankungen
- Welche Kategorien von Gesundheitsdaten werden gespeichert? Hier muss eine klare Benennung auf die absolut notwendigen Kategorien erfolgen, ähnlich, wie es in § 65c SGB V zur Einführung von klinischen Krebsregistern geschah.

[4] EuGH, Urt. vom 08.04.2014 Az.: C-293/12 und C-594/12. . [Online, zitiert am 2016-05-26]; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=EuGH&Datum=08.04.2014&Aktenzeichen=C-293/12

[5] Becke EM; Schwab D. (2015) Big Data im Gesundheitswesen - Datenschutzrechtliche Zulässigkeit und Lösungsansätze. ZD (4): 151 - 155

[6] Jensen PB, Jensen LJ, Brunak S (2012) Mining electronic health records: towards better research applications and clinical care. Nature Reviews Genetics (13): 395-405

[7] 13. Katko P, Babaei-Beigi A. (2014) Accountability statt Einwilligung? Führt Big Data zum Paradigmenwechsel im Datenschutz? MMR (6): 360 - 364

[8] 20. Weichert T. (2013) Big Data und Datenschutz - Chancen und Risiken einer neuen Form der Datenanalyse. ZD (6): 251 - 259

- Wie lange werden die Daten gespeichert? Zur Erforschung medizinischer Erkrankung ist eine langfristige Speicherung unumgänglich, so dass Vorgaben von 30 oder 50 Jahren sinnvoll erscheinen.
- Wer darf welche Daten zu welchen Zwecken nutzen? Nur für nationale Organe Tätige? (siehe EuGH-Urteil). Hierbei ist zu bedenken, dass die Ergebnisse der Big Data Anwendungen Patienten nur zugute kommen können, wenn diese Ergebnisse in praktisch direkt am Patienten anwendbare Erzeugnisse verarbeitet werden, was klassischerweise durch kommerzielle Hersteller erfolgt.
    - Häufig können Daten, die zu einem Zweck gesammelt werden, dazu dienen, andere Fragestellung zu beantworten. Entsprechend der Vorgabe von Art. 5 Abs. 1 lit. c DS-GVO bzgl. der Datenminimierung sollte gesetzlich bestimmt werden, wann bereits erhobene Daten zu einem anderen Zweck verwendet werden dürfen.
- Wie werden die Daten geschützt? Hier sind die Vorgaben der DS-GVO zu berücksichtigen, insbesondere Artt. 5, 25, 32 DS-GVO.
- Die Datensammlung muss einen anonymen Export zur Beantwortung einzelner Fragestellungen ermöglichen, sodass die Risiken des Betroffenen bzgl. eines Missbrauchs seiner Daten minimiert werden. (Bzgl. Anonymität siehe auch Abschnitt 5.4)
- Der Betroffene muss darüber informiert werden, welche seiner Daten von wem wofür verarbeitet werden (Artt. 12, 13, 14 DS-GVO), sofern die Daten nicht anonym verarbeitet werden.

Es bedarf also einer gesetzlichen Regelung für Big Data Anwendungen, welche die obigen Punkte berücksichtigt, z. B. für die Arzneimittelsicherheit.

4.5.4. Spezialfall Biomaterial

Insbesondere sollte eine nationale Regelung die Erlaubnis der Verarbeitung von personenbezogenen Daten, die zusätzliche Informationen von Dritten beinhalten, unabhängig von der Einwilligung regeln. Derartige Daten wie z. B. Biomaterial, welches prinzipiell auch Daten über verwandte Personen wie beispielsweise Kinder, Eltern, Enkel enthält, sind im Rahmen der Vorgabe der DS-GVO mittels Einwilligung kaum zu verarbeiten, da eine Einwilligung immer nur für die eigenen Daten, nicht aber für die Daten Dritter gegeben werden kann. Gibt eine Person heute beispielsweise Biomaterial ab, so kann ein heute noch nicht geborenes Enkelkind aufgrund der Kenntnis dieses gespendeten Biomaterials in der Zukunft durch eine Erkrankung diskriminiert werden, die heute noch gar nicht bekannt ist, die aber dem Erbgut innewohnt. Daher wird für die Verarbeitung derartiger personenbezogener bzw. personenbeziehbarer Daten ein gesetzlicher Erlaubnistatbestand benötigt, wenn seitens der Gesellschaft ein Konsens besteht, dass die Vorratsdatenspeicherung von Biomaterial mit recht allgemeiner Zweckbindung („medizinische Forschung“) gewünscht ist.

