

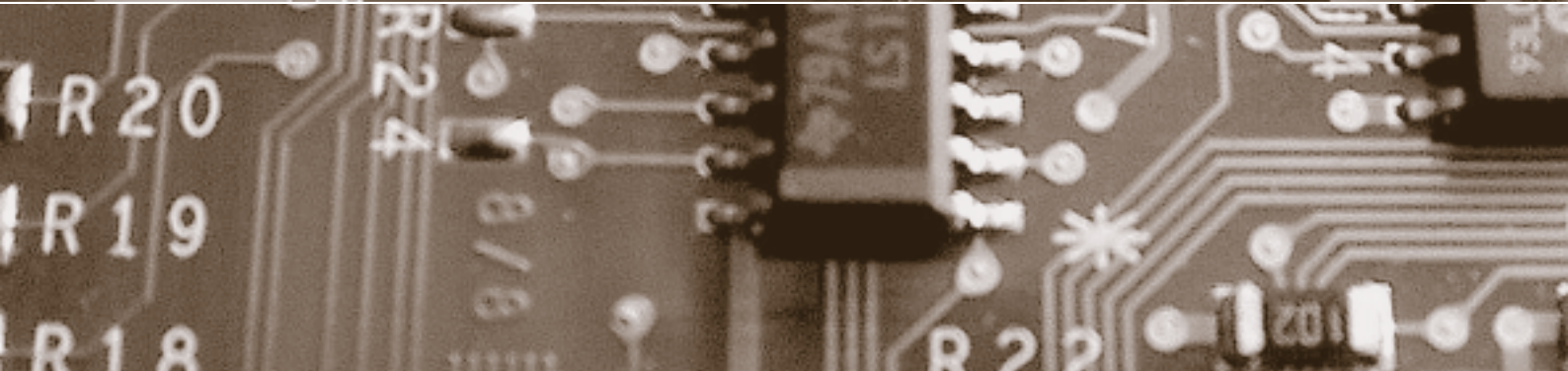
Schwerpunkt:

Anonymisierung

fokus: Das Recht auf Anonymität

fokus: Sind anonymisierte Daten anonym genug?

report: Drahtlose Sensornetze – eine Herausforderung



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

fokus



Schwerpunkt:

Anonymisierung

auftakt

Das Recht, in Ruhe gelassen zu werden
von Hans-Rudolf Merz

Seite 1

Der Schatten über der Anonymität
von Bruno Baeriswyl

Seite 4

Das Recht auf Anonymität
von Beat Rudin

Seite 6

zwischenakt

Der kleine Trick mit der Angst
von Urs Buess

Seite 13

Anonymisierung von genetischen Daten?
von Bruno Baeriswyl

Seite 14

Sind anonymisierte Daten anonym genug?
von Günter Karjoth

Seite 18

Anonymes E-Voting – eine Illusion?
von Rolf Oppliger

Seite 24

Folgerungskontrolle zum Schutz
von Information
von Joachim Biskup

Seite 28

Das Recht auf Anonymität ist ein Teil des Grundrechts auf informationelle Selbstbestimmung. In der Gesetzgebung finden wir etliche Gewährleistungen. Doch auch ausserhalb dieser Bereiche könnten mit Anonymisierungs- oder Pseudonymisierungslösungen in vielen Fällen die verfolgten Zwecke erreicht werden.

Das Recht auf Anonymität

Anonymisierung verhindert die Verletzung von Persönlichkeitsrechten. Ist das eine Lösung im Zusammenhang mit Biobanken? Jegliche Verwendung von Daten in einer Biobank setzt eine angemessene Aufklärung voraus.

Anonymisierung von genetischen Daten?

Wann reicht eine Anonymisierung aus, damit aus den anonymisierten Daten nicht doch wieder auf die betroffenen Personen zurückgeschlossen werden kann – und die Daten für den Forschungszweck trotzdem noch aussagekräftig genug sind?

Sind anonymisierte Daten anonym genug?

In der Theorie kann anonymes E-Voting mit Hilfe von blinden Signaturen relativ einfach realisiert werden. In der Praxis muss bei einer konkreten Realisierung eines E-Voting-Systems insbesondere darauf geachtet werden, dass nicht über verdeckte Kanäle Informationen über stimmberechtigte Personen z. B. in Tokens hineincodiert werden können.

