Institut für Informationsordnung
infino.org

Datenschutzrechtliches Gutachten

Datenschutzrechtliche Anforderungen an die Verarbeitung und Nutzung anonymisierter Daten für andere Zwecke nach § 300 Abs. 2 Satz 2, 2. Halbsatz SGB V durch Apotheken-Rechenzentren

von
Dr. Thomas Giesen, Rechtsanwalt *
Dr. Christian Schnoor, Rechtsanwalt **

*Sächsischer Datenschutzbeauftragter a. D.
**Referatsleiter beim Sächsischen Datenschutzbeauftragten a. D.

Institut für Informationsordnung e.V. · Palaisplatz 3 · 01097 Dresden
Vorstand: Dr. Thomas Giesen · Michael Schönfelder
Geschäftsführer: Dr. Christian Schnoor
Amtsgericht Dresden VR 5392
Telefon: 0351 8008177 · Telefax: 0351 8008120 · www.infino.org · info@infino.org

Inhaltsübersicht:

---

[1] Vorbemerkung zur Terminologie: Nachfolgend wird dort, wo es nicht auf die genaue Unterscheidung verschiedener Arten von Verarbeitungs(!)-Handlungen ankommt, aus Gründen der Vereinfachung des sprachlichen Ausdrucks (d.h. zur Vermeidung des umständlichen Begriffs „Verwendung“ oder gar „Umgang“ mit Daten) vielfach, übrigens in Übereinstimmung mit der Terminologie vieler landesgesetzlicher Datenschutzrechtsvorschriften, der Begriff der „Verarbeitung“ in einem weiteren, umfassenden Sinne verwendet.

1 Rechtliche Grundlagen und Ausgangsbedingungen

Nach § 300 SGB V sind die Apotheken verpflichtet, ihre Abrechnungsdaten auf elektronischem Weg an die Krankenkassen zu übermitteln, damit diese möglichst wirtschaftlich abrechnen können. Weil die einzelnen Apotheker als Einzelunternehmer technisch nicht in der Lage sind, die Abrechnungsdaten in die passende elektronische Form zu bringen, können sie sich eines Apotheken-Rechenzentrums (im Folgenden: ARZ) bedienen. Dort laufen die Informationen über Patienten und Ärzte personenbezogen zusammen. Ein gewichtiger, weil verdeckter Teil des Umgangs der ARZ mit diesen Daten und dessen Grenzen ist Gegenstand des vorliegenden Gutachtens: Die Weitergabe von Informationen über das Verordnungsverhalten der Ärzte, gelegentlich auch über den Bedarf einzelner Patienten an die Pharmaindustrie.

Mit der gesetzlich oktroyierten Datenverarbeitung im Auftrag ist eine Vielzahl datenschutzrechtlicher Implikationen verbunden. Sie vollzieht sich in einem Bereich, in dem sich das öffentliche Recht in Gestalt des Sozialrechts, das die Datenverarbeitung der gesetzlichen Krankenkassen (GKV) und der Kassenärztlichen Vereinigungen (KV) regelt, und das Privatrecht treffen, das die Tätigkeit der Ärzte, der Apotheker und der sonstigen Leistungserbringer sowie ihrer Datenverarbeiter im Auftrag regelt. Damit werden Graubereiche eröffnet, die sowohl die Herstellung eines Rechtsbewusstseins als auch angemessene Kontrollen erschweren. Das vorliegende Gutachten soll den beteiligten Kreisen, den Datenschutzaufsichtsbehörden für den öffentlichen und den nichtöffentlichen Bereich und dem Bundesgesetzgeber den grundlegenden Bedarf, die Grundlagen und einzelne erste Überlegungen für eine **Neuregelung dieses Bereichs zur Sicherstellung eines angemessenen Datenschutzes** liefern.

Es würde den Rahmen sprengen, würden die Verfasser die vielfältigen Verdachtsmomente nennen, aus denen zu schließen ist, dass die Pharmaindustrie einen enormen Appetit verspürt, Verordnungsdaten zu erfahren. Sie setzen voraus, dass die Fachkreise diese Gefahren sowohl aus dem Gesichtspunkt der (künftig gesondert strafbaren?) "Bestechlichkeit" der Kassenärzte und Apotheker, als auch aus dem Gesichtspunkt der Einflüsse auf die Wirtschaftlichkeit der Arzneimittelversorgung realisiert haben. Ferner verzichten die Verfasser auf die Benennung der ARZ in Deutschland und ihre Werbung: "Wir liefern Ihnen die Daten, die Sie brauchen".

1.1 Besondere Daten

Jeder Umgang mit personenbezogenen Daten[2] bedarf nach § 4 Bundesdatenschutzgesetz (BDSG) einer gesetzlichen Befugnis oder der (nach § 4a BDSG gestalteten, schriftlichen) Einwilligung des Betroffenen. Diese Grundnorm beruht auf Art. 7 der "Richtlinie 95/46 des Europäischen Parlaments und des Rates vom 24. 10. 1995[3] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr". Sie hat ihre verfassungsrechtliche Wurzel in der Würde und Entfaltungsfreiheit des Menschen, Art. 1 und 2 des Grundgesetzes: Das Persönlichkeitsrecht ist sowohl Teil der Würde als auch der Entfaltungsfreiheit jedes Einzelnen.

Eine besondere und wesentliche Verschärfung enthält Art. 8 der EG-Richtlinie, der in Abs. 1 ein grundsätzliches Verbot der Verarbeitung von Daten u. a. "über Gesundheit" ausspricht und als Intensivierung dieses Grundsatzes (neben hier ersichtlich nicht in Betracht kommenden Befreiungen) lediglich die **"ausdrückliche" Einwilligung oder die Verarbeitung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten** zulässt.

Im deutschem Recht muss diese verbindliche Vorgabe des höherrangigen Gemeinschaftsrechts umgesetzt werden; der Umgang mit "besonderen Daten" (siehe die Definition in § 3 Abs. 9 BDSG) hat diese Prinzipien einzuhalten; der Gesetzgeber hat insoweit eine Regelungs- und Beobachtungspflicht; die Exekutive sowie die Datenschutzbeauftragten haben die Gefahren realistisch zu erkennen und zu bekämpfen; die Justiz hat die Verfolgung von Verstößen ernsthaft und nachhaltig zu betreiben.

1.2 Das Apothekergeheimnis

Spezielle und historisch erfolgreiche datenschutzrechtliche Vorbehalte zum Umgang mit Patientendaten erwachsen aus dem Arztgeheimnis und dem Apothekergeheimnis des § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB): Apotheker machen sich wie Ärzte und andere Heilberufsausübende strafbar, wenn sie "unbefugt ein fremdes Geheimnis, namentlich ein zum **persönlichen Lebens-**

[2] Das sind alle Informationen über Menschen oder - in der Sprache des Gesetzes - nach § 3 Abs. 1 BDSG "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder **bestimmbaren** natürlichen Person".
[3] ABl. Nr. L 281 vom 23. 11. 1995 S. 31ff.

bereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbaren". Rechtsgüter dieser Strafvorschrift sind das **Persönlichkeitsrecht** des betroffenen Patienten, genauso die Individualinteressen der übrigen beteiligten und betroffenen Personen (Ärzte, Apotheker und ihre Helfer) und daneben gleichrangig das **Allgemeininteresse an der Funktionsfähigkeit der Heilberufe**: Wenn das Vertrauen in die absolute Verschwiegenheit von Arzt und Apotheker gestört würde, hätte dies schwerwiegende Folgen: Die Patienten würden sich nicht mehr rückhaltlos offenbaren; dies würde die Möglichkeit des Heilens nachhaltig verschlechtern. Das missbrauchte Schlagwort von der "Volksgesundheit"[4] bedarf hier keiner Erwähnung. Hier werden von der Rechtsordnung zum Schutz personenbezogener Daten folglich erhebliche Strafdrohungen ausgesprochen, die als solche zur Durchsetzung eines angemessenen Schutzes beitragen, andere, insbesondere präventive Vorkehrungen jedoch nicht ersetzen.

Das besondere und **höchstrangige Interesse des Staates** an der ungestörten und verlässlichen Vertrauensbeziehung zwischen dem Patienten und "seinem" Arzt oder "seinem" Apotheker kommt deutlich zum Ausdruck: Auch in Strafverfahren und bei der Gefahrenabwehr bleiben die Schweigeverpflichtungen der Heilberufe in der Entscheidungsbefugnis der Angeklagten oder Gefahrträger (§ 53 Abs. 1 Nr. 3 Strafprozessordnung, StPO) durch die Ermittlungsbehörden unberührt; ihre Datenträger sind beschlagnahmefrei (97 Abs. 1 Nr. 1 StPO): Der Respekt vor der Vertraulichkeit ist größer als das Interesse an Strafverfolgung und Gefahrenabwehr.

Ein ARZ trägt hingegen weder die strafrechtlichen Pflichten noch die strafprozessualen Rechte eines Apothekers oder seiner Berufshelfer; Geheimnisse, die dort verarbeitet werden, sind daher, abgesehen von allgemeinen Schutzvorkehrungen der Rechtsordnung, schutzlos. Lediglich dann sind Abrechnungsunterlagen auch im ARZ beschlagnahmefrei, wenn sich das Verfahren gegen einen Patienten richtet.

1.3 Datenverarbeitung im Auftrag

[4] Das "Apotheken-Urteil" in BVerfGE 7, 377, 414 ff. betont den hohen Wert des Ansehens der Apotheken für das Vertrauen, aus dem die Volksgesundheit hervorgeht. Deshalb ist auch jede negative Auswirkung eines Vertrauensverlustes von durchschlagender Bedeutung.

Grundsätzlich steht es jedem Verantwortlichen für eine Datenverarbeitung frei, sich eines Auftragnehmers für bestimmte, von ihm vorgegebene und ohne eigene Entscheidungsbefugnisse auszuführende technisch geprägte Verarbeitungsschritte zu bedienen. Dies umfasst auch den Umgang mit "besonderen Daten". Jedoch bleibt auch in diesem Fall die Verantwortlichkeit für die Datenverarbeitung vollends beim Auftraggeber, § 11 Abs. 1 BDSG.

Der Auftraggeber hat zuvor seinen Auftragnehmer "unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen **sorgfältig auszuwählen**", § 11 Abs. 2 S. 1 BDSG. Das Maß der Sorgfalt hat sich an der Schutzbedürftigkeit der Daten zu orientieren:

1.3.1 Die Gefahren, die dem Persönlichkeitsrecht des betroffenen Patienten drohen bestimmen die Schutzwürdigkeit: Verordnungsdaten können z. B. Karrieren brechen. Anders als unerbetene Werbung (§ 7 UWG) oder selbstveranlasst veröffentlichte Daten (Facebook) greifen Informationen über verordnete Medikamente in falschen Händen (Köpfen) tief in das Persönlichkeitsrecht ein. So wird eine Person, von der bekannt wird, dass ihr bestimmte Dosen eines Neuroleptikums verschrieben wurden, bei Headhuntern, Arbeitgebern, Kranken- und Lebensversicherern oder Banken keine reelle Chance auf faire Behandlung haben; sie ist auf Dauer sozial **stigmatisiert**.

1.3.2 Gefahren drohen aber auch dem Ansehen von Apothekern und Ärzten, wenn ihr Verordnungsverhalten ausgespäht und zum Gegenstand von Verlockungen und Angeboten genommen werden: Bewerbung, Beratung, Beeinflussung, Führung und Bestechung von Personen, die Arzneimittel verordnen oder abgeben, gehen ineinander über. Der Subtilität der Einflüsse - **sie alle gründen auf gezielt am Gesetz vorbei erworbenen Informationen** - und dem Erfindungsreichtum der Täter sind keine Grenzen gesetzt. Hier wird die Berufsausübungsfreiheit des Art. 12 Grundgesetz berührt, aber insbesondere die nur durch sach- und wissenschaftsbezogene bezogene Argumente geleitete ärztliche Sorgfalt untergraben. Zudem wird die Versichertengemeinschaft wirtschaftlich "ausgenommen"; die Solidargemeinschaft leidet.