4.5.5. Öffentliches Interesse

Generell ist es für einen Gesetzgeber schwierig, allgemeingültige Regelungen bzgl. des „öffentlichen Interesses“ bei medizinischer Forschung anzugeben. Eine Möglichkeit wäre es, neben den Anforderungen von Art. 5 und 6 bzw. 9 DS-GVO allgemeine Anforderungen wie

- Nachweis der Erforderlichkeit der Daten zur Erreichung des beabsichtigten Forschungszweckes,
- Darstellung, dass der Forschungszweck mit anderen Daten gar nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,

- Darstellung der Interessenabwägung zwischen der Bedeutung des Forschungsziels für die öffentliche Gesundheitsversorgung und dem Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung der Daten inkl. dem Nachweis, dass das Interesse an der Durchführung der Forschung überwiegt

zu definieren und zu bestimmen, dass eine Ethikkommission der zuständigen Ärztekammer (analog MBO-Ä[9]) anhand der Vorgaben im jeweiligen Kontext darüber entscheidet, ob die Forschung im öffentlichen Interesse liegt oder nicht.

Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit muss der Begriff der „öffentlichen Gesundheit" entsprechend Erwägungsgrund 54 zudem im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 ausgelegt werden, d. h. wie der Begriff in dieser Richtlinie bzgl. der Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz ausgelegt wird. Somit wird der Begriff relativ weit gefasst.

Erwägungsgrund 54 beschränkt jedoch auch die Gruppen, denen eine Verarbeitung durch eine nationale Regelung gestattet werden darf: „Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten." Somit muss der nationale Gesetzgeber bei der Verarbeitung von besonderen Kategorien von Daten aus öffentlichem Interesse explizit festlegen, wem diese Verarbeitung erlaubt ist, z. B. nationalen Stellen, denen entsprechende Forschungsaufträge als Aufgabe übertragen werden.

Im Rahmen der DS-GVO wird es jedoch wohl nicht möglich sein, dass beliebige Forscher in privaten Institutionen auf Grund von auf öffentlichem Interesse beruhenden Öffnungsklauseln Forschung betreiben dürfen.

4.5.6. Lehre und Ausbildung

Die praxisnahe Ausbildung von Medizinern, Pflegekräften usw. führt zunehmend zur Einbindung von Studenten, Praktikanten, Hospitanten etc. in den medizinischen Arbeitsablauf, ohne dass hierbei ein arbeitsrechtlichen Vertragsverhältnis entsteht. Der nationale Gesetzgeber sollte eine Zulässigkeit unter der Voraussetzung schaffen, dass diese Personen in die Organisation der medizinischen Einrichtung eingebunden werden und hierbei den datenschutzrechtlichen Pflichten unterworfen werden.

4.6. Datenverarbeitung für Zwecke der Qualitätssicherung

Art. 9 Abs. 2 lit. i DS-GVO erlaubt „die Verarbeitung ist aus Gründen des öffentlichen Interesses" zur „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten" auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, welches „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht".

[9] (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte. Online, zitiert am 2016-04-15]; Verfügbar unter http://www.bundesaerztekammer.de/recht/berufsrecht/muster-berufsordnung-aerzte/muster-berufsordnung/

Somit ist auch in diesem Fall der nationale Gesetzgeber gefordert, Regelungen zu erlassen, welche die Nutzung besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 zu Zwecken der Qualitätssicherung erlaubt. Dieses Gesetz muss insbesondere den Anforderungen von Art. 5 und 6 bzw. 9 DS-GVO als auch den Betroffenenrechten (Artt. 12 bis 22 DS-GVO) genügen („angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person"). Hier wäre ein gesetzlicher Erlaubnistatbestand analog § 28 Abs. 6 Nr. 4 BDSG wünschenswert, nur dass in diesem Fall die Qualitätssicherung und nicht die Forschung adressiert wird.

4.7. Nutzung von Beschäftigtendaten

Gemäß Art. 88 DS-GVO können die Mitgliedstaaten spezifische Vorschriften zur Verarbeitung von Beschäftigtendaten, insbesondere für Zwecke der Einstellung oder der Erfüllung des Arbeitsvertrags, erlassen.

Im Rahmen der Versorgung von Patienten müssen regelmäßig Beschäftigtendaten in Informationssystemen gespeichert werden, z. B. wann welche Mitarbeiter auf welche Patientendaten zugreifen. Hier wäre es wünschenswert, dass zumindest die Regelungen des § 32 BDSG auch nach Inkrafttreten der DS-GVO weiterhin gelten, damit für die Nutzung dieser Daten eine gesetzliche Grundlage vorhanden ist.

