Jahrbuch

neuer wissenschaftlicher Verlag
Recht

Datenschutzrecht und E-Government

09

herausgegeben von

Dietmar Jahnel

Rainer KNYRIM/Viktoria HAIDINGER

Datenschutzrechts-Compliance in medizinischen Einrichtungen und Pharmaunternehmen in der Praxis

Inhaltsübersicht

A. Einleitung

Compliance ist in aller Munde, Datenschutzrecht sollte Teil eines Compliance-Programms sein. Wie sich medizinische Einrichtungen und Pharmaunternehmen auch in diesem Rechtsbereich gesetzeskonform verhalten können und wie sie die Probleme rund um die Verarbeitung von Arzt-, Patienten- und Mitarbeiterdaten, Marketing und Globalisierung aufarbeiten müssen, soll in diesem Beitrag dargelegt werden.

In jüngster Zeit wird im Zuge von „Compliance" in Unternehmen verstärkt auch eine datenschutzkonforme Datenverwendung angestrebt. Sei es, weil das Unternehmensimage dadurch aufgebessert werden soll und Datenschutzkonformität nicht mehr nur eine leere Behauptung sein soll, weil Projekte wie die

„eCard" oder die „elektronische Gesundheitsakte"[1] Datenschutzrecht im medizinischen Bereich an die Öffentlichkeit und in die Medien gebracht haben, oder weil neuerdings medizinische Einrichtungen, Ärzte, Ethikkommissionen, Patienten oder eigenen Mitarbeiter und Betriebsräte diesbezüglich verstärkt nachfragen, oder es tatsächlich der verschiedenen Gerichtsurteile im Bereich des Datenschutzrechtes bedurfte.[2] Fakt ist: das Thema steht neuerdings sehr weit oben auf der Agenda von medizinischen Einrichtungen und Pharmaunternehmen. Doch wie soll man an das Thema herangehen? Wie macht man einen medizinischen Betrieb, in dem sich in den letzten Jahren kaum jemand um datenschutzrechtliche Fragen gekümmert hat, datenschutz-„Compliant"? Auf welche rechtlichen Fragen muss eine medizinische Einrichtung achten, die sich bislang vor allem mit Einzelproblemen des technischen Datenschutzes befasst hat? Diese und andere Fragen sollen im Folgenden Schritt für Schritt behandelt werden.

B. Identifikation von Datenanwendungen

Zunächst muss eine Bestandaufnahme gemacht werden, welche Datenanwendung überhaupt in Verwendung stehen. Oft wird man auf eine Vielzahl von – sich zum Teil überschneidenden – Datenbanken und Datenanwendungen stoßen. Datenschutz-Laien ist oft unbekannt, was überhaupt datenschutzrechtlich aufzuarbeiten ist. So werden etwa Genehmigungspflichten bei internationalem Datenflüssen nach wie vor oft übersehen,[3] weshalb die Einbindung externer Expertise bereits zu diesem Zeitpunkt zweckmäßig sein kann. Zu den Schwierigkeiten bei der Sachstanderhebung und Analyse der Datenanwendung in der Praxis siehe den nächsten Unterpunkt.

C. Analyse der Datenanwendungen

Der nächste Schritt ist, bei jeder einzelnen Datenanwendung nachstehende Punkte zu klären:

1. Was ist der Zweck der Anwendung?
2. Wer ist betroffen?
3. Welche Daten(-arten) werden darin konkret gespeichert und verwendet (genaue Liste!)?
4. Wer hat intern im Unternehmen Zugriff auf die Daten?[4]

---

1 Siehe etwa „Wer hat Angst vor ELGA?", ÖKZ 2008/06, 27.

2 ZB OGH 6 Ob 275/05t, Schadenersatz gemäß § 33 DSG, (MR 2006), 83 mit Glosse *Knyrim*; OGH 20.12.2006, 9 Ob A 109/06d – OGH bestätigt Klage des Betriebsausschusses auf Unzulässigkeit eines biometrischen Zeiterfassungssystems mittels Fingerscan in Bezirkskrankenhaus; OLG Wien 12.1.2007, 7 Ra 3/07y – OLG Wien hebt Entscheidung über Abweisung eines Antrages auf einstweilige Verfügung gegen die Einführung bzw. den Betrieb einer Videoüberwachungsanlage in einem Betrieb wegen Verfahrensmängeln (insbesondere der fehlenden Einvernahme des Betriebsrates) wieder auf und verweist zurück an das Erstgericht.

3 Siehe *Knyrim*, Outsourcing und Datenschutzrecht: Achtung, die Welt ist flach! ecolex 2009, 85.

4 Gemeint ist hier nur die jeweilige Rechtspersönlichkeit

5. Hat sonst jemand, im In- oder Ausland, Zugriff auf die Daten, an wen werden sie übermittelt?[5]
6. Werden Zugriffe protokolliert?
7. Wo werden die Daten physisch gespeichert?

So einfach die Erhebung des Sachstandes und die Analyse der Datenanwendung theoretisch zu sein scheint, in der Praxis ist sie meist die Hauptarbeit des Datenschutzrechts-Compliance-Projektes. Schon bei den ersten Gesprächen zeigt sich nämlich regelmäßig, dass weder IT-Verantwortliche, noch die Geschäftsführung, noch Bereichsleiter, noch einzelne Sachbearbeiter heute mehr einen umfassenden Überblick über ihren Arbeitsbereich, geschweige denn einen Gesamtüberblick über das Unternehmen haben. Vielmehr bedarf es oft erst akribischer Nachfrage- und Recherchearbeit und dem Zusammensetzen einzelner „Puzzelteile", um zum notwendigen Gesamtüberblick und gleichzeitig dem essenziellen Detailwissen über die einzelnen Datenanwendungen zu gelangen. Die Recherche erfolgt meist in einer Mischung aus Gesprächen, Korrespondenz, „durchforsten" von Listen von Datenfeldern in der jeweiligen Software, Durchsicht von Bildschirmkopien der Benutzeroberfläche von Datenbanken bis hin zum direkten „arbeiten" mit der Software oder Datenbank. Je international vernetzter etwa ein Pharmaunternehmen dabei in einem Konzern ist, desto schwieriger ist die Informationsbeschaffung. Vermeintlich einfache Fragen wie etwa, was der Zweck eines Datenzugriffes der ausländischen Konzernmutter ist, welche genauen Zugriffsberechtigungen auf Datensätze bestehen oder an welchem Ort der Welt die Daten eigentlich physisch gespeichert werden, sind in der globalisierten Welt oft nur mehr nach aufwändiger Korrespondenz im Konzern beantwortbar.

D. Datenschutzrechtliche Aufarbeitung

Ist der Sachstand ermittelt, kann mit der datenschutzrechtlichen Aufarbeitung begonnen werden, die typischer Weise mit der Suche nach einer Rechtsgrundlage (materielle Voraussetzung) sowie der Prüfung der Notwendigkeit von DVR-Meldungen (formelle Voraussetzung) beginnt. Die Rechtsgrundlage kann sich dabei entweder direkt aus dem DSG 2000 oder aus einem Materiengesetz ergeben. Mögliche Rechtsgrundlagen werden unter Punkt E) dieses Beitrages behandelt.

1. Meldung beim DVR

§ 52 Abs 2 Z 1 DSG 2000 sanktioniert die Ermittlung, Verarbeitung oder Übermittlung von Daten ohne die Meldepflichten erfüllt zu haben, mit Geldstrafen bis zu EUR 9.445,--. Übersehen wird bei dieser – im Verhältnis zum Aufwand eines Datenschutz-Compliance-Projektes eher geringen Strafe – wie bei allen Strafen des Datenschutzrechts, dass nach § 52 Abs 4 DSG 2000 der „Verfall" von Datenträgern und Programmen ausgesprochen werden kann. Dies kann für EDV-Anwendungen schlicht das „Aus" bedeuten, wenn weder Software noch Daten

5 Achtung: Im DSG gibt es kein „Konzernprivileg", Zugriffe von Konzerngesellschaften sind wie Zugriffe von (fremden) Dritten zu behandeln. So auch *Simitis* in *Simitis* (Hrsg), Bundesdatenschutzgesetz[6] (2006) § 4c Rz 61 mwN.

weiter verwendet werden dürfen und in einem Unternehmen dramatische Folgen haben.[6] Diese Tatsache und auch die künftig erhöhte Transparenz für den Bürger durch eine kostenlose, für jedermann im Internet zugängliche Abfragemöglichkeit des Datenverarbeitungsregisters[7] erfordern die Aufarbeitung des Standes der DVR-Meldungen im Pharmaunternehmen als prioritäres Projekt.