1.3.3 Die Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen bzw. berufsspezifischen (Schweige-)Verpflichtungen liegt bei der Auftragsdatenverarbeitung nach wie vor beim Auftraggeber, § 11 Abs. 1 S. 1 BDSG. Bei der vertraglichen Gestaltung des Auftragsverhältnisses stehen im Mittelpunkt u. a. die vom Auftragnehmer selbst vorzunehmenden, also internen Kontrollen und die externen "Kontrollrechte des Auftraggebers" (§ 11 Abs. 2 Nr. 7 BDSG).

Der Gesetzgeber geht folglich davon aus, dass der Auftraggeber dazu in der Lage ist, seinen Auftragnehmer zu führen und zu beaufsichtigen. Er geht ferner davon aus, dass dies auch regelmäßig geschieht. Die Ergebnisse seiner eigenständigen Kontrollen sind zu dokumentieren (§ 11 Abs. 3 BDSG).

Ist der Auftraggeber jedoch ein einzelner Leistungserbringer, etwa ein Apotheker, und ist der Auftragnehmer ein ARZ, so herrschen **disparitätische, eben nicht rollenkonforme und folglich von Grund auf unpassende Verhältnisse**: Der Apotheker ist naturgemäß nicht dazu in der Lage, seine Aufsichtsverpflichtungen gegenüber dem ARZ auch nur ansatzweise zu erfüllen. Er kennt die dort herrschenden Zustände, die Organisation, die Personen und insbesondere die die technischen und organisatorischen Maßnahmen auch nicht ansatzweise; erst recht kann er sie nicht beeinflussen. So bleibt die gesetzlich angeordnete Verantwortungsübernahme leeres Geschwätz. Die gesetzlichen Pflichten werden weder erkannt, noch auch nur ansatzweise erfüllt.

Sieht die Rechtsordnung - erst recht, wenn sie dies aus rein wirtschaftlichen Gründen tut - die Einbeziehung eines Auftragnehmers vor, obwohl der Auftraggeber seinen sich aus der Rechtsordnung ergebenden Verpflichtungen ersichtlich schwerlich oder gar nicht nachzukommen in die Lage versetzt ist, so hätte der Gesetzgeber spezialgesetzlich andere aufsichtliche Vorkehrungen zu treffen, die letztlich ersatzweise und anstelle der Aufsicht durch den einzelnen Auftraggeber das Ziel des Gesetzes sicherstellen könnten: **Die strenge und strikt durchgehaltene Zweckbindung der Daten, die Transparenz des Datenverarbeitungsvorgangs aus der Sicht des Patienten, des verordnenden Arztes und des Apothekers sind jedenfalls zu garantieren.**

1.3.4 Schreibt der Gesetzgeber in diesem Zusammenhang die Anonymisierung von Daten beim Auftragnehmer vor, so können schlechterdings nur Methoden einer vollständigen und endgültigen "Entpersönlichung" der Daten gemeint sein.

1.4 Kein Sozialdatenschutz, keine berufliche Schweigepflicht

1.4.1 Unter das Berufsgeheimnis und unter Strafe gestellt werden nicht nur die Ärzte und Apotheker persönlich, sondern auch deren "Berufshelfer". Nach § 203 Abs. 3 S. 2 StGB stehen die "berufsmäßig tätigen Gehilfen" ihren Arbeitgebern gleich. In der Rechtsprechung und in der Literatur werden selbständige Rechenzentren jedoch nicht als solche Gehilfen angesehen, weil und solange sie nicht unter der einzelnen, vom Auftraggeber persönlich verantworteten

Weisung und Kontrolle arbeiten. Sie sind nicht in den organisatorischen und weisungsgebundenen Bereich der vom Berufsträger verantworteten Vertrauensbeziehung zum Patienten einbezogen und eingebunden.[5] Mag man darüber in Bezug auf streng kontrollierte Privatärztliche Verrechnungsstellen noch geteilter Meinung sein[6], so ist jedenfalls ein ARZ so weit vom Einfluss- und Verantwortlichkeitsbereich des einzelnen auftraggebenden Apothekers entfernt, dass es keinerlei Möglichkeit gibt, es als "berufsmäßig tätigen Gehilfen" anzusehen.

1.4.2 Neben das Geheimnis der Heilberufe hat der Gesetzgeber in der Grundnorm des § 35 SGB I das Sozialgeheimnis gestellt, das den Schutz der in heilberuflichen Berufsausübung entstehenden Daten in die Welt der Sozialleistungen des Staates hinein verlängert. Denn es wäre wenig sinnvoll, die Daten in der Hand der Ärzte und Apotheker besonders streng und wirksam zu schützen, sie aber schutzlos zustellen, wenn sie bei den sozialen Leistungsträgern, den gesetzlichen Krankenversicherungen verarbeitet werden. (Auch die privaten Krankenversicherungen und die privatärztlichen Verrechnungsstellen werden in § 203 Abs. 1 Nr. 6 StGB in gleicher Weise mit Strafe bedroht wie die Ärzte und die Apotheker.)

Das Sozialgeheimnis erfüllt mithin rechtssystematisch betrachtet den gleichen Rechtsgüterschutz wie das Berufsgeheimnis, dies allerdings für die sozialen Leistungsträger in deren Verantwortungsbereich. Es verpflichtet sie sicherzustellen, dass die Sozialdaten (das sind nach § 67 Abs. 1 SGB X alle Angaben, wie sie auch in § 203 StGB genannt sind, also Patienten-/Versichertendaten und Arztdaten, auch deren Geschäftsgeheimnisse) nicht unbefugt erhoben, verarbeitet und genutzt werden und stellt alle Verantwortlichen und ihre Mitarbeiter unter die Strafandrohung der §§ 85 und 85a SGB X: Neben hohen Bußgeldern werden Strafen (Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe) angedroht, die dem Strafrahmen des § 203 Abs. 5 StGB entsprechen.

Das Sozialgeheimnis ergänzt und komplettiert folglich den Datenschutz im Gesamtsystem der Gesundheitsversorgung.

1.4.3 Die in § 300 SGB V erwähnten ARZ gehören aber weder zu den Heilberufen noch sind sie Teil der in § 35 SGB I genannten Leistungsträger. Sie und ihre

[5] Allgemeine Meinung; siehe z. B. Fischer Kommentar zum StGB, 58. Aufl. 2011, § 203 Rn.21.
[6] Dazu Giesen, "Zum Begriff des Offenbarens nach § 203 im Fall der Einschaltung privatärztlicher Verrechnungsstellen" in NStZ 2012, 122ff.

Mitarbeiter stehen folglich nicht unter den vg. speziellen Strafandrohungen, sondern nur dem allgemeinen Datenschutzrecht: § § 43 und 44 BDSG drohen Bußgelder und Strafen (ebenfalls Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe) demjenigen an, der vorsätzlich oder fahrlässig unbefugt Daten verarbeitet.

Im Ergebnis sind zwar missbräuchliche Datenübermittlungen strafbar; jedoch wird hier deutlich, dass die ApothekenARZ als private Einrichtungen zwar materiell mit Sozialdaten umgehen, sie aber nicht in den systemischen Datenschutz integriert sind.

1.5 Zwischenergebnis

Das hat zur Folge, dass nicht nur keine externe, wirklich unabhängige und durchschlagskräftige Datenschutz-Kontrolle besteht, sondern dass es kein gewachsenes Berufsethos gibt; die allgemeinen Strafvorschriften greifen nicht, weil es niemanden gibt, der willens und in der Lage wäre, Datenschutzverstößen nachzugehen, sie aufzuklären und den Datenschutzaufsichtsbehörden nach § 38 BDSG zu melden oder gar Strafanzeigen zu erstatten.

Ganz anders sieht das etwa mit dem ARZ aus, das die Abrechnungen der Deutschen Hausärzte durchführt: Es ist eine "Privatärztliche Verrechnungsstelle" im Sinn des § 203 Abs. 1 Nr. 6 StGB. Ausgelöst durch ein Urteil des Bundessozialgerichts[7] hat der Gesetzgeber zudem in der speziellen Vorschrift des § 295a SGB V sichergestellt, dass nicht der einzelne Hausarzt, sondern der auf Landes- bzw. KV-Bezirksebene organisierte Hausärzteverband der Auftraggeber des ARZs ist; damit wird das Ungleichgewicht zwischen Auftraggeber und Auftragnehmer beseitigt. Die Hausärzteverbände haben einen Datenschutzbeauftragten eingesetzt, der das ARZ wirksam kontrolliert. Ferner wird dieses ARZ in § 295a SGB V unter § 35 SGB I und unter die Vorschrift des § 80 SGB X, mithin unter den Sozialdatenschutz gestellt.

Als Zwischenergebnis des vorliegenden Gutachtens verdient es festgehalten zu werden, dass auch die ARZ unter den Auftrag einer leistungs- und insbesondere kontrollfähigen Einheit und (in gleicher Weise wie die Auftragnehmer in § 295a SGB V) unter den Sozialdatenschutz gestellt werden sollten. Nur so kann ein systemischer Datenschutz sichergestellt werden.

[7] BSG, Urteil vom 10. 12. 2008 B 6 KA 37/07 R.

2 Verarbeitung zu eigenen Zwecken: Pflicht zur Anonymisierung

In § 300 Abs. 2 S. 2, zweiter Halbsatz SGB V heißt es mit Blick auf die ApothekenARZ: **"anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden."**

Hier weicht der Gesetzgeber von der Rechte- und Pflichtenzuweisung eines ApothekenARZs als eines Auftragnehmers ab, der nur auf Weisung des einzelnen Apothekers zu arbeiten und nur dessen Verarbeitungszwecke zu verfolgen hat. Aus dem unselbständigen Helfer wird ein eigenständiger Datenverarbeiter, der "andere Zwecke" verfolgen und zu dem Zweck mit Daten umgehen darf.

Das ARZ wird aus der strikten Weisungsbindung entlassen. Die Daten, die es in Zuarbeit erhoben und durch Verarbeitung generiert hat, stehen ihm zur selbständiger Verarbeitung offen. Die Zwecke, die eigentlich auf die Erfüllung gesetzlicher Aufgaben des SGB begrenzt waren, werden gänzlich offen.

Vorausgesetzt wird jedoch, dass die Daten anonymisiert sind.

2.1 Der unbestimmte Rechtsbegriff des Anonymisierens

Es gibt in der deutschen Rechtsordnung mehrere Möglichkeiten, das Schutzniveau für bestimmte Daten zu regeln:

2.1.1 Der gesetzlich vorgeschriebene Schutz bestimmter Daten oder Datenkategorien orientiert sich an der Gefahr, die dem Persönlichkeitsrecht des möglichen Betroffenen droht: Der Missbrauch (datenschutzrechtlich formuliert: die Zweckänderung) wird eingedämmt oder ausgeschlossen, indem der berechtigte, befugte Personenkreis oder der Verwendungszweck im einzelnen definiert werden und der Zugang zu den Daten wird kontrolliert. In diesen Fällen wird ein relativer Datenschutz installiert.

2.1.2 Der Gesetzgeber will jede Nutzungsmöglichkeit unter Wiederherstellung eines Personenbezugs ausschließen. Nur in diesen Fällen spricht er von anonymisierten Daten.

2.1.3 Das Gesetz bestimmt (in § 3 Abs. 6 BDSG und) in § 67 Abs. 8 SGB X den Rechtsbegriff des Anonymisierens als Alternative:

2.1.3.1 Entweder können die Einzelangaben nicht mehr zugeordnet werden - dies ist der absolute Begriff der Anonymisierung mit der Folge, dass von personenbezogenen Daten nicht, besser nie, mehr gesprochen werden kann. Hier werden folglich alle Möglichkeiten, die Daten wieder "personal zu beleben" dadurch ausgeschlossen, dass die Echt- oder Klardaten nach dem Vorgang der Anonymisierung vernichtet werden. Hier handelt es sich um einen endgültigen Informationsverlust.

2.1.3.2 Oder die Einzelangaben können nur mit einem "**unverhältnismäßig großen Aufwand** an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden"; dies ist der relative Anonymisierungsbegriff. Hier bleiben auch nach der Anonymisierung die personenbezogenen Daten bestehen, mögen sie sich auch im Besitz, also der Zugriffsmöglichkeit einer anderen Stelle befinden.