4.8. Auftragsverarbeitung

4.8.1. Auftragsverarbeitung als Offenbarungsbefugnis im Sinne des StGB

Keine Arztpraxis und kein Krankenhaus kommt heute ohne die Wartung der medizinischen Geräte und IT-Systeme durch die Hersteller aus. Die Einholung einer Schweigepflichtentbindung jedes Patienten durch die verantwortliche Stelle ist jedoch nicht realisierbar: verweigert nur ein Patient die Abgabe einer Schweigepflichtentbindung, so können moderne Geräte wie MRT/CT, Strahlentherapiegeräte usw. nicht mehr gewartet und damit nicht mehr betrieben werden. Dies gefährdet jedoch die Versorgung aller Patienten. D.h. entweder muss die Versorgung eingestellt werden oder die Wartung auch ohne die Schweigepflichtentbindung des jeweiligen Patienten durchgeführt werden.

Somit ist keine Freiwilligkeit gegeben. Im Rahmen der Überarbeitung der Datenschutzgesetze ist eine Offenbarungsbefugnis zu schaffen und handelnde Personen als Gehilfen zu klassifizieren, sodass der Schweigepflicht genügt wird.

Die Vorrangstellung des europäischen gegenüber dem entsprechenden deutschen Recht eröffnet die Frage, ob die DS-GVO als vorrangiges Recht gegenüber dem StGB zu betrachten ist und somit der nationale Gesetzgeber eine datenschutzrechtliche Regelung treffen kann.

4.9. Klarstellung bzgl. der Verhängung von Bußgeldern

Entsprechend § 17 OWiG drohen Bußgelder bei Verstößen gegen entsprechende rechtliche Regelungen. Im Falle von Unternehmen betrifft dies i.d.R. Mitarbeiter. Bußgelder werden gegen ein Unternehmen i.d.R. nur dann verhangen, wenn ein leitender Angestellter verantwortlich ist; die §§30 und 130 OWiG sind hier eindeutig.

Die DS-GVO hingegen legt in Art. 83 auch die rechtswidrigen Handlungen einfacher Angestellter den Unternehmen zur Last. D. h. nach DS-GVO haftet das Unternehmen für Datenschutzverstöße aller Mitarbeiter, nach OWiG für die Verstöße leitender Angestellter. Verwaltungsrechtlich ist nicht sicher,

dass die EU Ordnungsstrafen rechtlich vorgeben darf, die rechtliche Kompetenz erstreckt sich auf die freien Handelswege bzgl. des Binnenmarktes (bzw. Abbau von Handelshindernissen.)

Hier sollte der nationale Gesetzgeber klarstellen, unter welchen Umständen die Verhängung eines Bußgeldes gemäß Art. 83 den nationalen Vorgaben entsprechen muss, damit die Bedingungen von Art. 83 Abs. 8 erfüllt sind. D.h. „angemessene Verfahrensgarantien“ entsprechend Unionsrecht und dem Recht des Mitgliedstaates Deutschland sind dann gegeben, wenn bei der Verordnung von Bußgeldern die Vorgaben des OWiG berücksichtigt sind.

5. Ändern bestehender gesetzlicher Regelungen

5.1. Schriftform der Einwilligung

Die Schriftform der Einwilligung ist hinsichtlich der heutigen IT-gestützten Versorgung kaum als Stand der Technik anzusehen. Insbesondere, wenn man den politischen Willen zur Etablierung von institutsübergreifenden elektronischen Patientenakten berücksichtigt, ist die Etablierung einer elektronischen Einwilligung unabdingbar.

Daher sollte die Anforderung aus der DS-GVO unverändert übernommen werden.

5.2. Datennutzung bei einem Verantwortlichen

Mehrere Landesregelungen bestimmen derzeit, dass Daten innerhalb eines Krankenhauses vor anderen Abteilungen des gleichen Krankenhauses geschützt werden müssen. D.h. die innere Klinik des Krankenhauses darf die alten Akten eines Patienten aus der Chirurgie nicht sehen, ausgenommen der Patient hat explizit eingewilligt. Die Erwartungshaltung eines Patenten ist in der Regel jedoch, dass die Daten innerhalb eines Krankenhauses für alle Behandler verfügbar sind.

Diese restriktive deutsche Regelung kann Patientenleben gefährden, z.B.: wenn der Internist nicht sehen kann, dass der Patient auf die Antibiotikagabe vor einem Jahr in der Chirurgie mit einem allergischen Schock reagierte, kann dieses Nicht-Wissen den Tod des Patienten zur Folge haben.