Anonymes E-Voting – eine Illusion?

impresum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

Anzeigenmarketing: Publimag AG, Europastrasse 30, Postfach, CH-8152 Glattbrugg
Tel. +41 (0)44 809 31 11, Fax +41 (0)44 809 32 22, www.publimag.ch, info@publimag.ch

Herstellung: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

**Die Crux der
Auskunft über
Verstorbene**

Die Verordnungsregelung zur Herausgabe von Daten an die Angehörigen von Verstorbenen ist anspruchsvoll, weil sie eine Interessenabwägung voraussetzt. Unter welchen Voraussetzungen ist ein Privatversicherer zur Auskunft an die Angehörigen berechtigt? Wann besteht eine Pflicht dazu?

**Datenschutz und
wirtschaftliche
Realität**

Unter welchen Voraussetzungen kann die Wirtschaft Datenschutz realistischerweise umsetzen? Der Diskussionsbeitrag aus dem Kreis des Vereins Unternehmens-Datenschutz fordert mehr Anreize (z. B. Steuererleichterungen) für erwiesenermaßen datenschutzkonform handelnde Unternehmen. Steuererleichterung für die Einhaltung von Gesetzen – eine aus Sicht der Redaktion etwas realitätsfremde Forderung.

**Drahtlose Sensor-
netze – eine
Herausforderung**

Drahtlose Sensornetze werden als die nächste Technologiewelle nach RFID gehandelt. Dabei offenbaren die im Beitrag erörterten Anwendungsfelder, dass es ratsam ist, datenschutzrechtliche, aber auch ethische Fragestellungen frühzeitig zu erörtern.

**Europarechtliche
Herausforde-
rungen**

Bund und Kantone stehen zurzeit im Evaluationsverfahren der EU im Hinblick auf die Assoziation der Schweiz an Schengen/Dublin. Passend dazu ist ein Buch erschienen, das umfassend die europarechtlichen Vorgaben darstellt, nach denen sich das schweizerische Datenschutzrecht künftig zu richten hat.

report



RECHT IN DER PRAXIS
Die Crux der Auskunft über Verstorbene
von Martin Hofer **Seite 34**

BETRUGSPRÄVENTION
Fraud Management: Kampf dem IT-Betrug
von Stefan Nöpflin **Seite 40**

RECHT UND PRAXIS
Datenschutz und wirtschaftliche Realität
von Esther Hefti
und Susanne Amrein-Fischer **Seite 42**

IT-SICHERHEIT
Unterwegs im World Wild Web
von Thomas Dübendorfer **Seite 46**

FORSCHUNG
Drahtlose Sensornetze – eine Herausforderung
von Dirk Westhoff
und Heinrich Stüttgen **Seite 48**

RECHTSPRECHUNG
Vertrauensarzt bis-repetitas
von Amédéo Wermelinger **Seite 50**

TRANSFER
Wie ist die Lage in der Informationssicherheit?
von Roland Portmann **Seite 52**

forum



BUCHBESPRECHUNG
Europarechtliche Herausforderungen
von Beat Rudin **Seite 54**

agenda **Seite 55**

schlussakt
Wo sind die Liberalen in der Schweiz?
von Beat Rudin **Seite 56**

Cartoon
von Hanspeter Wyss

Anonymisierung von genetischen Daten?

(Datenschutz)rechtliche Aspekte der Anonymisierung bei Biobanken



Dr. iur. Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich, Zürich
bruno.baeriswyl@dsb.zh.ch

Jegliche Verwendung von Daten in einer Biobank setzt eine angemessene Aufklärung der betroffenen Personen voraus. Daran ändern auch die Anonymisierung oder Pseudonymisierung nichts.