In der datenschutzrechtlichen Fachwelt ist streitig, ob die so anonymisierten Daten noch im weitesten Sinn als (irgendwie und irgendwann) personenbeziehbar und folglich personenbezogen anzusehen sind[8] Dieser Streit kann hier unentschieden bleiben, denn das Schwergewicht des Problems liegt auf einem anderen Feld.

Weil die Möglichkeit des totalen Informationsverlustes in Bezug auf Personen, also die absolute Anonymisierung vom Gesetz in einem Atemzug, nämlich alternativ zur relativen Anonymisierung genannt wird, müssen sich beide Möglichkeiten annähernd vergleichbar stark schützend erweisen, zumal eine höhere Sicherheit für das Persönlichkeitsrecht allenfalls in den Vernichtungsvorschriften gewährt wird.[9] Zwar wird eine absolute Unmöglichkeit in dieser Al-

[8] Zum Stand der Diskussion Buchner in Taeger/Gabel, Kommentar zum BDSG, Frankfurt 2010 § 3 Rn. 44 mit vielen Hinweisen.

[9] Siehe Holznagel/Sonntag: "Anonymes Auftreten ist wohl die effektivste Art des Datenschutzes" in "rechtliche Anforderungen an Anonymisierungsdienste" im Tagungsband

ternative nicht gefordert, es muss sich jedoch um eine "faktische Unmöglichkeit" handeln.[10]

2.2 Zum "unverhältnismäßigen Aufwand"

Die datenschutzrechtliche Literatur wird merkwürdig einsilbig und einfallslos, wenn es darum geht, den Begriff des "unverhältnismäßigen Aufwands" näher einzugrenzen und zu bestimmen. Hier kann der Gesetzgeber nur die Relation zwischen dem vorgestellten Nutzen der Daten für den, der den Umgang mit Klardaten im Wege der Deanonymisierung anstrebt und dem Schaden für das Persönlichkeit der einzelnen Betroffenen einerseits und dem Aufwand andererseits meinen, der ganz praktisch aufzuwenden ist, um den Personenbezug wieder herzustellen. Deshalb ist die Realität, nämlich das tatsächliche Interesse der beteiligten Kreise an Klardaten und die Korrumpierbarkeit der "Schlüsselinhaber" und die Leichtigkeit einer elektronischen Entschlüsselung nicht aus dem Auge zu verlieren.

Die Relativität des Anonymisierungsbegriffs kann sich nicht darin erschöpfen, dass rechtswidrige Versuche der Reidentifizierung/Deanonymisierung unmaßgeblich seien. Rechtswidriges Verhalten ist nicht unverhältnismäßig und nicht jede Rechtswidrigkeit ist unvorhergesehen. Hier müssen, wie auch bei anderen Datensicherheitsaufwendungen, alle vernünftigen Vorkehrungen als angemessen und verhältnisgemäß angesehen werden. Dies auch gegen rechtswidrige und technisch aufwendige Angriffe, wenn und soweit mit ihnen nach einiger Erfahrung zu rechnen ist.

Zu rechnen ist immer, ähnlich wie im Straßenverkehr oder bei der Diebstahlsicherung, mit allen erfahrungsgemäß nicht völlig unwahrscheinlichen Angriffen. Solche Versuche sind umso eher wahrscheinlich, umso höher der Nutzen der erlangten Daten für die Täter sind. Wesentlich ist, welchen Aufwand ein "vernünftiger" **Täter** (der stattdessen in diesem Zusammenhang in der Literatur verwendete Begriff des "Verantwortlichen" - gemeint ist der für die Verarbeitung Verantwortliche - ist in dem Sinn missverständlich, als ein Täter ja gerade unverantwortlich handelt), der an den Daten höchstes Interesse hat und

---

"Datenschutz und Anonymität", Hrsg. Landesbeauftragter für Datenschutz und Informationsfreiheit NRW, Düsseldorf 2000.

[10] So auch Tinnefeld /Ehmann, Einführung in das Datenschutzrecht, S. 187; siehe auch Gola/Schomerus, 11. Aufl. 2012 § 3 Anm. 43 bis 44a.

einen Betrieb eingerichtet hat, der Kunden aus der Pharmaindustrie beliefert, und ihn betreiben kann, ohne völlig unwirtschaftlich zu handeln.

Auch mit mittäterschaftlichem Handeln[11] ist jederzeit zu rechnen: Die beteiligten Kreise sind einander bekannt. Angesichts dessen, dass die Krankenkassen etwa bei ihren Abrechnungen nach § 295 SGB V versicherten- und arztbezogen alle Diagnosen und nach § 300 versicherten- und arztbezogen alle Medikationen erfährt[12], fällt es auch "Ehrenmännern" leicht, sich eine eigene Rechtfertigungsweste zu stricken: denn auch die Pharmaindustrie verfolgt für sich genommen, hier und da menschenfreundliche Ziele, etwa wenn es darum geht, den deutschen Markt als Finanzier für preiswerte Abgaben in ärmeren Ländern zu nehmen.

Hier fehlt das Unrechtsbewusstsein, weil die Gesetze nicht ernst genommen werden und die Verfolgungsbehörden ihre Pflichten nur mit spitzen Fingern erfüllen. Hinzu kommt die gewaltige finanzielle Versuchung, die jedem Gewissen zusetzt.

Mit anderen Worten: Will man ernsthaft über eine gelingende, also endgültige Anonymisierung nachdenken, muss man zwingend die Anreize betrachten, die für denjenigen bestehen, der solcher Daten habhaft werden will, um sie entweder teilweise oder ganz auf Personen beziehen zu können.

Aber selbst diese Überlegung zeigt nur in die richtige Richtung; sie engt die Beweglichkeit bei der Suche nach der für jeden Fall sicheren Lösung jedoch noch immer ein: Denn das Denkmodell der Anonymisierung hat keineswegs zwei ihrerseits jeweils schutzwürdige Seiten auszutarieren und in ein angemessenes Verhältnis zueinander zu bringen, wie das für Juristen etwa beim Widerstreit zweier Grundrechtspositionen (sog. praktische Konkordanz) vorgegeben ist. Im vorliegenden Fall geht es einzig darum, **alle gebotenen Maßnahmen zur endgültigen, also nie mehr rückabwickelbaren Anonymisierung zu ergreifen; je sicherer und einfacher, umso besser! Dabei gilt es, jedem denkbaren Einzelmissbrauch vorzubeugen. Denn jeder Betroffene, dessen Daten missbraucht werden könnten, ist einer zuviel.**

---

[11] In den USA wird das mit "Verschwörung" bezeichnet.

[12] Die Zeiten, in denen nur fallbezogene und gerade nicht versichertenbezogene Daten aus dem Bereich des Arztgeheimnisses und des Apothekergeheimnisses herausgingen, sind lange vorüber.

Denn es gibt kein rechtlich geschütztes Interesse, die Anonymisierung aufzuheben.

2.3 Deanonymisierung ist kein rechtlich geschütztes Anliegen

Es wäre ein verhängnisvoller Fehler, die Anonymisierung schon dann als erreicht anzusehen, wenn ein Laie sie für hergestellt hielte. Gerade die beteiligten Kreise und nur sie entscheiden nach ihren Erfahrungen und Regularien, ob ein Aufwand noch angemessen ist. Der Datenhunger der Pharmaindustrie gilt als groß.

Folglich muss der tatsächliche Aufwand nicht unbedingt noch größer sein, um die durchgängige Anonymisierung zu gewährleisten, vielmehr muss er radikaler wirken.

Dabei kann es durchaus zu prüfen sein, ob derjenige Aufwand, der eine nur scheinbare Anonymisierung herstellt - mit dem nicht ausrottbaren Hintergedanken, dass bestimmten Kreisen eine Deanonymisierung nicht gänzlich verschlossen bleiben soll - tatsächlich größer ist, als der Aufwand, der die Anonymisierung gänzlich und für immer und alle Beteiligten ausschließt.

Der endgültige Verlust eines Personenbezuges der Daten steht nach dem Gesetz folglich in keinem Verhältnis zur Deanonymisierung der anonymisierten Daten: Zwar kann dieses Verhältnis von Bedeutung sein, damit die Anonymisierung gelingen soll. Diese kann aber nur als gelungen bezeichnet werden, wenn die Gefahr einer personenbezogenen Nutzungsmöglichkeit erfahrungsgemäß gegen Null geht. Um Null zu erreichen, wird der Aufwand meist geringer sein, als derjenige, der veinkalkuliert, den Spalt der Deanonymisierung ein wenig offen zu halten.

Das Zusatzwissen bestimmter Personenkreise, die sich am Markt der Pharmaverordnungs-Daten bewegen, ist jedenfalls einzukalkulieren auch dann und soweit, als die intensive und neutrale Beobachtung dieses Marktes immer wieder Anstrengungen und Aufwendungen vermerkt, die auf den Erwerb von Klardaten ausgerichtet sind.

Es spricht in der vorliegenden Konstellation nichts dafür, den Aufwand der Anonymisierung zu beschränken: Denn dieser Aufwand schneidet jede Diskussion darüber ab, welche Gründe es dafür geben könnte, mit beträchtlichem

Aufwand - aus welchen illegalen Gründen auch immer - irgendwann eine De-anonymisierung zu betreiben.

Es wäre eine verfehlte Herangehensweise, die abstrakten, denkbaren Gefahren aufgrund Bekundungen der betroffenen Kreise als gebannt anzusehen.[13] Dies zumal auch, weil die lebenslange Arztnummer (LANR), aber auch die Versichertennummern sehr leicht am Markt zu beschaffen sind. Damit können die angeblich anonymen Datensätze recht einfach und elektronisch mit Klardaten "synchronisiert" werden.

2.4 Anonymisierung und Nutzung in einer Hand?

Wird die Anonymisierung von demjenigen Verarbeiter vorgenommen, der selbst die Daten vor ihrer Anonymisierung zu recht verarbeitet hat, so kann der Aufwand einer De-Anonymisierung (genau genommen handelt es sich um eine "Onymisierung") dann nicht unverhältnismäßig sein, wenn er selbst die Anonymisierungsschlüssel oder die Klardaten behält. Ein derartiger Anonymisierungsbegriff kann jedoch - aber nur auf den ersten Blick - im Gesetz nicht gemeint sein, weil er vielleicht sinnlos wäre: Eine Anonymisierung könnte schlechterdings nur vorgenommen werden, wenn die Klardaten dabei oder unmittelbar und automatisch unaufhaltsam danach gelöscht würden.

Im vorliegenden Fall ist es allerdings keineswegs ausgeschlossen, dass der Gesetzgeber in § 300 Abs. 2 S. 2 SGB V die Verarbeitungsschritte (erste Alternative: strikte Zweckausrichtung, aber Klardaten; zweite Alternative: Zwecköffnung, aber anonyme Daten) als temporäre Stufen nacheinander angelegt und gemeint hat: Das würde heißen, dass das ARZ die Daten erst anonymisieren dürfte, wenn es unmittelbar danach die Klardaten löschen würde. Das hätte zur Folge, dass anonyme Daten das ARZ erst verlassen, wenn es keinen Schlüssel zur Deanonymisierung mehr im Besitz hätte.

Ganz fernliegend und unpraktikabel ist diese Überlegung keineswegs, weil alle Versichertenkennzeichen (Versichertennummer) und alle Arztkennzeichen (LANR) nach Durchführung und Erledigung der Abrechnung gelöscht werden können und - wegen des Grundsatzes der Datensparsamkeit nach § 3a BDSG -

[13] Die vorgenannten Gefahren sind real: Der Spiegel berichtete in 7/2012 unter der Überschrift "Kartell der Hehler" und 13/2012 unter der Überschrift "Kopieren Sie die Datei".

gelöscht werden müssen. Lediglich die Apothekenkennzeichen (Apotheken-ID) und die Krankenkassenkennzeichen müssen als "Geschäftsbriefe" im Sinne der Abgabenordnung, also aus steuerrechtlichen Gründen als Nachweise der Herkunft der Einkünfte, 12 Jahre aufbewahrt werden. Weil aber die Apotheken selbst insoweit aufbewahrungspflichtig sind, ist insgesamt eine Aufbewahrung im ARZ nicht zu erkennen.