Ein Blick auf den Datenverarbeitungsregisterauszug eines Pharmaunternehmens zeigt häufig, dass Meldungen von Datenanwendungen Jahre, wenn nicht Jahrzehnte alt sind[8] und daher sehr fraglich ist, ob diese in Hinblick auf die rasche Vertiefung und Vernetzung der Datenverarbeitung in den letzten Jahren noch aktuell sind. Übersehen wird nämlich oft, dass einmal eingebrachte DVR-Meldungen laufend aktuell zu halten sind.[9]

Der Ablauf der Prüfung der DVR-Meldepflicht erfolgt derart, dass die Ergebnisse der Sachstandermittlung mit den Standard- und Musteranwendungen laut Anlage der Standard- und Musterverordnung[10] (StMV 2004) verglichen werden, um eine allfällige Meldepflicht festzustellen.[11] Typischerweise gehen die Datenanwendungen von medizinischen Einrichtungen oder Pharmaunternehmen, die meist sehr spezifisch sind, über die für normale Unternehmen oft anwendbaren Standards (insbesondere SA001 Rechnungswesen und Logistik, SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse, SA007 Verwaltung von Benutzerkennzeichen und SA022 Kundenbetreuung und Marketing für eigene Zwecke sowie MA002 Zutrittskontrollsysteme) hinaus und es liegt eine Meldepflicht für verschiedenste Datenanwendungen vor.

---

6 Das Verwaltungsgericht Wiesbaden untersagte in mehreren Verfahren (23 LG 485/5, 23 LG 511/05, 23 LG 560/05) die Einführung eines neuen Computerprogramms (SAP R/3 HR) in drei hessischen Polizeibehörden vorläufig. Nach Auffassung des Verwaltungsgerichts wies das Programm erhebliche Mängel auf und gefährdete das Recht auf informationelle Selbstbestimmung. Zudem seien die Beteiligungsrechte der Personalvertretungen verletzt worden. Erst Monate später gab der Verwaltungsgerichtshof in Kassel (22 TH 1496/05, 10.06.2005) wieder grünes Licht für das Projekt. Berichterstattung auf Heise unter http://www.heise.de/newsticker/meldung/59799 und http://www.heise.de/newsticker/Verwaltungsgerichtshof-gibt-gruenes-Licht-fuer-Computerprogramm-in-Polizeibehoerden--/meldung/60534 .

7 Laut Auskunft des Datenverarbeitungsregisters befindet sich diese Abfragemöglichkeit bereits im Testbetrieb und soll in absehbarer Zeit freigeschaltet werden und es jedem Bürger ermöglichen, zB durch Namensabfrage mit dem Firmennamen eines Unternehmens sofort den DVR-Registerauszug dieses Unternehmens als pdf-Dokument herunterzuladen. Beispiele für solche Register: Belgien https://www.privacycommission.be/elg/searchPR.htm?eraseResults=true&siteLanguage=fr oder England: http://www.esd.informationcommissioner.gov.uk/esd/search.asp.

8 Viele Meldungen stammen noch aus der Zeit der ersten Meldeflut nach Inkrafttreten des DSG 1978 BGBl 565/1978 am 1.1.1980.

9 Die Aktuellhaltung betrifft nicht nur die Datenanwendungen, sondern beginnt bereits bei der Aktualisierung von Firmenname und Adresse des jeweiligen Pharmaunternehmens, die bei Veränderungen zwar beim Firmenbuch angezeigt werden, dem DVR aber nicht gemeldet werden.

10 Standard- und Muster-Verordnung 2004 - StMV 2004 BGBl II 312/2004.

11 Eine genaue Anleitung zum Arbeiten mit den Standard- und Musteranwendungen findet sich in *Knyrim*, Praxishandbuch Datenschutzrecht, Leitfaden für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm (2003) 25 ff.

Um die Meldepflichten im medizinischen Bereich in Grenzen zu halten, wurden durch die Standard- und Musterverordnung 2000[12] und die StMV 2004 insgesamt vier spezifische Standardanwendungen geschaffen, nämlich

1. SA 024 Patientenverwaltung und Honorarabrechnung
2. SA 026 Verrechnung ärztlicher Verschreibungen für Rechnung begünstigter Bezieher durch Apotheken
3. SA 027 Verrechnung ärztlich verordneter Heilbehelfe und Hilfsmittel durch Gewerbetreibende
4. SA 028 Verrechnung ärztlich verordneter Behandlungen und diagnostischer Leistungen durch freiberuflich tätige Angehörige der medizinisch technischen Dienste, klinischen Psychologen und Psychotherapeuten.

Diese Standardanwendungen sind jedoch nur für die in diesen definierten speziellen Auftraggeber-Gruppen (zB Ärzte, Psychotherapeuten) und speziellen Zwecke (zB Patientenkarteien, Honorarverrechnung) und abschließend aufgezählten Datenarten (zB nur Rezept- und Versicherungsdaten bei SA 026) anwendbar. Eine andere medizinische Einrichtung oder ein Pharmaunternehmen wird sich typischer Weise daher auf gar keine dieser vier spezifischen Standardanwendungen stützen können, sondern vielmehr aufgrund der spezifischen Natur der Datenanwendungen der spezifische Datenarten, die es verarbeitet und der spezifischen Empfängerkreise (insbesondere Konzerngesellschaften, Behörden) gezwungen sein, eine Reihe von Datenanwendungen zu melden. Typische solcher meldepflichtigen Datenanwendungen sind etwa Besuchsberichtswesen der Außendienstmitarbeiter, Marketing (etwa wegen dem Versand von Promotionsmaterial an ausgesuchte medizinische Zielgruppen), Produktsicherheits- und Pharmakovigilanz-Datenanwendungen, Datenanwendungen im Bereich klinischer Prüfungen/medizinischer Studien, Kongress- und Veranstaltungsorganisation. Durch die auch im Gesundheitsbereich fortschreitende Datenvernetzung und „Datenglobalisierung" wird neben den „medizinischen" Datenanwendungen oft auch eine Meldepflicht bei „normalen" Datenanwendungen zur Betriebsorganisation eine Meldepflicht ausgelöst sein, etwa Personalverwaltung, -schulung, -beurteilung, Mitarbeiterverzeichnissen, Finanzbuchhaltung, Lieferanten- und Kundendatenverarbeitung, Callcentern etc.

Im Detail kann hier aus Platzgründen nicht auf alle der zahlreichen Datenanwendungen eingegangen werden, einige wurden als Beispiele herausgegriffen (siehe weiter unten). An dieser Stelle sei überdies auf zwei wesentliche Besonderheiten bei der Verwendung von Gesundheitsdaten hingewiesen:

Daten natürlicher Personen über ihre rassische und ethnische Herkunft, Gesundheit oder ihr Sexualleben fallen per Definition unter den Begriff „sensible Daten".[13] Sensible Daten dürfen nur in ganz bestimmten Fällen, unter denen die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzt werden, verwendet werden. Diese Fälle sind abschließend in § 9 DSG 2000 aufgezählt, nämlich ua bei Bestehen einer besonderen gesetzlichen Ermächtigung oder Verpflichtung, wenn die Verwendung zur Wahrung lebenswichtiger Interessen notwendig ist, wenn der Betroffen seine ausdrückliche Zustimmung zur Verwendung erteilt hat und zum Zweck der Gesundheitsvorsorge, der medizinischen

12 BGBl II 201/2000. Diese wurde durch die StMV 2004 BGBl II 312/2004 abgelöst.
13 § 4 Z 2 DSG 2000.

Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Aus dem letztgenannten Fall ergibt sich, dass eine Verwendung von Gesundheitsdaten durch andere Personen als ärztliches Personal oder einer Geheimhaltungspflicht unterliegenden Personen, sofern nicht lebenswichtige Interessen (zB im Bereich der Notfallversorgung) vorliegen und es keine Sondernormen gibt, oft nur mit der ausdrücklichen Zustimmung der Patienten überhaupt zulässig sein wird. Eine fehlende Rechtsgrundlage kann auch durch eine (formale) DVR-Meldung nicht „ersetzt" werden, sondern macht die Datenverwendung materiell unzulässig.