Bei der Errichtung von Biobanken steht aus datenschutzrechtlicher Sicht die Frage der Aufklärung und der Einwilligung der Person, welche Gewebeproben und weitere Informationen zur Verfügung stellt, im Vordergrund. Biobanken enthalten biologisches Material, insbesondere Gewebeproben, Blut oder sonstige menschliche Körpersubstanzen. Daneben sind in Biobanken oftmals eine grosse Anzahl von sogenannten «Lifestyle»-Daten, zu denen etwa Informationen zu Essgewohnheiten, Nikotin- und Alkoholkonsum, sportliche Tätigkeiten, gesundheitliche Probleme und weitere demografische Daten gehören, gespeichert.

Bei Biobanken handelt es sich sowohl um kleinere Datenbanken als auch zunehmend um grosse Datensammlungen, die mehr oder weniger systematisch diese Art von Daten sammeln. Seit einigen Jahren wird der systematischen Anlegung von Biobanken in Forschung und Wissenschaft, aber auch in der Industrie eine grosse Bedeutung zugemessen. Einerseits erhofft man sich mit der genetischen Forschung neue Erkenntnisse, und andererseits will die Industrie ihre Produkte genauer auf die genetische Disposition eines Menschen abstützen.

Sensible Informationen

Zweifellos liegen in den Biobanken sehr sensible Informationen. Die verschiedenen Angaben zum «Lifestyle» einer Person sind insgesamt geeignet, ein Persönlichkeitsprofil über diese zu erstellen. Das Datenschutzgesetz qualifiziert solche Informationen als besonders schützenswerte Personendaten (Art. 3 lit. c DSG). Ebenso können

aus den Körpersubstanzen Informationen abgeleitet werden, die als besonders schützenswert gemäss dem Datenschutzgesetz zu gelten haben, beispielsweise Informationen zum Gesundheitszustand einer Person.

Damit ist auch klar, dass das Bearbeiten von Informationen in einer Biobank als schwerer Eingriff in die Persönlichkeitsrechte der betroffenen Person gilt. Die Bundesverfassung (Art. 119 BV) gibt dabei vor, dass ein solcher Eingriff mit der notwendigen Transparenz zu erfolgen hat.

Die Frage der Transparenz der Datenbearbeitung steht demnach bei den Biobanken im Vordergrund. Die betroffene Person hat über die Datenbearbeitung aufgeklärt zu werden und in die Verwendung der Daten einzuwilligen. Gerade bei breit angelegten Biobanken ist der Verwendungszweck aber oftmals nicht auf ein bestimmtes Forschungsprojekt ausgelegt. Deshalb kann im Zeitpunkt der Datenerhebung noch nicht abschliessend über die Verwendung der Daten informiert werden. Damit zusammenhängend stellt sich das Problem der Einwilligung. Um rechtmässig zu sein, hat sie im Wissen um und mit Klarheit über die Risiken für die Persönlichkeitsrechte zu erfolgen.

Anonymisierung zur Risikoreduktion?

Aufgrund dieser Schwierigkeiten stellt sich die Frage, ob nicht mit anonymisierten Daten das Risiko für die Persönlichkeitsrechte bei den Biobanken umgangen werden kann.

«Anonym» in diesem Zusammenhang muss bedeuten, dass eine Person, von der sich Informationen in der Biobank befinden, über diese nicht mehr (re)identifizierbar ist. Zunächst stellt sich dabei die Frage, ob menschliche Körpersubstanzen überhaupt anonymisierbar sind. Grundsätzlich ist dabei festzuhalten, dass menschliche Körpersubstanzen über die genetische Analyse immer einer bestimmten Person zuordenbar sind. Am deutlichsten wird dies heute bei der Spurensicherung in der Strafverfolgung ersichtlich, wo DNA-Analysen von Körpersubstanzen und der Abgleich mit DNA-Profilen von Tatverdächtigen oder von in DNA-Datenbanken verzeichneten

Personen nichts anderes bezwecken als die Identifikation einer Person. Wer demnach unter einen Tatverdacht fällt oder wer aus den gesetzlich zugelassenen Gründen in einer DNA-Datenbank verzeichnet ist, muss damit rechnen, dass in einem bestimmten Zusammenhang seine Körpersubstanzen identifizierbar werden.