Jedenfalls ergibt sich aus der Erkenntnis, dass derjenige Verarbeiter, der noch über die Klardaten verfügt, die Daten solange zumindest für sich selbst niemals anonymisieren kann, für die Belange eines wirksamen Datenschutzes eine naheliegende Gefahr: Wenn und solange Abrechnungsdaten patienten- oder arztbezogen im ARZ vorhanden sind, existiert die (näher oder ferner liegende, jedenfalls reale und lediglich nur relativ ausgeschlossene) Möglichkeit, dass eine Deanonymisierung der Daten ohne großen Aufwand möglich ist.

Werden die zunächst aus dessen Sicht anonymen Daten einem Nutzer überlassen, der diese zumindest nicht fern liegende Möglichkeit kennt und sie in dem Sinn zu nutzen imstande ist, sich die Klardaten im ARZ zu beschaffen, so ist sein Aufwand - mag er vorhanden sein - nicht unverhältnismäßig.

Von einer wirklichen Anonymisierung lässt sich also nur sprechen, wenn für den jeweiligen Nutzer die Klardaten nicht mehr zugänglich, am besten nicht und nirgends mehr vorhanden, sind. Ob dieses Zwischenergebnis unabweisbar die einzige Möglichkeit eines wirksamen Datenschutzes ist, ergibt sich aus dem, was folgt.

3 Der tatsächliche und rechtliche Inhalt von § 300 Abs. 2 S. 2 SGB V

Vorbemerkung

Unter Beachtung dieser allgemeinen Überlegungen wenden wir uns nun der Rechtsvorschrift und ihrer Auslegung in den Einzelheiten zu.

Bei der Auslegung von Rechtsvorschriften spielen deren Wortlaut und Kontext die zunächst entscheidende Rolle. Deshalb ist der gesamte Wortlaut der Vorschrift in den Blick zu nehmen.

3.1 Die Art und Weise, in der Apotheken über die von ihnen aufgrund einer entsprechenden vertragsärztlichen Verordnung vorgenommene Abgabe von Arzneimitteln an gesetzlich Krankenversicherte abzurechnen haben, ist in **§ 300 SGB V** geregelt. Die Vorschrift bestimmt insbesondere den dabei von den Apotheken dem Kostenträger zu übermittelnden **Datensatz**, also welche Daten je Verordnungs- und Abgabevorgang an die Krankenkasse zu übermitteln sind. Ferner erlaubt die Vorschrift den Apotheken, zur Durchführung der Abrechnung-Vorgänge die Dienste eines sogenannten ARZs in Anspruch zu nehmen.

Mit der betreffenden Vorschrift **verpflichtet** das Gesetz somit die Apotheken dazu, die betreffenden Daten an die Krankenkasse zu übermitteln, zugleich spricht das Gesetz damit, vor allem im Hinblick auf das von dem Apotheker zu wahrende **Patientengeheimnis**, aber auch eine **Erlaubnis** für diese Übermittlung aus. Dabei erlaubt das Gesetz den Apotheken nicht nur die Übermittlung an die Krankenkasse des betreffenden Versicherten, sondern – zu diesem Zweck – zugleich auch die Weitergabe des betreffenden Datensatzes an das **ARZ.**

In diesem Zusammenhang regelt die Vorschrift auch näher, **was dieses ARZ** – also ein auf diese Dienstleistungen spezialisiertes privatrechtliches Unternehmen – jeweils mit diesen Datensätzen, die ihm die Apotheken überlassen, **tun darf - und was nicht**. Denn die Vorschrift enthält auch dazu Aussagen. Diesen Aussagen lassen sich Angaben dazu entnehmen, was an Verarbeitung von Abrechnungsdaten von Apotheken im Zusammenhang mit ihrer Weitergabe von den Apotheken über die ARZ an die Krankenkassen gerade *nicht mehr* als Beeinträchtigung des **Persönlichkeitsrechtes** der Betroffenen, **in der besonderen Ausprägung des Rechtes auf informationelle Selbstbestimmung**, durch das Recht der Gesetzlichen Krankenversicherung bzw. die Rechtsordnung überhaupt *erlaubt* sein soll.

3.2 Der **Datensatz**, den die Apotheke übergibt, ist, bei grundrechtsbezogener Betrachtungsweise[14], ein auf ***vier*** **Personen** bezogener Datensatz. Für die *Zwecke der Fragestellung dieses Gutachtens vereinfacht*[15] hat er nämlich folgendem Inhalt:

---

[14] Die Krankenkasse als fünfter Beteiligter kann im Hinblick darauf – wie auch bei zivilrechtlich-persönlichkeitsrechtlicher Betrachtungsweise - vernachlässigt werden.

[15] *Tatsächlich* handelt es sich bei dem sog. *Verordnungsdatensatz* (§ 300 Abs. 3 Satz 1 Nr. 2 SGBV) um einen deutlich umfangreicheren Datensatz; nämlich um den aus 25 Datenfeldern bestehenden, gemäß § 5 der (auf der Grundlage von § 300 Abs. 3 SGB V zwischen den GKV-Spitzenverbänden und dem Deutschen Apothekenverband e.V. geschlossenen) „Vereinbarung über die Übermittlung von Arzneimittelabrechnung gemäß § 300 SGB V" - im Gesetz kurz Arzneimittelabrechnungsvereinbarung - gebildeten Datensatz, also das digitalisierte strukturierte Formular für den Inhalt der sog. Verordnungsblätter.

„Apotheke A hat das Medikament M des Herstellers H aufgrund der entsprechenden Verordnung vom Tage T_1 des Arztes B dem bei der Krankenkasse K Versicherten V zu einem bestimmten Zeitpunkt T_2 abgegeben“.
Der Datensatz sagt also etwas aus:
- über den versicherten Patienten V, dem das Medikament verordnet worden ist ,
- über den Arzt B, der das Arzneimittel verschrieben hat,
- über den Apotheker A, bei dem der Versicherte das Rezept eingereicht hat, und
- über den Hersteller H des Arzneimittels.

Es handelt sich bei den in diesem Datensatz enthaltenen Angaben mithin um **personenbezogene Daten**, die zugleich weitgehend unter das Arzt- und das **Apotheker-Geheimnis**, als die besonderen, **strafrechtlich** sanktionierten Geheimhaltungsverpflichtungen der Angehörigen dieser beiden Berufsstände, fallen.

In der datenschutzrechtlichen Terminologie sind diese vier Personen, auf die sich der Datensatz jeweils bezieht, sog. *Betroffene*. Als Ganzer stellt der Datensatz ein Datum mit Vierfachbezug dar.

3.3 Indem der Gesetzgeber die Übermittlung derartiger Daten vorschreibt und damit zugleich natürlich auch erlaubt, greift er in ein Grundrecht der genannten Personen, also der Versicherten, der Ärzte und der Apotheker ein, und wohl auch in eines desjenigen Unternehmens (Art. 19 Abs. 3 GG), welches das betreffende Arzneimittel hergestellt hat. Es handelt sich um das **Grundrecht auf informationelle Selbstbestimmung**, auch **Datenschutz**-Grundrecht genannt.

In erster Linie betrifft dieser Grundrechtseingriff des Gesetzgebers natürlich das **Persönlichkeitsrecht des Patienten**. Denn bei diesem geht es um Informationen über seinen Gesundheitszustand, die mit sehr hoher Wahrscheinlichkeit aus der ärztlichen Verordnung erschlossen werden können, und damit um Informationen, deren Geheimhaltung durch die an dem Vorgang von Diagnose und Therapie beteiligten Berufs-Träger von der Rechtsordnung besonders geschützt ist und die namentlich anders als bei den auch betroffenen anderen Beteiligten nicht der bloßen Berufs-Sphäre zuzuordnen sind. Aber auch das **Persönlichkeitsrecht des Arztes** ist betroffen, weil seine Diagnose- und Verordnungs-Handlung, als (aus einem breiten Spektrum von Möglichkeiten gewählte) Therapie-Entscheidung, die der Datensatz indirekt bzw. unmittelbar wiedergibt, faktisch einen hohen Freiheitsgrad genießt und deswegen ihn in ausgesprochen starkem Maße hinsichtlich der Art und Weise seiner Ausübung des Arztberufes kennzeichnet. Dieser Schutz gilt zudem jedem Apotheker.

3.4 Weil er mit der Regelung des Abrechnungs-Verfahrens somit tief in die Grundrechte auf informationelle Selbstbestimmung, als Bestandteil des verfassungsrechtlichen Persönlichkeitsrechtes, eingreift, ist der Gesetzgeber von Verfassungs wegen verpflichtet, bei der Gestaltung der einschlägigen Vorschrift so genau wie möglich zu bestimmen, welche Daten-Verarbeitungs-Handlungen – vor allem, aber eben keineswegs nur betreffend Daten über den versicherten Patienten – erlaubt sein sollen und welche nicht (verfassungsrechtliches Bestimmtheitsgebot).

Bei der Ausgestaltung dieser von ihm zu treffenden Bestimmungen hat der Gesetzgeber wegen seiner verfassungsrechtlichen Pflicht zum Schutz der Grundrechte insbesondere auch Gefährdungen des Rechtes auf informationelle Selbstbestimmung, mit denen im Hinblick auf die von ihm - wie im Falle der Arzneimittelabgabe-Abrechnung - veranlassten Verarbeitungsvorgänge zur rechnen ist, in den Blick zu nehmen, zu beachten und Vorkehrungen gegen sie zu treffen.

Mit solchen Gefährdungen hat, wie sich nachfolgend zeigen wird, der Gesetzgeber offensichtlich im Falle der durch § 300 SGB V angeordneten Datenverarbeitungsvorgänge auch tatsächlich gerechnet (und also offenbar rechnen zu müssen gemeint).

4 Sedes materiae: § 300 Abs. 2 Satz 2 SGB V

Die nach den bisherigen Feststellungen erforderlichen Bestimmungen hat der Gesetzgeber in Abs. 2 Satz 2 des § 300 SGB V getroffen.

4.1 Diese Vorschrift lautet, und zwar seit dem 23. Februar 2002[16], folgendermaßen:

Die ARZ dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke und ab dem 1. Januar 2003 nur in einer auf diese Zwecke ausgerichteten Weise verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind;

Dem folgt ein 2. Halbsatz, der folgendermaßen lautet:

[16] Letzte Änderungen durch Artikel 1 des Gesetzes zur Begrenzung der Arzneimittelausgaben der gesetzlichen Krankenversicherung (Arzneimittelausgaben-Begrenzungsgesetz – AABG) vom 15. Februar 2002, BGBl. I S. 684, gemäß Art. 4 am 23. Februar 2002 in Kraft getreten.

anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.

4.2 Wesentlicher Inhalt des **ersten Halbsatzes** ist eine begrenzte Verarbeitungs-**Erlaubnis**. Dabei wird diese Erlaubnis in dreierlei Hinsicht **begrenzt**:

4.2.1 Die *erste Begrenzung* ist eine datenschutzrechtstypische Begrenzung der Erlaubnis, nämlich die übliche, über die Voraussetzungen der *Erforderlichkeit und Geeignetheit zur Erreichung bestimmter Zwecke* bewerkstelligte **Bindung an** in nicht-datenschutzrechtlichen Vorschriften **gesetzlich bestimmte Zwecke**, hier die durch das SGB bestimmten (nicht-datenschutzrechtlichen) Zwecke. Solcher Zweck ist vor allem die Durchführung der angeordneten Verfahrensweise der Abrechnung der Apotheken gegenüber den Krankenkassen.