Die zweite Besonderheit bei der Verwendung von Gesundheitsdaten ergibt sich aus § 18 Abs 2 Z 1 DSG 2000, dem zu Folge Datenanwendungen, die sensible Daten enthalten, erst nach Prüfung (Vorabkontrolle)[14] durch die Datenschutzkommission begonnen werden dürfen.[15] Dies ist bei neuen EDV-Projekten zeitlich mit entsprechender Vorlaufzeit von mindestens zwei Monaten, besser jedoch einem wesentlich längeren Zeitraum zu berücksichtigen.[16]

Zu den DVR-Meldungen kann festgestellt werden, dass sich das Datenverarbeitungsregister heute wesentlich detaillierter ausgearbeitete Meldungen als früher erwartet, sowohl in Hinblick auf die „Tiefe" der angeführten Datenarten, als auch auf die Detaillierung der Übermittlungsempfänger und der Rechtsgrundlagen. Waren früher DVR-Meldungen üblich, bei denen eine „Handvoll" Datenarten angegeben wurden, die – ohne nähere Erklärungen – an „Konzernunternehmen" und „an der Geschäftsabwicklung mitwirkende Dritte" übermittelt wurden, so sollten heute die Ergebnisse der internen Analyse wesentlich präziser angeführt werden, da die Komplexität heutiger EDV-Systeme es kaum noch glaubwürdig erscheinen lassen, dass lediglich eine sehr geringe Anzahl von Daten verarbeitet werden und an sehr wenige und kaum näher spezifizierbare Empfängerkreise übermittelt werden.[17]

Aus dem Anlass aktueller Gerichtsentscheidungen sei darauf hingewiesen, dass Videoüberwachungsanlagen, die Videos speichern, bei der Datenschutz-

---

14 Zur Vorabkontrolle siehe *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 2000 (2000) 76 und *Mayer-Schönberger/Brandl,* Datenschutzgesetz 2000 (1999) 30.

15 „Normale" Datenanwendungen, die keine sensiblen oder strafrechtlich relevanten Daten oder Daten über die Kreditwürdigkeit der Betroffenen enthalten oder in Form eines Informationsverbundsystems durchgeführt werden dürfen hingegen unmittelbar nach Abgabe der Meldung in Vollbetrieb aufgenommen werden (§ 18 Abs 1 DSG 2000), wobei die Datenschutzkommission diese binnen zwei Monaten prüfen muss (§ 20 Abs 1 DSG 2000).

16 Die zwei Monate Mindestfrist und die Empfehlung längerer Vorlaufzeiten ergeben sich aus § 20 Abs 1 DSG 2000 und der Erfahrung aus der Praxis, dass das DVR Verbesserungsaufträge meist erst am Ende der Frist absendet, danach jedoch nicht mehr an die 2-Monatsfrist gebunden ist und die Abarbeitung der allfälligen Verbesserungen oft erst viele Monate später erfolgt. Dem entsprechend sollte bereits möglichst früh – etwa bei Feststehen der tatsächlich zu verarbeitenden Datenarten in einer neuen Datenanwendung – Meldung eingebracht werden um nicht unter Zeitdruck zu gelangen.

17 Näheres zum DVR-Meldeverfahren siehe *Dohr/Pollirer/Weiss,* DSG[2] bei § 17; *Jahnel,* Datenschutzrecht in der Praxis, (2004) 35 ff; *Knyrim,* Praxishandbuch Datenschutzrecht 25 ff.

kommission vorab zu melden sind und eine Betriebsvereinbarung über diese abzuschließen ist. Ebenso sind Zutrittskontrollsysteme beim DVR entweder als Musteranwendung MA 002 oder, falls sie über diese hinausgehen, als (allenfalls auch vorab meldepflichtige) DVR-Meldung einzureichen und bedürfen ebenfalls einer Betriebsvereinbarung. Der Oberste Gerichtshof bestätigte jüngst die Entscheidung der Vorinstanzen, die aufgrund der Klage und des Antrages auf einstweilige Verfügung des Betriebsausschusses eines Bezirkskrankenhauses die Einführung eines biometrischen Zutrittskontrollsystems, das mit „Fingerscans" funktionierte, mittels einstweiliger Verfügung untersagte. Dies, weil das biometrische Fingerscanning die Menschenwürde der Arbeitnehmer iSd § 96 Abs 1 Z 3 ArbVG berühre und das System ohne Zustimmung des Betriebsausschusses eingeführt worden war.[18] Das OLG Wien hingegen hob in einer noch jüngeren Entscheidung die Abweisung eines Antrages auf einstweilige Verfügung gegen die Einführung bzw den Betrieb einer Videoüberwachungsanlage in einem Betrieb wegen Verfahrensmängeln (insbesondere der fehlenden Einvernahme des Betriebsrates) wieder auf und verwies die Entscheidung zurück an das Erstgericht.[19] Die beiden Entscheidungen zeigen, dass mittlerweile betriebsintern sogar unter Einschaltung der Gerichte die Einhaltung des Datenschutzrechts und der arbeitsverfassungsrechtlichen Mitbestimmungsrechte[20] bei Datenverarbeitung eingefordert wird.[21]

Da immer mehr Unternehmen auch im Gesundheitsbereich Daten innerhalb des eigenen Konzerns, aber auch mit anderen Unternehmen im oder außerhalb des Gesundheitsbereichs vernetzen, kann sich dadurch ein zusätzliches datenschutzrechtliches Problem ergeben, nämlich das Vorliegen eines Informationsverbundsystems. Nach § 4 Z 13 DSG 2000 ist die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Nutzung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden, ein Informationsverbundsystem. § 50 Abs 1 DSG 2000 verpflichtet die Auftraggeber eines Informationsverbundsystems, einen Betreiber für das System zu bestellen. Nach § 18 Abs 2 Z 4 DSG 2000 darf ein Informationsverbundsystem erst nach Vorabkontrolle durch die Datenschutzkommission in Betrieb genommen werden.[22] Ein Informationsverbundsystem könnte etwa dadurch entstehen, dass die Besuchsberichte der Außendienstmitarbeiter eines Pharmaunternehmens in einer Datenbank gespeichert werden, auf die mehrere Konzerngesellschaften (im In- und/oder Ausland) Zugriff haben. Dies könnte eine Vorabgenehmigungspflicht als Konsequenz haben und überdies müssten über dessen Existenz alle Betroffenen (eigene Mitarbeiter, dritte Personen) entsprechend § 24 Abs 2 Z 3 DSG 2000 informiert werden, was besonders hinsichtlich der typischerweise von solchen Datenbanken erfassten Ärzten oder anderen Personen aus der Gesundheitsbranche zu beachten ist.

---

18 OGH 20.12.2006 9 Ob A 109/06d.

19 OLG Wien 12.1.2007, 7 Ra 3/07y.

20 §§ 96, 96a ArbVG.

21 Soll eine solche Anlage in einem betriebsratslosen Betrieb eingeführt werden, so ist nach § 10 AVRAG in den dort genannten Fällen die Zustimmung jedes einzelnen Mitarbeiters einzuholen.

22 Siehe näher *Dohr/Pollirer/Weiss*, DSG[2], Anm zu § 50 sowie *Knyrim*, Praxishandbuch Datenschutzrecht 21 f.

2. Genehmigungspflichten für internationalen Datenverkehr; Outsourcing

Durch die verstärkte Vernetzung von Unternehmen im Gesundheitsbereich auch über die EU-Grenzen hinaus wird auch bei diesen die Problematik des internationalen Datenverkehrs – insbesondere wegen des Fehlens eines Konzernprivilegs im Europäischen Datenschutzrecht – zum Thema und diese sind dementsprechend gezwungen, zu prüfen, ob eine genehmigungsfreie Übermittlung oder Überlassung von Daten in das Ausland vorliegt (etwa weil die Betroffenen ihre Zustimmung dazu gegeben haben) oder, ob eine Genehmigungspflicht nach § 13 DSG 2000 vorliegt und daher der Genehmigungsprozess zu durchlaufen ist. Im Genehmigungsprozess wird heute typischerweise auf die „Standardvertragsklauseln" der Europäischen Union und neuerdings auch auf das Modell der „Binding Corporate Rules" der Datenschutzbehörden zurückgegriffen, wobei der grundlegende Ablauf dabei immer gleich ist und somit auf die allgemeine datenschutzrechtliche Literatur verwiesen werden kann. Ein Beispiel für solche Fälle sind etwa breiter angelegte klinischen Prüfungen oder medizinische Studien, bei denen die Daten von Studienzentren aus mehreren Ländern auf verschiedenen Kontinenten zusammengeführt und ausgewertet werden. Auch wenn die Patientendaten in diesen anonymisiert sein sollten, so sind in solchen Studiendatenbanken dennoch meist personenbezogene Daten von Studienzentren, Prüfärzten, Sponsoren und deren Mitarbeitern enthalten, die dann über die EU-Grenzen hinaus übermittelt werden. Sofern nicht die Zustimmung jedes einzelnen Betroffenen eingeholt wird und das Argument der Notwendigkeit der Datenübermittlung zur Vertragserfüllung nicht greift, müsste ein derartiger Datentransfer dem entsprechend von der Datenschutzkommission vorab genehmigt werden. Im Genehmigungsverfahren etwa für Standardvertragsklauseln sollte man sich nicht von den wenigen Zeilen des Vordrucks im Anhang der Standardvertragsklauseln dazu verleiten zu lassen, dort nicht vollständig nachgeprüfte und gut definierte Zwecke oder Datenarten einzusetzen, weil die Datenschutzkommission jeden einzelnen Zweck und jede einzelne Datenart auf Plausibilität und Konsistenz nachprüft und bei Unklarheiten den Antrag auch abweist.