Wie steht es nun mit den menschlichen Körpersubstanzen, die in einer Biobank abgelegt sind? Die Feststellung, dass Körpersubstanzen nicht grundsätzlich anonymisierbar sind, bleibt bestehen. Doch wenn lediglich Substanzen ohne Bezug zu weiteren Daten aufbewahrt sind und der Zweck ihrer Aufbewahrung nicht die Identifikation einer Person ist, wird die Wahrscheinlichkeit der Identifikation sehr gering. Somit würden in diesem Fall die datenschutzrechtlichen Bestimmungen nicht zur Anwendung gelangen, da keine Personendaten bearbeitet werden. Personendaten im datenschutzrechtlichen Sinne sind nur Daten, die sich auf eine bestimmte oder eine bestimmbar Person beziehen (Art. 3 lit. a DSGVO). Bestimmbar bedeutet in diesem Zusammenhang, dass der Aufwand in einem üblichen Rahmen liegt und eine Identifikation der Person auch ohne spezifische Anstrengungen erfolgen kann. Bei Biobanken ist deshalb zu berücksichtigen, dass in diesem Kontext objektiv betrachtet davon auszugehen ist, dass der Aufwand zur Identifikation einer Person unverhältnismässig hoch ist und mindestens von den mit der Forschung beschäftigten Personen nicht beabsichtigt ist.

Fragen der menschlichen Würde

Der Ausschluss der datenschutzrechtlichen Bestimmungen bedeutet nicht, dass eine solche Verwendung von Körpersubstanzen nun gänzlich ohne den Einbezug der betroffenen Person möglich wäre. Grundlegend stellt sich die Frage der menschlichen Würde beim Einbezug eines Menschen in die Forschung. Diese ist auch zu respektieren, wenn nur geringfügig Körpersubstanzen betroffen sind. Indessen werden sich andere Anforderungen an die Aufklärung der betroffenen Personen und deren Einwilligung stellen. Die Aufklärung könnte dabei sogar Teil einer allgemeinen Forschungsbewilligung sein, wobei hier auch Ethikkommissionen eine wichtige Rolle spielen könnten.

Anonymisierung der Informationen

Wie eingangs erwähnt, bestehen Biobanken neben Körpersubstanzen aus einer grossen Anzahl demografischer Daten einer Person. Diese Daten lassen sich grundsätzlich anonymisieren, so dass kein Bezug auf eine bestimmte oder bestimmbar Person mehr vorliegt. Damit würde wiederum die Anwendbarkeit datenschutzrecht-

licher Bestimmungen ausgeschlossen, da keine Bearbeitung von Personendaten vorliegt. Allerdings erscheint eine solche Anonymisierung in einer primären Biobank, bei der die Daten mehrheitlich bei der betroffenen Person oder aus mit ihr verbundenen Unterlagen erhoben werden, eher theoretisch. Die Erfassung von Lifestyle-daten hat gerade die möglichst genaue Beschreibung des Individuums zum Zweck, womit eine Identifizierung erleichtert wird. Doch je weiter entfernt von diesem Kontext, desto eher erscheint eine (Re)Identifizierung ohne einen übermässigen Aufwand nicht mehr möglich.

Aus einer datenschutzrechtlichen Sicht kann deshalb das Bearbeiten von biologischem Material und Daten als anonym und deshalb nicht unter das Datenschutzgesetz fallend betrachtet werden. Indessen löst diese Sichtweise nur einen

Grundlegend stellt sich die Frage der menschlichen Würde beim Einbezug eines Menschen in die Forschung.

Teil der datenschutzrechtlichen Problematik: Die Verwendung solcher Daten ist keinen datenschutzrechtlichen Schranken mehr unterworfen. Hingegen bleibt für die *Erhebung* solcher Daten das Datenschutzgesetz massgebend, soweit Daten von identifizierbaren Personen erhoben werden. In jedem Fall ist deshalb die Frage der notwendigen Aufklärung und Einwilligung näher zu betrachten. Wie gesehen ist diese Frage auch aus ethischer Sicht und unter dem Aspekt der menschlichen Würde nicht ausser Betracht zu lassen.

Kurz & bündig

Mit der Anonymisierung von Personendaten lassen sich Eingriffe in die Persönlichkeitsrechte weitgehend vermeiden. In Forschung und Statistik ist dies deshalb eine gängige Methode, um die Risiken für die betroffenen Personen zu beschränken.