Allerdings fällt an dieser Zweck-Vorgabe für die Verarbeitungsvorgänge das ungewöhnliche Fehlen des Wörtchens „nur" (das an anderer Stelle durchaus folgt) auf: Ausnahmsweise ist diese Zweckvorgabe **nicht abschließend**. Anders ausgedrückt ist dieser ersten Begrenzung zufolge die Bezogenheit auf den in ihr genannten Zweck der Datenverwendung - nämlich Zwecke der Erfüllung von Verarbeitungspflichten, die sich aus dem SGB ergeben - noch nicht notwenige Voraussetzung der Erlaubtheit jeglicher Verarbeitungen (sc. dieser Daten) durch das ARZ. Es deutet sich also schon in diesem Satz an, dass zusätzlich die Verarbeitung zu anderen Zwecken zulässig, also - selbstverständlich in einem noch zu bestimmenden Maße! - dem ARZ erlaubt sein könnte.

4.2.2 Die im „Soweit"-Satz, am Schluss des Halbsatzes, vorgenommene *zweite* Begrenzung, nämlich die **Bindung an den Auftrag**[17] des Auftraggebers, ist nicht ungewöhnlich: Sie spricht diejenige Begrenzung aus, die für die **Datenverarbeitung im Auftrag** spezifisch ist (vgl. etwa § 11 Abs. 2 Satz 2 Nr. 9, Abs. 3 Satz 1 BDSG und, dort etwas anders geregelt , § 80 Abs. 2 Satz 2 Nr. 9, Satz 3 und Abs. 4 SGB X).

Somit stellt dieser Teil der Vorschrift zunächst einmal allem Anschein nach klar, dass es sich bei dem Verhältnis zwischen den Apotheken und dem von ihnen im Rahmen des § 300 Abs. 1, Abs. 2 Satz 1 SGB V eingeschalteten sog. ARZ daten-

[17] Vorsorglich sei darauf hingewiesen, dass „Auftrag" hier ein spezieller terminus des Datenschutzrechtes ist, das insoweit von der (allgemeinen) Terminologie des Zivilrechtes abweicht. Im Sinne des BGB handelt es sich in aller Regel um Werkvertrag.

schutzrechtlich um ein **Auftragsdatenverarbeitungsverhältnis** handelt – wie es jedenfalls einhellige Auffassung der Literatur ist[18], soweit sie sich zu dieser Frage äußert.

Zum anderen begrenzt dieser Passus die dem ARZ im Gesetz erteilte Verarbeitungserlaubnis in der für die Datenverarbeitung im Auftrag spezifischen Weise auf diejenigen Verarbeitungsvorgänge bzw. denjenigen Verarbeitungsumfang, die bzw. den der Auftraggeber[19] beim Auftragnehmer in Auftrag gibt, also werkvertragsrechtlich gesprochen beim Auftragnehmer „bestellt".

Das bedeutet: Auf Grund dieser Vorgabe darf das ARZ keinerlei Verarbeitung auf der Grundlage des 1. Halbsatzes durchführen, die nicht von den Apotheken oder den insoweit gesetzlich dazu ermächtigten Datenempfängern, die das Gesetz anscheinend nicht als Auftraggeber innerhalb eines Auftragsdatenverarbeitungsverhältnisses, sondern als aus anderen Gründen (gesetzlicher Anspruch aus dem SGB) dazu berechtigt ansieht, berechtigterweise von ihnen verlangt werden.

4.2.3 Gänzlich ungewöhnlich, ja vermutlich einmalig[20] im deutschen Datenschutzrecht ist dagegen die zusätzliche, - im Gesetzestext als zweite genannte - *dritte Begrenzung,* die dem 1. Halbsatz zu entnehmen ist. Sie stellt eine **verschärfte Formulierung des** datenschutzrechtsüblichen, ja das Datenschutzrecht prägenden **Zweckbindungs-Gebotes** dar. Die Verschärfung kommt zum einen schon dadurch zum Ausdruck, dass diese Zweck-Bindung zu derjenigen, die bereits in der ersten Begrenzung ausgesprochen ist, hinzukommt – die *Zwecke* der Verarbeitung werden ja ein zweites mal als maßgeblich erwähnt. Und zum anderen darin, dass diese zusätzliche, **zweite Zweckbindung** schon die „Ausrichtung" der Verarbeitung be-

---

[18] Allerdings entgegen Kranig in Hauck/Noftz SGB V Rdnr. 10 zu § 300 nicht eine unter § 80 SGB X, sondern eine unter § 11 BDSG fallende Auftragsdatenverarbeitung (zutreffend U. Schneider in: Kraushaar, Soziale Krankenversicherung/Pflegeversicherung, Stand Nov. 2011, Rdnr. 8 zu § 300 SGSB V).

[19] Zu Vereinfachungszwecken sei hier vernachlässigt, dass das Gesetz sich nicht auf die Apotheken als Auftraggeber der ARZ beschränkt, sondern, wie oben im Text nachstehend erwähnt, auch vorsieht, dass andere Stellen – ausschließlich kraft des SGB – dem ARZ Weisungen erteilen können, bestimmte Verarbeitungshandlungen vorzunehmen. Das betrifft ersichtlich die Übermittlungsempfänger nach § 300 Abs. 2 Satz 3 bis 6 SGB V sowie auch Anforderungen, welche die Krankenkassen aussprechen können.

[20] Einmalig, wenn man von dem weitgehend ganz gleichgelagerten und vom Gesetzgeber entsprechend weitgehend wortgleich geregelten Parallelfall des § 302 Abs. 2 Satz 3 SGB V (Rechenzentren der Leistungserbringer im Bereich Heil- und Hilfsmittel) absieht.

stimmen und damit auch diese begrenzen, nämlich die Gesamtheit der Verarbeitungsumstände („Weise“) prägen soll.

Darin hat man allem Anschein nach ein vom Gesetzgeber ausnahmsweise für erforderlich gehaltenes, vorsorgliches, besonderes und deutliches Gebot zu sehen, die Verarbeitungsvorgänge in jeder Hinsicht, auch die Zwischenschritte und Modalitäten der Ausgestaltung der Verarbeitungsvorgänge, anders als sonst vorgeschrieben ausschließlich in der Weise auszugestalten, dass die vom SGB vorgegebenen Zwecke optimal erfüllt werden können, und nicht etwa bei ihrer Ausgestaltung Rücksicht auf andere, hinzukommende Verarbeitungszwecke zu nehmen. Anders ausgedrückt: Das Gesetz **verbietet für die gesamte Ausgestaltung der auf der Grundlage des 1. Halbsatzes stattfindenden Verarbeitungsvorgänge** im ARZ eine solche **Berücksichtigung anderer Verarbeitungszwecke**.

Die Zeitbestimmung, die für diese zweite Begrenzung gilt – nämlich ab 1. Januar 2003 – , zeigt, auch ohne in einen näheren Blick in die Gesetzgebungsgeschichte notwendig zu machen, dass der Gesetzgeber diese Begrenzung nachträglich und aus gegebenen Anlass eingefügt hat, also deswegen, weil bis dahin anders verfahren worden war.

Dieses Allein-Ausrichtungs-Gebot lässt sich zwanglos auch als besondere Ausprägung des Datensparsamkeitsgebotes der §§ 3a BDSG, 78b SGB X verstehen. Eine Auslegung, die diesem Allein-Ausrichtungs-Gebot keine eigenständige Bedeutung gegenüber dem Inhalt des 2. Halbsatzes (an dieser Stelle höchst vereinfacht kurz: Anonymisierungs-Gebot) zukommen ließe, wäre mit dem Gesetzeswortlaut nicht vereinbar. Denn sie hielte einen Teil des Gesetzeswortlautes ohne Grund für funktions- und damit sinnlos, und sie verkennte, dass dies Gebot im 1. Halbsatz und nicht im 2. Halbsatz steht.

4.3 Diese besondere, hier als dritte aufgeführte Vorgabe des 1. Halbsatzes ist nun allerdings nichtsdestoweniger im *Zusammenhang* mit dem folgenden 2. Halbsatz zu sehen, in dem in der Tat nun doch **zusätzliche Verarbeitungszwecke**, also Verarbeitungszwecke neben denjenigen, die sich aus dem SGB ergeben, erwähnt werden - wie es das fehlende „nur“ in der ersten Vorgabe des 1. Halbsatzes ja schon hat vermuten lassen: So streng die Zweckbindung mit besonders schutzwürdigen Daten und die Weisungsbindung im ersten Teil der Vorschrift ist, umso freier ist das ARZ bei der (Er-)Findung von Zwecken in eigener Regie - allerdings eben nur mit anonymisierten Daten. **Diese "Symmetrie" der Vorschrift ist auffällig. Sie legt die Gewichte.**

5 Der zweite Halbsatz des § 300 Abs. 2 Satz 2 SGB V: Anonymisierung

5.1 Der zweite Halbsatz des § 300 Abs. 2 Satz 2 SGB V stellt eine **Erlaubnis** dar. Er erlaubt dem ARZ, solche Daten, die die Eigenschaft haben, „**anonymisiert**“ zu sein, für beliebige (andere) Zwecke zu verwenden, also für **Zwecke außerhalb des SGB**, und damit insbesondere außerhalb der Verwendung von Arzneimittel-Abrechnungsdaten zu den im SGB V vorgesehenen Verwendungszwecken. Diese Zweck-Freigabe bedeutet auch, eben wegen der auch freigegebenen Verfügbarkeit und Übermittlungsmöglichkeit, dass es beliebig neue Datenempfänger und -Verarbeiter, wo auch immer, geben darf. Welche Beschaffenheit Daten haben müssen, um im Sinne des § 300 Abs. 2 Satz 2, 2. Halbsatz SGB V anonymisiert zu sein – und damit eben einer freien Verwendung zugänglich zu sein -, ist dem allgemeinen Gesetz zu entnehmen. Einschlägig ist allerdings nicht die in § 67 Abs. 8 SGB X enthaltene Legaldefinition des Begriffes „Anonymisieren“. Denn diese bezieht sich nur auf *Sozialdaten* im Sinne des *Abs. 1* der Vorschrift, und weder die Apotheken noch deren ARZ fallen, wie dort vorausgesetzt, unter die in § 35 SGB I genannten Stellen. Statt dessen ist der begriff des Anonymisierens der Legaldefinition des § 3 Abs. 6 BDSG zu entnehmen, die sich von derjenigen des § 67 Abs. 8 SGB X allerdings nur dadurch unterscheidet, dass sie sich auf personenbezogene Daten allgemein bezieht statt nur auf solche, die Sozialdaten sind. Diese Vorschrift lautet:

„Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“

5.2 Somit dürfen die Daten, deren Gewinnung und Weiterverwendung zu *beliebigen* Zwecken § 300 Abs. 2 Satz 2, 2. Halbsatz SGB V erlaubt, (auch) „**Einzelangaben**“[21] sein, also *individualisierte* Daten, d.h. Daten, die sich auf einen Sachverhalt beziehen, der an und für sich, sachlich, auf einen einzelne Person bezogen ist, die aber in ihren gesamten Angaben[22] - eben auch mittelbar über den Sachverhalt - keine Angaben enthalten, die eine Bestimmung der Identität dieser Person erlauben. Darunter fallen auch Daten, die mehrere Vorgänge oder sonstige Umstände zusammenfassen, die alle ein und dieselbe Person betreffen.

---

[21] Es handelt sich um denselben terminus und auch denselben Begriff wie im Statistikrecht, namentlich in den Bestimmungen des BStatG über das Statistikgeheimnis (§ 16 BStatG).

[22] Daten sind (verkörperte) Angaben über Sachverhalte.

Mit anderen Worten: In diesem, eben datenschutzrechtlichen, Sinne anonymisierte Daten müssen nicht aggregierte Daten sein, also nicht tabellarische Gestalt haben. Der schematische Inhalt tabellarischer, datenschutzrechtlich personenbezugsfreier aggregierter Datensätze ist: Auf n Personen trifft zu, dass bei ihnen die Merkmalsausprägung P_1 vorliegt, mit n größergleich 3. Diese Größenbegrenzung ergibt sich aus dem Statistik-Datenschutzrecht [23].