Für Datenübermittlungen, die etwa von Konzerngesellschaften zurück an die österreichische Konzernmutter eines Gesundheitsunternehmens erfolgen, ist aufgrund des räumlichen Anwendungsbereiches im Normalfall das Datenschutzrecht des dortigen Sitzstaates der Konzerngesellschaft anwendbar, sofern dies nicht ein EU Mitgliedsstaat ist und die Datenverwendung für die Zwecke der in Österreich gelegenen Konzernleitung geschieht. Dementsprechend sind für Datenübermittlungen aus diesen Ländern nach Österreich die dortigen materiellen als auch formellen Melde- und Genehmigungspflichten, sofern diese bestehen, zu berücksichtigen. Die Verarbeitung der von dort übermittelten Daten in Österreich kann zusätzlich nach österreichischem Datenschutzrecht beim DVR meldepflichtig sein.

Auch Outsourcing liegt – wie in anderen Branchen – im Gesundheitsbereich im Trend. Outsourcing erfolgt dabei sowohl extern als auch innerhalb des Konzerns, etwa bei der Erbringung von EDV-Dienstleistungen innerhalb des Konzerns oder der Erbringung verschiedener operationeller Tätigkeiten durch zentralisierte Stellen im Konzern. Innerhalb der Europäischen Union ist hierbei vor

allem auf die oft übersehene, datenschutzrechtlich geforderte vertragliche Ausgestaltung des Auftraggeber-/Dienstleisterverhältnisses zu achten.[23] Bei Outsourcing in Drittstaaten ist überdies die Frage der Genehmigungsfreiheit zu prüfen und, wenn diese nicht gegeben ist, eine Genehmigung einzuholen; dies unabhängig von materiellrechtlichen und datensicherheits- sowie technischen Fragen des Outsourcings. Auch zum Outsourcing ist wieder auf die allgemeine datenschutzrechtliche Literatur zu verweisen.

3. Zustimmungserklärungen

Häufig muss auf die Zustimmung des Betroffenen als Rechtsgrundlage zurückgegriffen werden bzw wird eine solche von den Materiengesetzen angeordnet. Das DSG 2000 definiert Zustimmung als die *„gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt"* (§ 4 Z 14).[24] In Anlehnung an § 9 Z 6 DSG 2000 sehen bspw das AMG und das GTG[25] vor, dass die Zustimmung zur Verwendung sensibler Daten, worunter auch Gesundheitsdaten zu verstehen sind (vgl § 4 Z 2 DSG 2000), nicht nur ausdrücklich, sondern darüber hinaus schriftlich zu erfolgen hat.[26] Die Formulierung solcher Zustimmungserklärungen ist durchaus „heikel", wie sich an der vielfältigen Judikatur des OGH der letzten Jahre zeigt.[27] Geht es um sensible Daten, so kann man sich weiterhin an die Grundsätze des Rundschreibens des BKA-VD vom 10.8.1985 zu 810.008/1-V/1a/85 leiten lassen, vor allem dann, wenn ein Schriftlichkeitsgebot besteht[28]. Diese Grundsätze lauten zusammengefasst:

1. Keine Kenntnisnahme als bloßer Bestandteil von AGB.
2. Deutliche Hervorhebung vom übrigen Text.
3. Deutliche Lesbarkeit der Erklärung (keine kleinere Schriftgröße).
4. Gesonderte Unterzeichnung der Erklärung.
5. Inhaltlich hat eine solche Erklärung folgende Angaben zu enthalten: Zweck der Datenanwendung, Bezeichnung der Datenarten, ausdrücklicher Hinweis

---

23 *Knyrim,* Outsourcing und Datenschutzrecht: Achtung, die Welt ist flach! ecolex 2009, 85.

24 Häufig auch *„informed consent"* genannt. Allgemeines zur Zustimmung nach DSG 2000 s *Dohr/Pollirer/Weiss,* DSG[2], Anm 15 zu § 4.

25 Für die Teilnahme an klinischen Studien s §§ 38 f Arzneimittelgesetz - AMG idF BGBl I 115/2008; für genetische Analysen s § 66 und § 69 Gentechnikgesetz – GTG idF BGBl I 13/2006.

26 Zwischen „AMG-Einwilligung" und „DSG-Zustimmung" zunächst differenzierend *Höhnel/Raschauer/Wessely,* Datenschutzrechtliche Fragestellungen im Zusammenhang mit klinischen Prüfungen, RdM 2006/76, um dann letztlich zu einer Parallelität zu gelangen.

27 Etwa OGH 4 Ob 28/01y ecolex 2001, 147 (mit Glosse *Rabl*) oder OGH 4 Ob 179/02 f ÖBA 2003, 41; eine Zusammenfassung sämtlicher E siehe *Knyrim,* Datenschutzrechtliche Zustimmungserklärungen richtig formulieren und platzieren, in *Knyrim/Leitner/Perner/Riss,* Aktuelles AGB-Recht (2008), 133 ff.

28 Dieses Rundschreiben erging zur alten Rechtslage (§ 7 Abs 1 Z 2 DSG 1978 BGBl 565/1978), der zufolge eine schriftliche Einwilligung geboten war. Es ist bei *Dohr/Pollirer/Weiss,* DSG[2], Anm zu § 4 sowie *Reimer* in *Jahnel/Siegwart/Fecher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2008) 208 abgedruckt.

auf den jederzeit möglichen schriftlichen Widerruf, allenfalls Benennung der Übermittlungsempfänger sowie der Übermittlungszwecke.

Weitere Anforderungen, insbesondere in Hinblick auf den Inhalt der Information, enthalten die jeweiligen Materiengesetze (§§ 38 f AMG, § 66 und 69 GTG). Eine besondere Herausforderung stellt die jederzeitige Widerrufbarkeit der Zustimmung dar. Ein solcher Widerruf hat nämlich zur Folge, dass die weitere Verwendung der Daten unzulässig wird und vorhandene Daten zu löschen sind.[29] Diese Pflicht kollidiert im medizinischen Bereich häufig mit gesetzlich verankerten Dokumentationspflichten.[30] Eine ausdrückliche gesetzliche Regelung bspw im AMG fehlt jedoch bislang. Der im Oktober 2008 zur Begutachtung ausgesandte Entwurf für eine AMG-Novelle[31] sah einen neuen § 39a vor, der jene Fälle enthielt, in denen eine Speicherung trotz Widerruf zulässig sein soll, was vielfach auf Kritik stieß.[32]

4. Pseudonymisierung und Anonymisierung von Patientendaten

Ein oft diskutiertes Thema ist die Pseudonymisierung und Anonymisierung von Patientendaten in klinischen Prüfungen oder sonstigen medizinischen Anwendungen wie etwa der Pharmakovigilanz.[33] Dazu ist zunächst auf einige gesetzliche Definitionen hinzuweisen: Personenbezogene Daten sind nach § 4 Z 1 DSG 2000 Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. In der Literatur wird zwischen primären und sekundären Identifikationsdaten unterschieden.[34] *„Primäre Identifikationsdaten sind Attribute oder Attributkombinationen, die von Natur her oder aufgrund ihrer Definition oder Verwendung dazu dienen, eine Person eindeutig zu identifizieren, auch wenn dazu eine Verknüpfung mit anderen Daten notwendig ist."*[35] Neben dem Namen sind daher auch Adresse, Sozialversicherungsnummer, Telefonnummer, Aufnahmezahl oder Untersuchungsnummer in einem Krankenhaus als primäre Identifikationsmerkmale zu qualifizieren (gleichzeitig sind sie personenbezogene Daten![36]). In diesem Falle ist die Identität bestimmt.[37] Sekundäre Identifikationsdaten sind jene Attribute einer Person, *„die bei Kombination und aufgrund der möglichen Attributwerte ein eindeutiges Muster ausprägen können, so dass in dieser Form*

29 Vgl § 8 Abs 1 Z 2 DSG 2000.

30 *Höhnel/Raschauer/Wessely,* Datenschutzrechtliche Fragestellungen im Zusammenhang mit klinischen Prüfungen, RdM 2006/76.

31 236/ME (XXIII. GP) Novelle zum AMG, GSG, KAKuG, BSG und GESG, abrufbar unter http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00236/pmh.shtml.

32 S ua die Stellungnahme des BKA-VD, http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00236_07/pmh.shtml .

33 Siehe etwa die Verpflichtung zur Einführung eine Informationssystems zur Pharmakovigilanz und zur Auskunftserstattung bzw. Meldungslegung in § 10 Abs 4 Pharmakovigilanz-VO BGBl II 472/2005 idF BGBl II 40/2009.

34 *Simonic/Gell,* Magdalena Datenschutz-Policy[1.1] (2001), http://www.meduni-graz.at/imi/de/projects/DS-Policy-FL-V1-1.pdf 11.