Aus Sicht der DS-GVO (Art. 4 Nr. 7) ist die jeweilige Institution „Verantwortlicher“ und somit die Stationen innerhalb eines Verantwortlichen nicht Dritter. Dies entspricht auch den Anforderungen, die aus der heute stattfindenden Patientenversorgung erwachsen. Daher sollten diese restriktiven nationalen Regelungen, die derzeit in Bremen, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen und Saarland existieren, ersatzlos gestrichen werden.

5.3. Ort der Auftragsverarbeitung

In mehreren landesrechtlichen Datenschutzregelungen (z.B. in Bayern oder Berlin) wird gefordert, dass die Verarbeitung von Patientendaten nur in einem Krankenhaus stattfinden darf.

In großen (60-80 Mitarbeitern) EDV-Abteilungen kann ein Rechenzentrum vermutlich sicher betrieben werden. Aber bedingt durch die heutige Komplexität (virtuelle Server, Firewallregeln bzgl. dezentraler Patientenversorgung, Verteilung von Antivirensignaturen, unterschiedliche Betriebssysteme, Anbindungen unterschiedlichster Systeme wie z.B. KV-Safenet - die Liste kann beliebig lang aufgeführt werden) ist die Sicherheit eines Klinik-Rechenzentrums, wie sie auch im IT-Sicherheitsgesetz thematisiert wird, nur durch externen Einsatz von entsprechend geschultem Fachpersonal sicherzustellen.

Hier sollte man diesen Anforderungen (im Sinne gestiegener Anforderungen an der EDV-Verfügbarkeit bei der Patientenversorgung) folgen und im Sinne einer verbesserten Rechenzentrumssicherheit den externen Rechenzentrumsbetrieb legalisieren. Damit müssen die Betreiber und dessen Mitarbeiter als Gehilfe des Arztes im Sinne § 203 StGB betrachtet und die Auftragsverarbeitung in diesem Sinne legalisiert und vertraglich vereinbart werden.

5.4. Begriff der Anonymität

In den letzten Jahren wurde immer wieder gezeigt, dass bei der Zusammenführung medizinischer Daten eine Re-Identifizierung bei „anonymen" Daten durchgeführt wurde[10]. Unter Berücksichtigung der stetig wachsenden Menge an personenbezogenen Daten in sozialen Netzwerken, welche auch Gesundheitsdaten beinhalten, und die als ergänzende Datenquellen zu den vorhandenen Datensätzen dienen können, steigt das Re-Indentifikationsrisko selbstverständlich noch weiter an. Daher wird heute davon ausgegangen, dass es im Rahmen von medizinischen Daten keine Anonymität gibt, wenn hinreichend viele Daten zusammengeführt werden. Dies trifft insbesondere auf Big Data Anwendungen zu, letztlich muss aber bei jeder Zusammenführung medizinischer Daten die Möglichkeit einer Re-Identifikation geprüft und das Risiko eingeschätzt werden.

Um die Forschung mit anonymen Datensätzen weiterhin zu ermöglichen, sollte der Gesetzgeber die heutige Definition anonymer Daten dahingehend ändern, dass Daten als anonym gelten, wenn der Datenverarbeiter keine Möglichkeit der Re-Identifikation hat. Dies sollte von einer strafrechtlichen Sanktionierung der Re-Identifikation begleitet werden.

Diese Sanktionierung sollte beinhalten: persönliche Haftung der Leitung der für die Datenverarbeitung verantwortlichen Stelle (Freiheits- oder Geldstrafe) flankiert von einer entsprechenden Geldbuße für das Unternehmen selbst, wobei antragsberechtigt für die Strafverfolgung neben dem Betroffenen auch Datenschutzaufsichtsbehörden und Verbraucherverbände sind. Damit kann eine Ausgewogenheit hergestellt werden, d.h. dem Schutzbedarf der sensitiven Daten eines Betroffenen wird eine entsprechende Sanktionsmöglichkeit gegenübergestellt, welche diesen Schutz vor einer Re-Identifikation gewährleistet.

Die heutige Begriffsbestimmung in § 3 Abs. 6 BDSG sollte bei der Anpassung der nationalen rechtlichen Vorgaben an die Vorgaben der DS-GVO in die entsprechende Nachfolgeregelung übernommen und dahingehend ergänzt werden, dass bei der Beurteilung, ob Daten als re-identifizierbar anzusehen sind, nur rechtlich zulässige Methoden betrachtet werden.

[10] Z.B. Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y (2013) Identifying Personal Genomes by Surname Inference. Science 339: 321ff oder auch Franzosa et al. (2015) Identifying personal microbiomes using metagenomic codes. PNAS (online first, http://www.pnas.org/content/early/2015/05/08/1423854112.abstract)