In diesem Sinne anonymisierte Daten dürften also – um es konkreter im Hinblick auf die Daten von ARZ zu formulieren – die Datensatz-Gestalt haben:
"Zum Zeitpunkt t_1 hat irgendein bestimmter Arzt irgendeinem bestimmten Versicherten das Medikament M verordnet, der es zum Zeitpunkt t_2 in irgendeiner bestimmten Apotheke abgeholt hat" unter der Voraussetzung, dass der Personenbezug auf den Hersteller des Arzneimittels M im Wege einer teleologischen Reduktion der Vorschrift oder jedenfalls deswegen[24] vernachlässigt werden könnte, weil die Daten nur dem betreffenden Hersteller übermittelt werden, dessen eigenes Datum es ist.

Es wird noch zu zeigen sein (s. unten 6.3.3), dass auch ein derartiger Datensatz wegen seiner möglichen Bezogenheit auf natürliche Personen als Arzneimittel-Hersteller problematisch ist. Übrigens dürfte der Datensatz auch neben den Daten, die beim Pharma-Großhandel aus seiner Geschäftstätigkeit ohnehin anfallen, wohl uninteressant sein.

Erlaubt wäre jedoch – fehlende Identifizierungsmöglichkeit für jeden Dritten unterstellt - ein Datensatz mit dem Inhalt: *„Es gibt einen Arzt, der im Zeitraum Z das Medikament M n-mal verschrieben hat."*
Oder: *„Es gibt einen Arzt, dessen Verordnungen im Zeitraum Z in n Apotheken eingereicht worden sind, wobei auf Apotheke A_1 m_1 Prozent, auf Apotheke A_2 m_2 Prozent entfallen usw."*

---

[23] Letzteres ist nicht Voraussetzung der Aggregierung(sform) als solcher, sondern Gebot der Wahrung des Statistikgeheimnisse, also des Datenschutzes, wobei die Mindestgröße 3 eine anerkannte Faustregel für die Vermeidung von Personenbezug für Datenempfänger jedweder Art ist. Tabellen mit Tabellenfeldwerten kleinergleich 2 dürfen, wenn es sich um Statistiken über Sachverhalte handelt, an denen (auch: juristische) Personen beteiligt sind, veröffentlicht werden, wenn der zu kleine Tabellenwert (0 bis 2 also) in eine unbestimmte Angabe umgewandelt, also etwa durch die Angabe"*" ersetzt wird.

[24] Die Begründung statt dessen darauf zu stützen, dass es in den einschlägigen Vorschriften nur um Bezug auf *natürliche Personen* gehe, erfaßt nicht per se alle Hersteller von Arzneimitteln siehe oben im Text die nachstehenden Ausführungen.

Das sind vom Gesetz im 2. Halbsatz grundsätzlich erlaubte Datensätze mit *Einzel-Angaben*.

5.3 Aber: Diese Einzel-Angaben enthaltenden, d.h. sie formulierenden Datensätze müssen **anonymisiert** (worden) sein. Das ist in zweierlei Hinsicht von Bedeutung:

5.3.1 *Zum einen* für die **Übermittlungstätigkeit** des ARZ, also für die Daten, die das ARZ auf der Grundlage des 2. Halbsatzes an Dritte **herausgibt**. Diese Daten sind nur dann „anonymisiert", wenn sie weder mit Hilfe vom ARZ hinzugefügter Identifikatoren noch aufgrund der im Datensatz enthaltenen Kombination von Merkmalsausprägungen demjenigen, der über das Datum, also über den Datensatz mit der Einzelangabe, verfügt, es auch mit Zusatzwissen ermöglichen, herauszubekommen, auf welche (natürliche) Person sich die Einzelangabe bezieht.

Die **Verantwortung**, dies und damit die Rechtmäßigkeit einer Datenweitergabe auf der Grundlage des 2. Halbsatzes zutreffend zu beurteilen, **liegt** naturgemäß beim Handelnden, und das ist zunächst das **ARZ**[25]. Die ARZ müssen also, wenn sie rechtswidrige[26] und strafbare Daten-Verwendungen in Gestalt von Übermittlungen von nach dem 2. Halbsatz verarbeiteten Daten vermeiden wollen, sich selbst kundig machen, wie die Dateninteressenten (Daten-Käufer) oder deren Dritt-Abnehmer die Daten wohl verwenden können werden, insbesondere welches Zusatzwissen sie haben oder sich beschaffen können.

Mit anderen Worten: Welches Zusatzwissen bzw. welche Zuordnungs-Möglichkeit bei möglichen Empfängern bestehen, muss derjenige, der Daten weitergibt, selbst einschätzen, und er muss sich dabei **auf der sicheren Seite** halten, wenn er nicht seiner Tätigkeit als ARZ gewerberechtlich wegen **Unzuverlässigkeit** verlustig gehen, sich nicht **bußgeldpflichtig** machen und bei Vereinbarung von Entgelten für die Datenweitergabe sich nicht **strafbar** machen will. Ein Beispiel dafür: Gibt ein Dateninteressent an, er wolle die (feingegliederten) Einzelangaben ausschließlich zu Zwecken einer statistischen Auswertung haben, sollte im Zweifelsfall das ARZ

---

[25] Weiter dazu unten Abschnitt 7.

[26] Für die Rechtswidrigkeit des Handelns (Folge: Unterlassungsansprüche, Schadensersatzansprüche mit Entlastungsmöglichkeit, vor allem aber Unzuverlässigkeit als Auftragsdatenverarbeiter, also Wegfall der Tätigkeit für die betreffenden Apothekerverbände, erzwingbar durch die Aufsichtsbehörden) desjenigen, der die Daten weitergibt, reichen die objektiven Gegebenheiten, für die Bußgeldpflichtigkeit (§ 43 Abs. 2 Nr. 1 BDSG) die Fahrlässigkeit und für die Strafbarkeit (im Falle der entgeltlichen Weitergabe, § 44 Abs. 1 BDSG) reicht der bedingte Vorsatz, also in der Sprache des juristischen Laien die Gleichgültigkeit (Wurschtigkeit).

sicherheitshalber die statistische Auswertung selbst vornehmen (was nicht notwendig mit zeitweiligem Lizenzerwerb verbunden sein muss, denn auch die Überlassung des Auswertungsprogramms zur eingekapselten Verwendung ist möglich).

Inwieweit diese Deanonymisierungs-Möglichkeit für einen möglichen Datenempfänger besteht, die rechtlich gesehen (schon) das übermittelte Datum unanonymisiert, d.h. personenbezogen sein läßt, bestimmt sich jeweils nach den – verschiedenen! – Verhältnissen desjenigen, der das Datum hat, dem es vorliegt. Dies ist der Grundgedanke des – zutreffenden – sog. **relativen Personenbezugs-Begriffes.** Der demgegenüber vielfach vertretene und **strengere sogenannte absolute Personenbezugs-Begriff** führte demgegenüber zu einer über den Schutzzweck des Datenschutzrechtes hinausschießenden und daher ebenso unsinnigen wie verfassungswidrigen Anwendung des Datenschutzrechtes auf Daten, deren Kenntnis keinerlei Gefährdung des Persönlichkeitsrechtes mit sich bringen – eben weil die Daten zwar individualisiert, aber gleichwohl gerade nicht personenbezogen sind. Allerdings kommt im Hinblick auf die Wahrscheinlichkeit freien Handels mit gegebenenfalls von ARZ irgendwelchen Dritten abgegebenen Daten der Unterschied zwischen diesen beiden Personenbezugs-Begriffen vorliegend nicht zum Tragen.[27] Dies insbesondere dann nicht, wenn die möglichen (und nun schon erfahrenen) gefahren realistisch eingeschätzt werden.

Daten, welche die ARZ nach dem 2. Halbsatz übermitteln dürfen, dürfen außer einer laufenden Nummer keine Pseudonyme enthalten. Die bloße Verschlüsselung von Original-Pseudonymen (Arztnummer) oder von sonst sprechenden Pseudonymen wäre gefährlich, weil eine Entschlüsselung nicht ausgeschlossen werden kann (konkreter dazu unten 6.3.4). Zudem muss die Sortierung ausgegebener Einzeldatensätze in einer Reihenfolge zufällig sein und darf keine Erkenntnismöglichkeiten für mögliche Datenempfänger mit sich führen. Werden diese Regeln eingehalten, dürfte kein Empfänger einer Liste von Einzeldatensätzen von dieser Liste einen Nutzen haben können.

5.3.2 *Zum anderen* gilt das Anonymisiertheits-Erfordernis für die **Speicher-Tätigkeit** des ARZ, also für einen zusätzlichen, zweiten Datenbestand, den sich das ARZ auf der Rechtsgrundlage des 2. Halbsatzes gegebenenfalls aufbaut. Ohne einen solchen anonymisierten gespeicherten **Sekundär-Datenbestand** darf das ARZ auf der Grundlage des 2. Halbsatzes nur ad hoc aus dem Primär-Datenbestand Auszüge herstellen, diese sofort übermitteln und bei sich umgehend löschen, darf es also auf der Grundlage des 2. Halbsatzes nicht speichern.

[27] Der Hinweis auf diesen Unterschied soll nur erkennbar machen, dass dem vorliegenden Gutachten nicht etwa insoweit eine besonders strenge Auffassung zugrundeliegt.

Inwieweit in einem solchen Sekundär-Datenbestand von Dritten oder interne, also vom ARZ vergebene, Pseudonyme zulässig sind, wird noch zu prüfen sein. Ausgeschlossen ist aber sicherlich, dass dieser Sekundär-Datenbestand Klarnamen oder andere unmittelbare oder auch nur mittelbare offene Identifikatoren enthalten darf.

Zu beachten ist auch, dass das ARZ nicht etwa Daten seines Primär-Bestandes speichern darf, die es nach dem 1. Halbsatz, also für SGB-Zwecke, nicht mehr benötigt (also zu löschen hat).

6 Auslegung des 2. Halbsatzes des § 300 Abs. 2 Satz 2 SGB V

Aus den bisherigen Ergebnissen ergeben sich Folgerungen für eine differenzierte Auslegung der Vorschrift:

6.1 Die vom Gesetz im 2. Halbsatz erlaubten Einzelangaben, die keine *natürlichen* Identifikatoren (Namen; indirekter: Anschriften) mehr enthalten, sind für das ARZ selbst gar nicht anonymisiert in diesem Sinne. Das wird vor allem dann[28] deutlich, wenn das ARZ einen längerfristig vorgehaltenen *Sekundär-Datenbestand* aufbaut, der für sich genommen gemäß dem 2. Halbsatz anonymisiert ist. Denn in diesem Fall verfügt das ARZ zugleich ja, in seinem Primär-Datenbestand, auch über die (ihm von den Apotheken übermittelten und von ihm im Rahmen des SGB auch personenbezogen zu verwendenden) mit natürlichen Identifikatoren versehenen Datensätze (Daten), aus denen es die identifikatorenlosen Daten erst gewonnen hat. Das ARZ kann – zumindest in den allermeisten Fällen – im Wege einer Rückverfolgung zu diesen identifikatorenlosen Daten die ursprünglichen Ausgangsdaten finden, und zwar ohne großen Aufwand. Das gilt so lange, wie die Ausgangsdaten, aus denen die Sekundär-Daten gewonnen sind, nicht vollständig gelöscht oder jedenfalls selbst vollständig anonymisiert sind. Deswegen sind insoweit die Daten, die das ARZ nach dem 2. Halbsatz verarbeiten dürfen soll, für es selbst, also, solange sie sich bei ihm befinden, gar nicht „anonymisiert“ im Sinne der genannten Legaldefinitionen.