35 *Simonic/Gell,* Magdalena 11.

36 Zur Sozialversicherungsnummer als personenbezogenes Datum s die Empfehlung der DSK 6.9.2006, K210.523/0008-DSK/2006.

37 Vgl *Drobesch/Grosinger,* Datenschutzgesetz Anm zu § 4 Z 1, 117 f.

eine Identifikation des Betroffenen durch Verknüpfung mit anderen Daten möglich ist."[38] Meist handelt es sich um demographische Daten, die sich nicht oder nur selten ändern, wie bspw Geburtsort, Wohnort, Geburtsdatum, Religionsbekenntnis und Familienstand.[39] Sie machen eine Person daher bestimmbar.[40] Die Erläuternden Bemerkungen beziehen sich zur Konkretisierung der Bestimmtheit auf ErwGr 26 der Datenschutz-RL: *„Als mögliches Mittel zur Identifikation ist nur ein solches anzusehen, das ‚vernünftigerweise' angewendet wird, dh das also weder seiner Art nach, noch seinem Aufwand nach vollkommen ungewöhnlich ist."*[41]

Als Unterfall der bestimmbaren personenbezogenen Daten kennt das DSG 2000 den Begriff der indirekt-personenbezogenen Daten und definiert diese in § 4 Z 1 2. Fall wie folgt: *„nur indirekt personenbezogen sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann."* Es handelt sich hierbei um ein *Austriacum*, denn in der Datenschutz-RL sucht man den Begriff vergeblich und das deutsche BDSG kennt zwar die „Pseudonymisierung", womit de facto das Gleiche gemeint ist, verwendet ihn allerdings nicht um eine verminderte Schutzbedürftigkeit daran zu knüpfen[42], sondern im Hinblick auf den Grundsatz der Datensparsamkeit und -vermeidung.[43]

Daten – also etwa Patientendaten in einer Studie –, die niemand mehr auf eine Person zurückführen kann, sind anonym.[44] Dem DSG 2000 ist der Begriff „Anonymität" zwar gänzlich fremd, aber er findet sich im AMG und dem GTG, worunter jedoch lediglich das Verschlüsseln gemeint ist, und nach der Definition des DSG 2000 idR ebenfalls indirekt-personenbezogene Daten vorliegen.[45] Es stellt sich nun die Frage, wann bspw der Datensatz eines Patienten so hinreichend verschlüsselt ist, dass eine Re-Identifikation mit legalen mitteln unmöglich ist. Dies bestimmt sich an Hand mehrerer Faktoren, insbesondere den Schlüsselmerkmalen sowie Anzahl der in Betracht kommenden Personen.[46] Weiters ist

38 *Simonic/Gell*, Magdalena 11.

39 *Jautz*, Analyse und Umsetzung von Methoden zur Anonymisierung und Pseudonymisierung personenbezogener, medizinischer Daten (Diplomarbeit MedUniWien 2006), http://www.meduniwien.ac.at/msi/mias/studarbeiten/2006-DA-Jautz.pdf 10.

40 Vgl *Drobesch/Grosinger*, Datenschutzgesetz Anm zu § 4 Z 1, 117 f.

41 ErläutRV 1613 BlgNR 20. GP zu § 4 Z 1.

42 ErläutRV 1613 BlgNR 20. GP zu § 4 Z 1.

43 *Bizer* in *Simitis* (Hrsg), Bundesdatenschutzgesetz § 3a Rz 68.

44 ErläutRV 1613 BlgNR 20. GP zu § 4 Z 1.

45 S *Knyrim/Momeni*, Datenschutz bei klinischen Prüfungen, RdM 2003, 68 (70) (abrufbar unter: http://www.preslmayr.at/admin2/untermenue/pdf/10/20080630120202KY_DSR_RdM_Heft303.pdf) sowie ausdrücklich § 66 Abs 1 GTG.

46 S die Beispiele bei *Knyrim/Momeni*, Datenschutz bei klinischen Prüfungen, RdM 2003, 68, *Jautz*, Analyse und Umsetzung von Methoden zur Anonymisierung und Pseudonymisierung personenbezogener, medizinischer Daten (Diplomarbeit MedUniWien 2006), http://www.meduniwien.ac.at/msi/mias/studarbeiten/2006-DA-Jautz.pdf 19, *Simonic/Gell*, Magdalena Datenschutz-Policy[1.1] (2001), http://www.meduni-graz.at/imi/de/projects/DS-Policy-FL-V1-1.pdf 9 sowie Stellungnahme 4/2007 der Art-29-Datenschutzgruppe zum Begriff „personenbezogene Daten" WP, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf 15 f und 22 f. Im Bereich

zu berücksichtigen, welches Wissen für die Re-Identifikation notwendig und verfügbar ist. Hierbei ist jeweils auf den durchschnittlich zu erwartenden Informationsstand des angesprochenen Empfängerkreises abzustellen[47], also zB des Krankenhauspersonals. Auf Personen, welche aufgrund räumlicher oder emotionaler Nähe zum Betroffenen (zB Bekanntschaft, Verwandtschaft, Nachbarschaft) über Sonderwissen verfügen, welches die Identifizierung allenfalls ermöglicht, ist nicht Bedacht zu nehmen.[48] Das beim Auftraggeber tatsächlich vorhandene Wissen ist jedenfalls zuzurechnen.[49] Was etwa im Rahmen einer klinischen Prüfung noch als ausreichende Pseudonymisierung angesehen werden kann, wird unterschiedlich gesehen: In Österreich eher streng, dass nämlich die im Rahmen klinischer Prüfungen übliche Verschlüsselung durch Reduktion auf Initialen und Geburtsdatum der Patienten im Hinblick auf den lediglich eingeschränkten Personenkreis vielfach die Bestimmbarkeit der Identität nicht beseitigen,[50] während die französische Datenschutzkommission in der medizinischen Forschung die Verarbeitung der Initialen oder der ersten drei Buchstaben des Namens und das volle Geburtsdatum zulässt.[51] Siehe dazu auch weiter unten bei den Pharmakovigilanz-Datenbanken.

5. Interne Datenschutzrechts-Organisation und Mitarbeiterschulung

Die beste juristische Aufarbeitung von datenschutzrechtlichen Fragen in einem medizinischen Betrieb hilft nichts, wenn diese nicht durch Maßnahmen der internen Organisation und Schulung flankiert wird. Diese sind keine „freiwilligen Mehrleistungen", sondern ausdrückliche gesetzliche Verpflichtung: § 14 Abs 1 und 2 DSG 2000 fordert für alle Organisationseinheiten eines Auftraggebers (oder Dienstleisters), die Daten verwenden, Maßnahmen zur Gewährleistung der Datensicherheit. Insbesondere ist die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen, die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden und es sind die Mitarbeiter über ihre nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren.[52] Wie sich in der täglichen

---

der Statistik („statistical dislosure control") stößt man auf die gleichen Probleme (vgl dazu *CENEX-SDC* (Hrsg), Handbook on Statistical Disclosure Control (2006), http://neon.vb.cbs.nl/cenex/default.htm).

47 DSK 1.2.2005, K 120.854/0002-DSK/2005.

48 DSK 22.4.2005, K 120.966/0005-DSK/2005.

49 *Arning/Forgó/Krügel*, Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DuD 2006/11, 703, abrufbar unter http://www.iri.uni-hannover.de/kruegel.html?file=tl_files/pdf/Datenschutzrechtliche+Aspekte+der+Forschung+mit+genetischen+Daten.pdf.

50 *Hönel/Raschauer/Wessely*, Datenschutzrechtliche Fragestellungen im Zusammenhang mit klinischen Prüfungen, RdM 2006/76 (bei FN 32 mit Verweis auf *Knyrim/Momeni*, Datenschutz bei klinischen Prüfungen, RdM 2003, 68 (70).

51 CNIL Dokument MR-001 abrufbar unter http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/sante/MR-001.pdf, Seite 8 Fußnote 1.

52 § 14 Abs 2 Z 1 bis 3 DSG 2000.

datenschutzrechtlichen Beratung in verschiedensten Branchen oftmals zeigt, ist der Fokus bei Datensicherheitsmaßnahmen überwiegend auf die technischen Datensicherheitsmaßnahmen gerichtet,[53] nicht jedoch auf die ebenfalls geforderten organisatorischen Maßnahmen sowie die Mitarbeiterbelehrung, die sich nicht auf die bloße vertragliche Verpflichtung zum Datengeheimnis[54] beschränken kann, sondern datenschutzrechtliches Training beinhalten muss.[55] Ziel der Entwicklung einer internen Datenschutzorganisation muss sein, dass den einzelnen Mitarbeitern und den übergeordneten Verantwortlichen die Aufgabenverteilung und ihre Arbeitsanordnungen klar sind[56] und eine aktive Befassung mit dem Thema Datenschutzrecht für die Zukunft erreicht wird. Dies sollte dazu führen, dass etwa bei Änderungen in der Organisationsstruktur oder in der „IT-Landschaft" oder bei Software-Updates bei den Involvierten selbstständig darüber nachgedacht wird, ob dies allenfalls Auswirkungen auf bestehende DVR-Meldungen haben könnte, allfällige Vorabkontrollen nach § 18 Abs 2 DSG 2000 oder Genehmigungspflichten nach § 13 DSG 2000 ausgelöst werden oder sich ein Änderungsbedarf für Zustimmungserklärungen ergibt und dies intern an die dafür als verantwortlich bestimmte Stelle (etwa interner Datenschutzbeauftragter[57] oder der Rechtsabteilung) gemeldet wird, damit diese die nötigen Veranlassungen treffen.