Auch bei Biobanken stellt sich die Frage, wieweit mit einer Anonymisierung datenschutzrechtliche Fragen ausgeschlossen werden können. Grundsätzlich ist festzuhalten, dass eine Anonymisierung von Körpersubstanzen nicht möglich ist, hingegen die Qualifizierung auch von Körpersubstanzen als «anonym» im datenschutzrechtlichen Sinne nicht ausgeschlossen ist. Dennoch kann auch in diesem Fall nicht auf eine angemessene Aufklärung der betroffenen Personen verzichtet werden. Schon aus Gründen der menschlichen Würde und weiterer rechtlicher Ansprüche der betroffenen Person braucht es eine Aufklärung.

Aus diesem Grunde bilden die Richtlinien der SAMW zu Biobanken einen angemessenen regulatorischen Rahmen, der auch in einem zukünftigen Humanforschungsgesetz abzubilden wäre.



Generell lässt sich indessen festhalten, dass an eine Aufklärung weit weniger hohe Ansprüche in Bezug auf deren Detaillierungsgrad zu stellen sind, wenn keine Identifizierung im weiteren Verlauf der Datenbearbeitung möglich ist.

So sieht beispielsweise der Entwurf für das Humanforschungsgesetz¹ vor, dass die Weiterverwendung von biologischem Material in anonymisierter Form zu Forschungszwecken grundsätzlich erlaubt sein soll, wenn die betroffene Person nicht widersprochen hat. Über das Recht auf Widerspruch ist sie zu informieren.

Recht auf Wissen

Ob die Anonymisierung im diskutierten Sinne überhaupt in Betracht gezogen werden soll, ist noch aus einem anderen Grund zu hinterfragen. Gerade bei genetischen Untersuchungen und Forschungen muss berücksichtigt werden, dass

Bei genetischen Untersuchungen und Forschungen muss berücksichtigt werden, dass jeder Person ein Recht auf Wissen oder Nichtwissen zusteht.

jeder Person ein Recht auf Wissen oder Nichtwissen zusteht. Nur wenn das Recht auf Wissen nicht weiter zur Diskussion steht – wenn die betroffene Person sich für das Nichtwissen entschieden hat – kann überhaupt anonymisiert werden.

Wenn man allerdings auch hier der betroffenen Person die Möglichkeit einräumt, einen solchen Entscheid widerrufen zu können, wird die Anonymisierung als Möglichkeit bei Biobanken zunehmend fraglich.

Pseudonymisierung als Ausweg

Bei neu zu errichtenden Biobanken wird heute deshalb vor allem mit der Pseudonymisierung gearbeitet. Dieses Vorgehen – meistens als Codierung bezeichnet – arbeitet mit der Verschlüsselung insofern, dass der Zugang zu identifizierenden Informationen nur über einen speziell generierten Schlüssel möglich ist. Dabei kommen verschiedene Verfahren zur Anwendung, insbesondere auch die sogenannte doppelte Codierung, bei der die Wahrscheinlichkeit einer (Re)

Identifizierung ohne Schlüssel praktisch ausgeschlossen ist. Ein besonders datenschutzfreundliches Verfahren wurde auch zertifiziert². Als Kernfrage bei diesen Verfahren verbleibt die Regelung des Zugangs zum Schlüssel: Wer soll unter welchen Umständen eine Identifikation vornehmen dürfen? Da dieser Zugang von unterschiedlichen Interessen geprägt sein kann, wird auch erwogen, den Schlüssel einer vertrauenswürdigen Instanz («Trusted Third Party») zu übergeben. Allerdings ist dabei noch unklar, wer eine solche Rolle übernehmen kann.

Aufklärung und Einwilligung

Aus diesen Überlegungen wird klar, dass die Forschung mit Biobanken nicht um die Frage der Aufklärung und Einwilligung der betroffenen Person herumkommt. Der Entwurf für ein Humanforschungsgesetz und die Richtlinien der SAMW³ stecken heute die Rahmenbedingungen ab, wie eine solche Aufklärung erfolgen soll.