Ist das jedenfalls so lange der Fall, wie die entsprechenden Daten im Ausgangs-Datenbestand noch nicht gelöscht oder doch anonymisiert sind, dann gibt es eigent-

[28] Es gilt aber *immer* dann, wenn die anonymisierten Daten vom ARZ selbst aus den ihm auf Grund und gemäß der Arzneimittelabrechnungsverordnung von den Apotheken übermittelten Daten gewonnen werden. Denn zumindest für eine kurze Zeit (logische Sekunde vor einer Löschung der Primär-Daten) hat das ARZ beide Daten.

lich gar keine unter den 2. Halbsatz fallende Verarbeitung, dann läuft der 2. Halbsatz leer und ist legislatorischer Unsinn[29], nämlich in sich widersprüchlich. In Anbetracht dessen ist eine Gesetzesauslegung geboten, die dafür sorgt, dass der 2. Halbsatz gerade nicht leerläuft, sondern eine sinnvolle (wenn auch, wie wir sehen werden, sehr eingeschränkte) Regelung enthält. Als eine solche Auslegung drängt sich auf, dass das Anonymitäts-Gebot, oder genauer gesagt, das Anonymisiertheits-Gebot, für diejenigen Daten, die vom ARZ zu anderen, SGB-fremden Zwecken verwendet werden dürfen, für das ARZ selbst nicht in voller Strenge gilt (sondern nur bei – für das ARZ selbst eben fiktiver - isolierter Betrachtung des von zumindest den natürlichen Identifikatoren freien Datenbestandes, den das ARZ gegebenenfalls zusätzlich aus seinem ursprünglichen Datenbestand gewonnen hat, eben auf der Grundlage des 2. Halbsatzes). Ein solches Verständnis der Norm führt nicht zu einer Beeinträchtigung des Persönlichkeitsrechtes, denn das ARZ als der „Verarbeiter“[30] verfügt ja ohnehin über die betreffenden personenbezogenen Daten. Dass das ARZ gegebenenfalls einen länger vorgehaltenen zweiten Datenbestand aufbaut, der wegen der Verfügung über den ursprünglichen Datenbestand für den „Verarbeiter“ – mit nicht allzu hohem Aufwand – ebenfalls personenbezogen ist, beeinträchtigt das Persönlichkeitsrecht der Betroffenen nicht nennenswert.

Diese Auslegung[31] des 2. Halbsatzes läuft kurz gesagt darauf hinaus, dass die Vor-

---

[29] Es sei denn, der Anonymisierung schließt sich unmittelbar und vor der Weitergabe des Sekundärdatenbestandes die Löschung des Primärdatenbestandes an.

[30] Das ARZist, auf Grund einer Art Fiktion, mit der das Rechtsinstitut der Auftragsdatenverarbeitung arbeitet, nicht im technischen Sinne des Datenschutzrechtes Verarbeiter im Außenverhältnis zum Betroffenen. Faktisch und im Hinblick auf andere Rechtsbeziehungen, zum Beispiel zur Datenschutzkontrollbehörde, ist das ARZ natürlich gerade selbst Verarbeiter (im weiteren Sinne).

[31] Es handelt sich um die am häufigsten vertretene Rechtsmeinung: Im Ergebnis im wesentlichen wie hier, wenn auch ohne Begründung und ohne Auseinandersetzung mit der Gegenmeinung, Kranig in Hauck/Noftz SGB V, Stand Juni 2008, Rdnr. 11 zu § 300; zumindest der Tendenz nach („relative Anonymisierung“ im Hinblick auf den möglichen Verarbeitungszweck berufspolitische Interessenvertretung der Apotheker) auch U. Schneider in: Kraushaar, Soziale Krankenversicherung/Pflegeversicherung, Stand Nov. 2011, Rdnr. 10 zu § 300 SGB V.
Nicht genau einzuschätzen, aber vermutlich auch in diese Richtung gehend Hess im Kasseler Kommentar zum Sozialversicherungsrecht Rdnr. 4 zu § 300 SGB V mit der allerdings nicht ganz eindeutigen Formulierung „Die Verarbeitung anonymisierter Daten für andere Zwecke bleibt zulässig“ (sein ergänzender Hinweis auf die BT-Ausschußberatungen ist in sich zu der Frage, wer die anonymisierten Daten herstellen bzw. liefern darf, nicht aussagekräftig).

schrift implizit eine[32] **Erlaubnis** für das ARZ enthält, die ihm nach § 300 Abs. 1 SGB V übermittelten (personenbezogenen) Daten dazu zu **nutzen**, aus ihnen Daten zu gewinnen, die abgesehen von den Erkenntnismöglichkeiten, die das ARZ deswegen hat, weil es zugleich über die Klar-Daten verfügt, anonymisiert sind. Die in der Literatur ebenfalls vertretene *gegenteilige Auffassung*, der zufolge das ARZ auf der Grundlage des 2. Halbsatzes nur Daten speichern und nutzen sowie übermitteln darf, die ihm (schon) anonymisiert (vermutlich gemeint ja doch: von den Apotheken) übermittelt worden sind[33], vermag auch aus anderen Gründen als denjenigen des Leerlaufens der Vorschrift nicht zu überzeugen.[34]

6.2 Uneingeschränkt gelten die **Anonymisierungs-Anforderungen** jedoch für alle anderen möglichen Empfänger der im 2. Halbsatz zur zusätzlichen Verarbeitung (im engeren Sinne der §§ 3 Abs. 4 BDSG, 67 Abs. 6 SGB X), also vor allem auch zur Übermittlung und zur Nutzung, durch das ARZ zugelassenen Daten. Es sind gerade diese anderen möglichen Empfänger - also die Verarbeitungshandlung der Übermittlung an sie -, auf die das Anonymisierungs-Erfordernis des 2. Halbsatzes zielt. Deswegen dürfen die ARZ zu anderen als den im SGB genannten Zwecken und den betreffenden dazu im SGB genannten Stellen, also auf der Grundlage des 2. Halbsatzes und damit überhaupt **an SGB-Außenstehende, keine Daten**

---

[32] Nämlich eine vom Gesetzgeber nicht für nötig gehaltene oder in ihrer Notwendigkeit übersehene zusätzliche Erlaubnis. Erfahrungsgemäß wird die Notwendigkeit von Nutzungserlaubnissen für die Pseudonymisierung oder die Anonymisierung in der datenschutzrechtlichen Praxis recht häufig übersehen.

[33] So, allerdings ohne nähere Begründung, Michels in Becker/Kingreen, Rdnr. 4, zwar nicht zu § 300 Abs. 2 Satz 2 (dort enthält die Kommentierung keine Ausführungen zu dieser Frage), aber zum insoweit gleichgelagerten § 302 Abs. 2 Satz 3 SGB V.

[34] a) Die Erhebung und Weiterverarbeitung von Daten, die für den Verarbeiter wirklich anonym sind, ist mit Ausnahme der Weitergabe an solche Dritte, für die sie nicht mehr anonymisiert wären (weil sie im Unterschied zum Übermittler die nötigen Deanonymisierungsmöglichkeiten hätten), datenschutzrechtlich irrelevant und nicht erlaubnisbedürftig[34].

b) Nimmt man demgegenüber die auf nichtpersonenbezogene Daten sich beziehende Erlaubnis des 2. Halbsatzes insofern ernst, dass sie zugleich das verbietet, was sie nicht an Umgang mit anonymisierten Daten erlaubt, dann muss man auch das Fehlen einer Erlaubnis der *Erhebung* ernst nehmen.

c) Die oben unter 2.2.3 erörterte besondere Begrenzung der *Ausrichtung* der aufgrund des 1. Halbsatzes stattfinden Verarbeitung zeigt gerade, dass der Gesetzgeber davon ausgegangen ist, dass das ARZ gerade seine Primär-Daten noch anderweitig nutzen wird, also auch darf, d.h. es ihm nicht vollständig verboten sein soll. Diese zusätzliche Begrenzung der Verarbeitung nach dem 1. Halbsatz wäre daher sinnlos, wenn ohnehin vollständig verboten wäre, die Daten zu anderen Zwecken zu nutzen.

herausgeben, die der Empfänger oder auch nach einer etwaigen Weiter-Übermittlung jeder mögliche Dritt-Empfänger auf Grund ihm zu Gebote stehenden - also auch mit angemessenem, sinnvollem Aufwand beschaffbaren – Zusatzwissens, oder etwa auch durch Anwendung mathematisch-statistischer Methoden der Rückrechnung, wieder einzelnen Ärzten oder Apotheken zuordnen kann, von Versicherten ganz zu schweigen.

6.3 Betrachtet man nun den Inhalt der Datensätze, die der von den ARZ gegebenenfalls aufgebaute Sekundärbestand haben darf, sowie die möglichen Empfänger der von den ARZ auf der Grundlage der Erlaubnis des 2. Halbsatzes erarbeiteten (zusätzlichen) Daten, ergibt sich folgendes:

6.3.1 Zunächst einmal hat das ARZ schon die nach dem 1. Halbsatz ab dem 1. Januar 2003 einzuhaltende – zusätzliche - Beschränkung der Verarbeitung der Primär-Daten auf eine auf die SGB-bestimmten Zwecke ausgerichteten Verarbeitungs- und Nutzungsweise zu beachten (oben 4.2.3). Diese gesetzliche Vorgabe geht ersichtlich auf eine dem Gesetzgeber bekannt gewordene anders gestaltete Praxis in ARZ zurück, die hat untersagt werden sollen. Die Vorschrift ist dahin zu verstehen, dass der *Primärdaten-Bestand*, also die Gesamtheit der mit Identifikatoren versehenen, für die Verwendung nach dem SGB bestimmten Datensätze, in keiner Hinsicht mit (zusätzlicher) Rücksicht auf die (Verwendbarkeit für die) vom 2. Halbsatz erlaubten Verarbeitungen ausgestaltet, insbesondere etwa geordnet oder durch Kennungen organisiert, oder aufbewahrt werden darf.

6.3.2 Innerhalb der dadurch gesetzten Grenzen erlaubt § 300 Abs. 2 Satz 2 SGB V in seinem 2. Halbsatzes neben der im 1. Halbsatz erlaubten Datenverwendung auch eine für sich gesehen, wie vorstehend unter 6.1 gezeigt, gar nicht dem Anonymisiertheits-Erfordernis des 2. Halbsatzes genügende, aber der Erfüllung dieses Erfordernisses dienende Verarbeitung, nämlich die Verarbeitung nicht zu SGB-Zwecken, aber zum Zweck der Anonymisierung und damit der Herbeiführung eines Datenzustandes, für den der 2. Halbsatz eine Verwendungserlaubnis ausspricht. Es handelt sich, wie oben unter 6.1 dargelegt, um eine Erlaubnis der Nutzung der Primär-Daten (Halbsatz-1-Daten) zum Zweck der Gewinnung von nach dem 2. Halbsatz zu verarbeitenden Daten, die dem Gesetz, genauer gesagt dem 2. Halbsatz, nur indirekt – aber zwingend - zu entnehmen ist. Das Schaffen der Voraussetzung der Anonymität ist ein Verarbeitungszweck, den das Gesetz vorsieht.

6.3.3 Aus dem Anonymisiertheits-Erfordernis des 2. Halbsatzes folgt, dass das ARZ sogar **nicht einmal generell, sondern nur unter bestimmten Voraussetzungen einzelnen Apotheken Auswertungen der (ausschließlich) auf sie selbst**

bezogenen Daten zur Verfügung stellen darf. Diese Voraussetzungen gelten auch dann, wenn diese Daten, wie auf jeden Fall geboten ist, frei von jedem Bezug auf einzelne Versicherte und einzelne Ärzte sind, (wobei es auch hier wieder auf den für den Empfänger und zusätzlich wegen der in keiner Weise ausgeschlossen Möglichkeit der Weitergabe durch diesen für jeden denkbaren Empfänger bestehenden Möglichkeiten der Zuordnung ankommt). Das ergibt sich im einzelnen aus folgendem:

Erlaubt ist eine solche Auswertung und Übermittlung dann, wenn durch die Auswertung ausschließlich ein einzelner sich auf die betreffende einzelne Apotheke beziehender Datensatz (bzw. Komplex derartiger Datensätze) entsteht. Denn es handelte sich insoweit ja um Daten der einzelnen Apotheke, deren Auftragnehmer das ARZ ist, so dass es sich datenschutzrechtlich gesehen um eigene Daten des Verarbeiters[35] Apotheke und damit um Daten handelt, die sich ausschließlich auf den Daten-Empfänger Apotheke beziehen (und ja aus den von dieser gelieferten Daten unter Beseitigung des Personenbezuges auf alle Dritten gewonnen sind). Man kann also geltend machen, dass bezogen auf die betreffende Apotheke im ARZ in diesem einzelnen Datensatz bzw. Datensätze-Komplex keine Daten eines Dritten und damit, was diesen Datensatz(-Komplex) betrifft, keine personenbezogenen Daten im Sinne des Datenschutzrechts verarbeitet werden.