6. Weitere Themen

Aus Platzgründen kann an dieser Stelle nur in Stichworten auf weitere Themen hingewiesen werden, die Unternehmen in Hinblick auf ihre Datenschutzrechts-Compliance beachten sollten: Zusätzlich zu den organisatorischen Datensicherheitsmaßnahmen sind die im Unternehmen geforderten spezifischen technischen Datensicherheitsmaßnahmen[58] besonders zu beachten.

Vor allem in Hinblick auf die voranschreitenden Möglichkeiten von EDV-Systemen zur Beurteilung und Bewertung der eigenen Mitarbeiter – etwa der Leistungsbeurteilung von Außendienstmitarbeitern – sollte geprüft werden, ob für deren Betrieb eine Zustimmung der Mitarbeiter (und allenfalls eine Betriebsvereinbarung nach § 96 oder 96a ArbVG oder – mangels Betriebsrat – in Kombination mit einer Zustimmung nach § 10 AVRAG) erforderlich ist oder, falls eine derartige schon besteht, diese erweitert werden muss. Eine derartige Zustimmung basiert auf § 8 Abs 1 Z 2 bzw § 12 Abs 3 Z 5 DSG 2000, ist jederzeit widerruflich und ist nicht zu verwechseln mit der vertraglichen Verpflichtung des Mitarbeiters zum Datengeheimnis nach § 15 Abs 2 DSG 2000.

---

53 § 14 Abs 2 Z 4 bis 7 DSG 2000.

54 § 15 Abs 2 DSG 2000.

55 Die Forderung nach Mitarbeiterschulung und Fortbildungsprogrammen der Mitarbeiter hinsichtlich Geldwäscherei und Terrorismusfinanzierung stellen *Bozkurt/Grubhofer,* Kredit- und Finanzinstitute, Geldwäsche und Terrorismusfinanzierung, OBA 2006, 242 (244) auf.

56 § 14 Abs 2 Z 1 und 2 DSG 2000.

57 Zum Fehlen einer gesetzlichen Regelung des Datenschutzbeauftragten im DSG 2000 siehe *Knyrim,* 25 Jahre Datenschutzrecht in Österreich – Bestandsaufnahme auf Lösungsansätze für aktuelle Probleme, MR 2005, 115.

58 § 14 Abs 2 Z 4 bis 7 DSG 2000.

E. Beispiele für Datenanwendungen

1. Pharmakovigilanz-Datenbanken

Das Arzneimittelgesetz (AMG) verpflichtet Pharmaunternehmen unerwünschte Ereignisse (vgl § 2a Abs 18 und Abs 20 AMG) und Nebenwirkungen (§ 2a Abs 19 und Abs 21 AMG) zu dokumentieren und in manchen Fällen den Behörden zu melden (§§ 41d und 41e sowie § 75b AMG). Die Pharmakovigilanz-V[59] enthält die diesbezüglichen Ausführungsbestimmungen. Zur Erfüllung dieser Verpflichtungen werden bei Pharmaunternehmen in ihrer Eigenschaft als Zulassungsinhaber häufig so genannte „Pharmakovigilanz-Datenbanken" eingerichtet. Die gänzliche anonyme Führung, mit der Konsequenz, dass das DSG 2000 nicht anwendbar wäre, ist deswegen nicht möglich, weil die Namen der Meldungsleger, sofern es sich dabei um medizinisches Personal gehandelt hat, den Behörden mitzumelden sind. Patientendaten sollten jedenfalls soweit wie möglich anonymisiert werden, siehe dazu schon oben im Punkt Anonymisierung und Pseudonymisierung. Je nach Anzahl der in Betracht kommenden Betroffenen sollte die Aufnahme von Initialen und der genauen Geburtsdaten in die Datenbank vermieden werden, weil eine Re-Indentifizierung an Hand dieser Daten nicht ausgeschlossen werden kann. In die Meldung an die Behörden sind diese Daten jedoch aufzunehmen,[60] was allerdings nicht ganz nachvollziehbar ist, da das „gelindere Mittel" iSd § 7 Abs 3 DSG 2000 auch eine Codierung des Patienten mittels eines Zahlen/Buchstabencodes auf den Formularen und auch in der EDV des Einmelders eine Re-Identifizierung durch den Einmelder (etwa durch eine bei diesem im Safe in Papierform aufbewahrte Codierungsliste) zulassen würde. Mangels in Betracht kommender Standardanwendung[61] für diese Datenanwendung ist diese meldepflichtig (vgl § 17 Abs 2 Z 6 DSG 2000).

Bei derartigen Pharmakovigilanz-Datenbanken kann ein Informationsverbundsystem nach § 50 DSG 2000 vorliegen. Solche Systeme – oder die Teilnahme an solchen – sind uU melde- oder genehmigungspflichtig bei der Datenschutzkommission.[62] Zu beachten sind weiters die Informationspflichten nach § 24 DSG 2000, die im Falle eines Informationsverbundsystems genau einzuhalten sind.

Von Informationsverbundsystemen zu unterscheiden sind ebenfalls in der Praxis häufig anzutreffende Datenbanken, bei denen lediglich die Daten im Ausland gespeichert werden, aber darüber hinaus andere Personen als Mitarbeiter des Pharmaunternehmens nur zu Dienstleisterzwecken Zugriff auf die Daten haben (zB CRO's, Personen zur Datenwartung, sonstige IT-Services). Unabhängig davon ob die Daten nur im Ausland gespeichert werden, oder zur Verwendung zu eigenen Zwecken des ausländischen Empfängers weitergegeben

59 V betreffend Pharmakovigilanzanforderungen und Pharmakovigilanzmeldungen (Pharmakovigilanz-Verordnung 2006 - PhVO 2006) BGBl II 472/2005.

60 Die entsprechenden Formulare sind unter http://www.basg.at/servlet/sls/Tornado/web/ages/content/E1FE9D29C1A62735C12570FA002F4126 abrufbar.

61 Anlage 1 zur StMV 2004.

62 Zu beachten ist, dass – mangels anderer Rechtsgrundlage – eine Zustimmung zum Informationsverbundsystem nicht notwendig ist, sondern nur für die internationale Übermittlung.

werden (oder dieser Zugriff erhält), ist diese Weitergabe meist genehmigungspflichtig, wenn der Empfänger in einem EU-Drittstaat ansässig ist, welcher weder durch Entscheidung der EU-Kommission noch eine nationale Verordnung gleichgestellt worden ist (vgl §§ 12, 13 DSG 2000) und nicht von jedem Betroffenen eine ausdrückliche Zustimmung für die Speicherung und/oder den Zugriff eingeholt wurde.[63] Während die oben zitierten Bestimmungen des AMG als Rechtsgrundlage für die Verarbeitung und Übermittlung an die Behörden dienen (§ 8 Abs 1 Z 1 bzw § 9 Z 3 DSG 2000), trifft dies für sonstige Übermittlungen etwa im Pharmakonzern nicht zu. Die Datenschutzbehörden fordern für die Genehmigung eines solchen Datentransfers daher eine genaue Zweckbeschreibung, dh es muss ein konkreter und nachvollziehbarer Grund genannt werden, warum die Zugriffsgewährung/Weitergabe in personenbezogener Form an eine ausländische Konzerngesellschaft oder die Einspeisung in eine Konzerndatenbank notwendig ist. Die Suche nach der Rechtsgrundlage ist also eine der Hauptschwierigkeiten in diesem Zusammenhang. Möchte man auf Nummer sicher gehen, sollte man von den Betroffenen (also vor allem den Mitarbeitern der Studienzentren, die Patientendaten sollten ohnehin anonymisiert sein) eine Zustimmung einholen. Bei der Formulierung der Zustimmungserklärung ist die strenge Judikatur des OGH einzuhalten, siehe zu dieser bereits oben.

2. Datenbanken von klinischen Studien

Im Rahmen klinischer Studien bietet sich an, die entsprechende Klausel über die Zustimmung der Datenverarbeitung der Mitarbeiter der Studienzentren bereits in den Vertrag mit dem Prüfarzt aufzunehmen. Eine Möglichkeit ist dabei, dass der Prüfarzt im Studienvertrag erklärt, dass er die Zustimmung von seinen Mitarbeitern eingeholt hat bzw. einholen wird, da es nicht praktikabel scheint, dass der Sponsor von jedem einzelnen betroffenen Mitarbeiter des Studienzentrums selbst die Zustimmung einholt.

Bei klinischen Studien zeigt sich in der Praxis, dass eine wesentliche Frage ist, wer Auftraggeber der Studie ist. Als Auftraggeber der Datenbank mit den Patientendaten kommen zunächst einmal die Prüfärzte selbst in Frage, da diese die Patientendaten unverschlüsselt in die Studiendatenbanken eingeben, womit diese eine DVR-Meldung über Studiendatenverarbeitung beim Datenverarbeitungsregister als Auftraggeber einreichen müssen, soferne keine Standardanwendung anwendbar ist.[64]

Erhält der Sponsor aus der Studie ausschließlich verschlüsselte Patientendaten und verarbeitet auch keine Daten über sonstige Beteiligte an der Studie (zB Mitarbeiter des Prüfzentrums, eigene Mitarbeiter), so liegt für ihn keine Meldepflicht vor. In der Praxis enthalten die Studiendatenbanken des Sponsors typischer Weise aber Hinweise zu den Prüfärzten bzw. deren Mitarbeitern und den eigenen, die Datenbank bearbeitenden Mitarbeiter, Mitarbeiter der CRO, so liegt

63 Siehe die Liste unter http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_de.htm.

64 Denkbar wäre die Anwendbarkeit der SA 0024 Patientenverwaltung und Honorarabrechnung, es hängt aber vom konkreten Zweck und den Datenarten und -übermittlungen im Einzelnen ab, ob eine Subsumtion unter diese möglich ist, insbesondere in Hinblick darauf, dass die SA 0024 als Basiszweck Patientenverwaltung und nicht Studiendurchführung hat.

auch für den Sponsor der Studie zusätzlich ebenfalls eine Meldpflicht vor und er muss als Auftraggeber seines Teils der Studienverarbeitung eine DVR-Meldung erstatten.

Die Studie kann eine rein österreichische Studie mit einem österreichischen Sponsor sein, kann aber auch eine internationale, multizentrische Studie sein, bei der der datenschutzrechtliche Auftraggeber seinen Sitz in einem anderen EU-Staat oder außerhalb der EU hat. Ist die Studie lokal unter der Verantwortung einer österreichischen Gesellschaft, so ist diese datenschutzrechtlicher Auftraggeber. Ist die Studie hingegen eine internationale, multizentrische Studie, die unter der Verantwortung einer außereuropäischen Konzerngesellschaft des Pharmaunternehmens durchgeführt wird, so könnte zunächst darüber diskutiert werden, ob auf diese überhaupt österreichisches Recht anzuwenden ist. Da der Ort der Datenermittlung bei den Patienten in Österreich aber Österreich ist, wird wohl auf diese österreichisches Recht anzuwenden sein. Wenn die österreichische Tochtergesellschaft des Konzerns in der Studie überdies als Dienstleister für jene Konzerngesellschaft, die die Studie durchführt, auftritt, ist dies ein weiterer Konnex zum österreichischen Recht und es läge eine Meldpflicht für eine solche internationale Studie in Österreich vor. Ein sinnvoller Weg wäre hier aufgrund Art 4 Abs 2 EU-Datenschutzrichtlinie, die österreichische Tochtergesellschaft als Repräsentanz („Vertreter") der außereuropäischen Konzerngesellschaft die DVR-Meldung einbringen zu lassen, wobei eine solche Konstruktion beim Datenverarbeitungsregister sehr selten gemeldet wird. Im Formblatt Anlage 1 zur Datenverarbeitungsregister-V ist diese Konstruktion in Punkt 5. bereits vorgesehen. Bei internationale Studien, die von einer europäischen Konzerngesellschaft durchgeführt werden, kann diese europäische Konzerngesellschaft direkt als Auftraggeber in der DVR-Meldung genannt werden, oder es wird ebenfalls eine Vertretungskonstruktion gewählt, wobei sich empfiehlt, diese Wahl vor Einreichung mit dem DVR zu besprechen.

In der Praxis ist es häufig so, dass die österreichische Konzerngesellschaft eines Pharmaunternehmen in Österreich sowohl nationale österreichische Studien in eigener Verantwortung als auch europäische oder internationale Studien in Vertretung anderer Konzerngesellschaft durchführt. Diesfalls sind allenfalls zwei oder mehr DVR-Meldungen einzubringen (etwa eine für österreichische Studien mit der österreichischen Konzerngesellschaft, eine für internationale Studien mit der außereuropäischen Konzerngesellschaft als Auftraggeber und der österreichischen Konzerngesellschaft als Repräsentanz und weiter für europäische Studien mit den europäischen Konzerngesellschaften als Auftraggeber oder Österreich als Repräsentanz.)

3. Datenbanken für Marketing gegenüber Ärzten

Marketing von Pharmaunternehmen gegenüber Ärzten geschieht im Regelfall durch Außendienstmitarbeiter, welche die Ärzte persönlich aufsuchen und darüber Besuchsberichte in Marketing-Datenbanken ablegen. Zunächst sollte man eine solche Marketing-Datenbank mit der Standardanwendung SA022 der Standard- und Musterverordnung[65] vergleichen. Sofern man sich im Rahmen dieser Standardanwendung bewegt, wird keine Meldepflicht ausgelöst. Die Standard-

65 Anlage 1 zur StMV 2004 BGBl II 312/2004.

anwendungen sind allerdings keine Rechtsgrundlage für die Datenbank. Sie stellen nur die formelle Voraussetzung für die Rechtmäßigkeit einer Datenanwendung dar. Es muss immer auch eine materielle Rechtsgrundlage vorhanden sein (§§ 7 bis 9 DSG 2000). Die im Regelfall einzige in Betracht kommende Rechtsgrundlage wird eine Zustimmung der Ärzte sein. In praxi könnte man diese von den Außendienstmitarbeitern schriftlich oder sogar mündlich einholen lassen.

Außendienstmitarbeiter verwenden bei ihrer Arbeit häufig mobile elektronische Geräte wie PDAs und Notebooks. Anders als in Deutschland ist dies für das DSG 2000 kein erheblicher Umstand, abgesehen von der Notwendigkeit der Ergreifung angemessener Datensicherheitsmaßnahmen. Wesentlich ist vielmehr, wer auf die Daten nach der Synchronisation mit dem Unternehmensserver des Pharmaunternehmens zugreifen kann und wie die Daten ausgewertet werden. Beides sollte genau analysiert und rechtlich geprüft werden, da Datenzugriffe etwa durch andere Konzerngesellschaften (inkl der Konzernmuttergesellschaft) wie Datenübermittlungen an Dritte zu behandeln sind und eine Rechtsgrundlage dafür vorhanden sein muss (zB eine Zustimmung der betroffenen Ärzte) und spezifische Datenauswertungen oder sogar Datenverknüpfungen ebenfalls eine Rechtsgrundlage (etwa Einschluss in eine Zustimmung) erfordern.

Zu Beachten sind in Marketing-Datenbanken weiters allfällige freie Textfelder, in die die Sachbearbeiter persönliche Anmerkungen einfügen können, was gerade bei Marketing-Datenbanken besonders weit verbreitet ist. Diese sollten nach Tunlichkeit vermieden werden, weil eine Steuerung des Inhaltes fast unmöglich ist und, wie die Praxis zeigt, in diesen regelmäßig sehr persönliche Informationen über die Beworbenen eingegeben werden (etwa über spezifische Interessen, Familienverhältnisse, persönliche Umstände), die zB im Falle eines Datenlecks oder -missbrauchs zu einer Bloßstellung des Beworbenen führen könnte, die in eine Schadenersatzforderungen durch diesen münden könnte. Besser ist daher, solche Freitextfelder zu streichen oder durch Felder mit vordefinierten Auswahlmöglichkeiten (zB drop-down-Menüs mit vorgefertigten, unbedenklichen Textbausteinen) zu ersetzen.

4. Gendatenbanken

In einer Gendatenbank werden genetische Informationen von Organismen gespeichert, bspw Gewebeproben. Bei Genproben ist zunächst zwischen dem eigentlichen Material (also der Blut- oder Gewebeprobe) und der daraus gewonnen Information (Ergebnisse der DNA-Analyse) zu unterscheiden.[66] Erstere fallen nicht in den Anwendungsbereich des DSG 2000, und sind Gegenstand besonderer Regelungen des GTG und des Gewebesicherheitsgesetzes (GSG).[67] Der Schutz des GTG erstreckt sich auf die aus den Genproben gewonnenen Informationen, die in den Anwendungsbereich des DSG 2000 fallen. Bedauerlich

66 S dazu die Stellungnahme 4/2007 der Art-29-Datenschutzgruppe zum Begriff „personenbezogene Daten" WP, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf 9 f. AA sind mit durchaus beachtlichen Argumenten *Stelzer/Lehner,* Datenschutz in Biobanken, ZfV 2008, 744 f.