Allerdings dürften diese Datensätze *nicht personenbezogen* in einem *Sekundär-Datenbestand* des ARZ stehen, der viele[36] auf vielerlei Apotheken bezogene Einzel-Datensätze enthielte. Denn diese wären jeweils für jeden anderen Apotheker, und erst recht für sonstige Dritte, *fremde* Daten, die im ARZ vorhanden wären.

Eine zusätzliche Begründung für diese Überlegung ergibt sich wohl aus folgendem: Man wird das erläuterte „Ausrichtungs"-Erfordernis des 1. Halbsatzes zusammen mit dem 2. Halbsatz aller Wahrscheinlichkeit so auszulegen haben, dass dem Gesetz in Satz 2 eine kollektive Betrachtung des gesamten Datenbestandes des ARZ zugrunde liegt, mit der Folge, dass der Sekundär-Datenbestand, den das ARZ in Gebrauchmachen von der diesbezüglichen (wie gezeigt erweitert auszulegenden) Erlaubnis des 2. Halbsatzes aufbauen darf, als Ganzer zu sehen ist und daher insgesamt anonymisiert sein muss.

Deswegen gibt es für Auskünfte – also die Herstellung, Speicherung und Übermittlung von Datensätzen – für Apotheken über sich ausschließlich auf diese selbst beziehende Umstände für das ARZ nur zwei erlaubte Möglichkeiten:

---

[35] S. oben Fußnote 1

[36] Gemeint ist natürlich: Mehr als einen!

- Entweder erarbeitet und übermittelt es nur einzelne Auskünfte ad hoc, die vom ARZ nicht (namentlich in einer Datei mit gleichartigen Datensätzen) gespeichert, sondern nach Gewinnung und sofortiger Übermittlung umgehend gelöscht werden.
- Oder die gleichartigen Datensätze verschiedener Apotheken werden in einem *Sekundär-Datenbestand* ausschließlich unter einem nur vom ARZ selbst entschlüsselbaren (zuordnungsfähigen) Pseudonym gespeichert.

6.3.4 An Arzneimittelhersteller oder Händler oder für diese tätige Vermittler oder überhaupt **an Dritte**, die ja die betreffenden Daten frei weitergeben dürften, darf das ARZ keine Daten übermitteln, die diesen oder eben irgendwelchen denkbaren Empfängern in einer Ketten-Weitergabe einen Rückschluss auf Umstände ermöglichten, die sich auf eine einzelne bestimmte Person (oder auch Stelle) beziehen, also auch auf Ärzte, Arztpraxen, medizinische Versorgungszentren oder Krankenhäuser, oder gar auf einzelne Versicherte. **Das bedeutet insbesondere, dass diejenigen Daten, die ARZ auf der Grundlage des 2. Halbsatzes weitergeben dürfen sollen, keine von Dritten vergebenen und verwendeten und daher diesen *zuordnungs-bekannten* Pseudonyme wie etwa Versichertennummer, Arztnummer (LANR oder ähnliches), Betriebsnummer, Institutionenkennzeichen oder dergleichen enthalten dürfen. Denn die diesen Pseudonymen zugeordneten, zu ihnen „gehörenden" natürlichen Identifikatoren lassen sich vielfach, zumindest in erwartbaren Einzelfällen, ohne größeren Aufwand von jedermann beschaffen, und deswegen wären die betreffenden Angaben wegen ihrer Zuordnung zu solchen Pseudonymen nicht mehr hinreichend anonymisiert.**

6.3.5 Geolokalisierende Datensatzbestandteile, etwa aus Anschriften, namentlich den Postleitzahlen[37], abgeleitete, dürfen vom ARZ nur unter Zuordnung zu Einteilungs-Einheiten verwendet werden, die in jeglichem Zusammenhang in der *Sekundär-Datenbank* so groß sind, dass sie für keinen zugeordneten Datensatz eine Zuordnung zu bestimmten Personen ermöglichen. Insbesondere im Hinblick auf seltene Fachrichtungen oder sonstige Arztpraxis-Eigenheiten (Tätigkeitsprofile besonders spezialisierter Ärzte) müssen diese Einheiten so gestaltet sein, dass niemals eine bestimmte Kombination von Merkmalsausprägungen weniger als 3 mal in dem betreffenden geographischen Bezirk vorkommt.

[37] Inwieweit den ARZ ein Zukauf anschriftenbezogener Geokoordinaten-Daten angesichts des latenten Personenbezuges dieser Daten als Datenerhebung erlaubt sein könnte, ist dem Ausrichtungs-Gebot des 1. Halbsatzes zu entnehmen: Es ist ihm verboten.

6.3.6 Man kann den Bereich der durch den 2. Halbsatz erlaubten Datenweitergabe auch **vom Ergebnis**, d.h. von den Verwendungsmöglichkeiten des Datenempfängers **her bestimmen**:

6.3.6.1 Daten für Empfänger, die etwas mit dem Vertrieb und namentlich dem Bewerben von Arzneimitteln zu tun haben - und damit eben für jeden Empfänger, weil eine Weitergabe dorthin ja alles andere als ausgeschlossen ist – **dürfen keine Daten enthalten, die für diese Empfänger für die Zwecke gezielter werblicher Ansprache einzelner Arztpraxen, Krankenhäuser oder Apotheken auch nur die geringste Aussagekraft oder sonstige Anhaltspunkte enthielten**. Nur Daten, die eine Datengrundlage für die gezielte werbliche Ansprache von Berufsträgern (Ärzten, Apotheken) *einheitlich in ganzen Regionen* enthalten, sind von der Verarbeitung und insbesondere Weitergabe auf der Grundlage des 2. Halbsatzes nicht von vornherein ausgeschlossen. Das aber sind Daten, die aller Wahrscheinlichkeit nach wegen der weitgehenden recht engen Ortsbeziehung zwischen verordnendem Arzt und ausgebender Apotheke ohnehin vom Pharma-Großhandel aus eigenen, schon vorhandenen Kenntnissen vermutlich mit viel weniger Rechenaufwand ermittelt werden und dann entsprechend kostengünstiger zur Verfügung gestellt werden können.

6.3.6.2 Des weiteren muß man, um das Zusatzwissen und die sonstigen Zuordnungsmöglichkeiten der Datenempfänger richtig einzuschätzen, einfach folgern: Sofern es in Fachkreisen **Informationen** gibt, denen zufolge auch nur **in einzelnen Fällen** sich hat beobachten lassen, dass Apotheken oder vor allem **Ärzte** oder ärztliche Einrichtungen **von Seiten der Arzneimittelhersteller werblich** so **angesprochen** worden sind, dass erkennbar ist, dass **Kenntnisse über ihr Verschreibung-Verhalten bekannt** waren bzw. genutzt worden sind, können diese Kenntnisse mit an Sicherheit grenzender Wahrscheinlichkeit nach nur entweder von einzelnen Apotheken oder, viel wahrscheinlicher, von ARZ stammen, so dass in beiden Fällen, nicht nur im ersteren, eine rechtswidrige Datenübermittlung stattgefunden haben muss. (Diese Überlegung lässt natürlich Rückschlüsse genau auf in jüngster Zeit erfolgte Datenübermittlungen zu, denn sie müssen einerseits schon geschehen und andererseits noch frisch genug sein, um noch von praktischem Wert gewesen zu sein.)

Darüber hinaus **erlauben** gegebenenfalls auch von Dateninteressenten den ARZ angebotene **Entgelte** für auf der Grundlage des 2. Halbsatzes erarbeitete und angebotene Daten **Rückschlüsse** auf die Zuordnungsmöglichkeiten der Empfänger: Die Höhe solcher Entgelte lässt Rückschlüsse darauf zu, wie nahe an den Verordnungs-

Entscheidern – sprich: Ärzten - (und damit umsatzwirksam) die übermittelten Informationen oder die aus diesen gewinnbaren Informationen nach Einschätzung der Datenerwerber genutzt werden können.

7 Bestimmung der Verantwortungsträger; Zuordnung personaler Verantwortung

Die oben unter 5.3.1 näher dargelegte zivilrechtliche (genauer datenschutzrechtliche), ordnungswidrigkeitenrechtliche und strafrechtliche Verantwortung und die Folgen datenschutzaufsichtsrechtlicher sowie sozialrechtlicher aufsichtsbehördlicher Maßnahmen liegt zunächst beim ARZ selbst, das heißt bei den dort leitend oder, vermindert, auch nur ausführend Tätigen. Die zivilrechtliche, ordnungswidrigkeitenrechtliche und strafrechtliche Verantwortung für etwaige Verstöße des ARZ gegen § 300 Abs. 2 Satz 2 schlägt jedoch zusätzlich auch auf **jeden einzelnen Apotheker** durch, der seine Daten dem betreffenden ARZ zu Abrechnungszwecken übermittelt.

Das folgt daraus, dass das Rechtsinstitut der *Auftragsdatenverarbeitung*, unter das, wie oben 4.2.2 gezeigt, das rechtliche Verhältnis zwischen dem einzelnen Apothekeninhaber und dem Rechtsträger des ARZ fällt, die Verantwortung für die faktisch beim Auftragnehmer stattfindende Verarbeitung im Außenverhältnis zum Betroffenen, also demjenigen, auf den sich die Daten beziehen, datenschutzrechtlich ausschließlich dem Auftraggeber auferlegt (§ 11 Abs. 1 Satz 1 BDSG). Und diese Verantwortungszuweisung gilt auch ordnungswidrigkeitenrechtlich, jedenfalls zusätzlich zur diesbezüglichen Verantwortung des Auftragnehmers, und das schlägt auch auf die strafrechtliche Verantwortung des Auftraggebers, also eben des einzelnen Apothekers, durch. Denn die ihm (nach § 1 Abs. 2 Satz 2 Nr. 7, Satz 4 BDSG) hinsichtlich der von ihm gelieferten Daten datenschutzrechtlich obliegende Pflicht, das Verarbeitungshandeln des Auftragnehmers zu kontrollieren, begründet, in Verbindung mit seinem Weisungsrecht (§11 Abs. 2 Satz 2 Nr. 9, Abs. 3 Satz 1 BDSG), also seinen Möglichkeiten zur Einwirkung auf den Auftragnehmer, strafrechtlich eine sogenannte **Garantenpflicht**, mit der Folge, dass **der einzelne auftraggebende Apotheker *zumindest wegen Unterlassung* strafbar ist,** wenn vom ARZ strafbar Daten übermittelt werden und dem Apotheker zumindest bedingter Vorsatz nachzuweisen ist. Für einen solchen bedingten Vorsatz reicht es aus, wenn der Apotheker weiß oder wenn es ihm gleichgültig ist, dass das ARZ nennenswerte Entgelte für von ihm außerhalb des 1. Halbsatzes, also an Empfänger außerhalb des SGB V, übermittelte Daten erhält.

8 Zusammenfassung in praktisch-wirtschaftlicher Hinsicht

In praktisch-wirtschaftlicher Hinsicht lässt sich zusammenfassend als Ergebnis feststellen, dass gemäß § 300 Abs. 2 Satz 2, 2. Halbsatz SGB V den ARZ nur in einem sehr eingeschränkten Ausmaß die Verarbeitung der ihnen von den Apotheken übermittelten Daten zu anderen als den ihnen im SGB, namentlich in § 300 SGB V, vorgeschriebenen Zwecken erlaubt ist. Es ist nicht ersichtlich, dass die **erlaubterweise** von den ARZ Dritten zur Verfügung zu stellenden Daten für diese wirtschaftlich interessant sein könnten, damit also nennenswerte Entgelte erzielt werden könnten. Insbesondere dürfen die ARZ keine Daten übermitteln, die für Entscheidungen über irgendwelche individuelle werbliche Ansprache von Ärzten relevant sein könnten.

Die rechtliche, auch strafrechtliche, Verantwortung trifft in erster Linie diejenigen, die Leitungsverantwortung für das ARZ haben, daneben aber grundsätzlich auch jeden einzelnen Apotheker, der über das betreffende ARZ abrechnet.

Dr. Thomas Giesen Dr. Christian Schnoor