67 BG über die Festlegung von Qualitäts- und Sicherheitsstandards für die Gewinnung, Verarbeitung, Lagerung und Verteilung von menschlichen Zellen und Geweben zur Verwendung beim Menschen (Gewebesicherheitsgesetz-GSG) BGBl I 49/2008.

ist, dass diese Normen ebenso wie andere medizinrechtliche Gesetze nicht ganz einfach mit dem DSG 2000 in Einklang zu bringen sind.[68] Dem Datenschutzrechtler ist es im Hinblick auf § 1 DSG 2000 am liebsten, wenn Daten anonymisiert sind. Im GTG könnte dies möglicherweise problematisch sein: Eine gänzliche Anonymisierung könnte nämlich gegen § 71 Abs 1 Z 2 GTG verstoßen. Dort heißt es unter der Überschrift „Datenschutz": *„Der untersuchten Person sind unerwartete Ergebnisse mitzuteilen, die von unmittelbarer klinischer Bedeutung sind oder nach denen sie ausdrücklich gefragt hat. Diese Mitteilung ist insbesondere dann, wenn die untersuchte Person nicht danach gefragt hat, so zu gestalten, dass sie auf die untersuchte Person nicht beunruhigend wirkt; in Grenzfällen kann diese Mitteilung gänzlich unterbleiben."* Man könnte nun aufgrund dieser Bestimmung annehmen, dass zum Zwecke der Information des Patienten über wichtige Informationen seiner Gesundheit die Entfernung des Personenbezuges geradezu unzulässig ist. Aus datenschutzrechtlicher Sicht wäre dies insofern unbedenklich, als die Verwendung der Daten im lebenswichtigen Interesse des Patienten erfolgt und sich somit auf die Rechtsgrundlage nach § 9 Z 7 DSG 2000[69] stützen könnte (Voraussetzung ist allerdings, dass die Zustimmung des Betroffenen nicht rechtzeitig eingeholt werden konnte, weshalb sich eine Aufnahme dieser Datenverwendung in die Zustimmungserklärung zur klinischen Prüfung anbietet). Gegen diese Rechtsansicht könnte man einwenden, dass § 66 Abs 1 GTG Genanalysen an anonymen Proben – wozu im Rahmen des GTG, wie bereits erwähnt, auch indirekt-personenbezogene Daten gehören – vorsieht.[70]

Auch das GSG enthält mit dem DSG 2000 divergierende Vorschriften. Nach § 5 Abs 1 GSG sind die Ergebnisse der Beurteilung der gesundheitlichen Eignung der Spender von der Entnahmeeinrichtung zu dokumentieren sowie relevante anormale Befunde dem Leberspender mitzuteilen. Die Dokumentation ist mindestens 10 Jahre aufzubewahren; jene Teile der Dokumentation, die für eine lückenlose Rückverfolgbarkeit unerlässlich sind, sind mindestens 30 Jahre aufzubewahren.

Aufgrund des § 7 GSG wurde die Gewebeentnahmeeinrichtungsverordnung (GEEVO)[71] erlassen. Diese sieht in § 6 Abs 1 vor, welche Angaben die Spenderdokumentation für jeden Spender enthalten muss. Dazu zählt unter anderem die Spenderidentität (Z1), das Alter, Geschlecht, medizinische Verhaltensanamnese (Z2) und gegebenenfalls der Befund der körperlichen Untersuchung (Z3).

---

68 Dies fängt bereits mit den Begriffsdefinitionen an: Während nach der Diktion von GTG, AMG und MPG unter den Begriff der „anonymen Daten" auch indirekt personenbezogene iSd § Z 1 DSG 2000 fallen, versteht das DSG 2000 bzw die Datenschutz-Richtlinie 95/46/EG nur solche Daten als anonym, die unter Einsatz vernünftiger Mittel nicht mehr re-identifiziert werden können (Erwägungsgrund 26 der Datenschutz-RL).

69 Gesundheitsdaten sind sensible Daten iSd § 4 Z 2 DSG 2000.

70 Siehe dazu auch *Stelzer,* Datenschutz im Gentechnikrecht, in *Stelzer (Hrsg.),* Biomedizin – Herausforderung für den Datenschutz (2005), 79 (91 ff) sowie *Kotschy,* Datenschutzrechtliche Fragen zum geltenden österreichischen Gentechnikrecht, in *Kopetzki/Mayer (Hrsg.),* Biotechnologie und Recht (2002) 75 ff (81 ff).

71 Verordnung zur Festlegung von Standards für die Gewinnung von zur Verwendung beim Menschen bestimmter menschlicher Zellen und Geweben (Gewebeentnahmeeinrichtungsverordnung – GEEVO) BGBl II 191/2008.

Diese Informationen sind nach § 6 Abs 4 GEEVO mindestens 30 Jahre nach der klinischen Verwendung oder dem Verfalldatum in geeigneter Weise aufzubewahren. Auch diese Bestimmung widerspricht den Grundsätzen des DSG, nämlich der prinzipiellen Anonymisierung personenbezogener Daten. Man könnte allerdings argumentieren, dass das GSG und auch die GEEVO eine Rechtfertigung nach § 8 Abs 1 Z 1 betreffend nicht sensible Daten darstellen. Demnach sind bestehende schutzwürdige Geheimhaltungsinteressen bei Verwendung nichtsensibler Daten dann nicht verletzt, wenn eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht. Gleiches gilt für die Verwendung sensibler Daten nach § 9 Z 3 DSG, wenn sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen.[72]

F. Sanktionen

Neben verwaltungs- und justizstrafrechtlichen Rechtsfolgen (§§ 51 ff DSG 2000, diverse Delikte im StGB und der Haftung der juristischen Person nach dem Verbandsverantwortlichkeitsgesetz) ist bei Verstößen gegen gesetzliche Bestimmungen an § 1 UWG zu denken.[73] Aber die gefürchtetste Sanktion ist immer noch eine „Aufdeckerstory" in den Medien. Wenige Unternehmen werden es ohne weiteres verkraften, wenn in den Medien berichtet wird, dass sie die Rechte ihrer Kunden oder noch schlimmer, von Patienten, nicht beachten. Im Datenschutzrecht selbst drohen Verwaltungsstrafen bis rund EUR 19.000,-- sowie Freiheitsstrafen bis zu einem Jahr.[74]

Zusammenfassend kann Unternehmen und Organisationen im medizinischen Bereich nur empfohlen werden, sich verstärkt aktiv nicht nur um die laufende Aktuellhaltung der DVR-Meldungen zu kümmern, sondern sich auch mit anstehenden Themen wie etwa Genehmigung des internationalen Datenverkehrs, Datenschutz in klinischen Studien, bei Außendienst-Marketingdatenbanken oder Pharmakovigilanz-Datenbanken zu befassen. Ein bloßes „Zuwarten", ob Themen zu Problemen werden können, scheint etwa in Hinblick auf das negative Medienecho[75] zum „Arzneimittel-Sicherheitsgurt" nicht angebracht zu sein. Die Erfahrung zeigt, dass es wesentlich angenehmer ist, Themen mit dem Datenverarbeitungsregister und der Datenschutzkommission in „Ruhe" und ohne den Druck anstehender Beschwerden oder Anfragen auszudiskutieren und aufzuarbeiten um dann auch den Medien mit gutem Gewissen gegenübertreten zu können.

---

72 S zu Gewebedatenbanken weiters die GewebevigilanzV BGBl II 190/2008 sowie die GewebebankenV BGBl II 192/2008. Dies setzt freilich voraus, dass sich die Verwendungsermächtigung bereits aus dem GSG selbst ergibt, weil § 9 Z 3 DSG 2000 ausdrücklich von „gesetzlichen Vorschriften" und nicht etwa allgemein von Rechtsvorschriften spricht. Siehe auch den Überblick über die in Krankenanstalten anfallenden Datenschutzthemen im Zusammenhang mit Gentechnik bei *Schlemmer,* Aktuelle Probleme des Datenschutzes in der Krankenanstalt in Verbindung mit dem Gentechnikgesetz in *Stelzer (Hrsg.),* Biomedizin – Herausforderung für den Datenschutz (2005), 51.

73 Vgl *Jahnel/Thiele*, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004/55.

74 §§ 51 und 52 DSG 2000.

75 Siehe etwa „Die Presse" am 26.8.2007: „Arzneimittel-Sicherheitsgurt ist rechtswidrig" unter http://diepresse.com/home/politik/innenpolitik/325662/print.do.