Generell soll die Forschung am Menschen, ob an ihm selbst als lebende oder verstorbene Person oder ob er der Forschung seine Materialien oder Daten zur Verfügung stellt, nur erlaubt sein, wenn eine Einwilligung nach hinreichender Aufklärung vorliegt. Ausnahmefälle müssen ausdrücklich in einem Gesetz geregelt sein.

Freiwilligkeit der Teilnahme

Diese Voraussetzungen müssen auch gegeben sein, um den Grundsatz der Freiwilligkeit der Teilnahme an einem Forschungsvorhaben gewährleisten zu können. Nur wenn sie gegeben ist, kann eine betroffene Person auch von ihrem Recht auf Widerruf einer einmal erteilten Einwilligung Gebrauch machen. Es kann verschiedene ethische Überlegungen geben, warum eine Person an einem bestimmten Forschungsprojekt teilnehmen oder nicht teilnehmen will. Dies ist zu respektieren.

Gemäss der erwähnten Richtlinie der SAMW muss die betroffene Person in verständlicher Form mindestens über die folgenden Punkte aufgeklärt werden:

- Art, Zweck, Dauer und Verlauf des Forschungsprojekts;
- die voraussehbaren Risiken und Belastungen;
- den erwarteten Nutzen für sie oder für andere Personen;

Fussnoten

¹ <<http://www.bag.admin.ch/themen/medizin/00701/00702/03990/03993/index.html?lang=de>> (letztmals kontrolliert: 28.1.2008).

² Vgl. digma 2005.1, 24 ff.

³ http://www.samw.ch/docs/Richtlinien/d_RL_Biobanken.pdf (letztmals kontrolliert: 28.1.2008).

- die Massnahmen zum Schutz der Personendaten;
- ihre Rechte.

Zwischen Aufklärung und Einwilligung ist der betroffenen Person eine angemessene Bedenkfrist zu geben. Die Einwilligung darf ohne Begründung verweigert werden, und die Verweigerung darf insbesondere nicht zu Diskriminierungen in der medizinischen Behandlung führen.

Abweichungen von der Aufklärung

Abweichungen vom Grundprinzip der aufklärten Einwilligung sollen möglich sein, wenn dies von einem Gesetz vorgesehen ist. Insbesondere die folgenden Situationen sehen Ausnahmen vor:

- Methodische Gründe sprechen für eine unvollständige oder erst nachträgliche Aufklärung;
- das Forschungsprojekt verfolgt ein wesentliches Ziel, und es ist unmöglich oder unzumutbar, die Einwilligung einzuholen oder über das Widerspruchsrecht zu informieren, und es liegt auch keine dokumentierte Ablehnung der betroffenen Person vor.

Zum Inhalt der Aufklärung gehören unter anderem

- der Verwendungsbereich, insbesondere die Verwendung in späteren Forschungsprojekten sowie Angaben, ob eine kommerzielle Nutzung erfolgt;
- Schutz- und Sicherheitsmassnahmen;
- Dauer der Aufbewahrung;
- Einsichts- und Auskunftsrechte;
- Überprüfung durch unabhängige Kontrollorgane.

Die Einwilligung hat ebenfalls schriftlich zu erfolgen. Sie kann entweder generell in Bezug auf

die Aufnahme der Materialien und Daten in die Biobank erfolgen oder nur für ein spezifisches Projekt gegeben werden.

Fazit

Mit diesen Grundsätzen zur Aufklärung und Einwilligung werden das Recht auf Privatheit und

Die Forschungsfreiheit muss dort an Grenzen stossen, wo die Persönlichkeitsrechte und Fragen der menschlichen Würde tangiert werden.

die Anforderungen an die menschliche Würde angemessen umgesetzt, ohne dass die Forschungsfreiheit eingeschränkt wird.

Die Forschungsfreiheit muss deshalb dort an Grenzen stossen, wo die Persönlichkeitsrechte und Fragen der menschlichen Würde tangiert werden. Mit Aufklärung und Einwilligung kann in den meisten Fällen ein Interessenausgleich zwischen den Forschungsinteressen und den Persönlichkeitsrechten erzielt werden und die menschliche Würde angemessen berücksichtigt werden.

Dieser Ansatz hat sich bewährt. Angesichts der hohen Sensitivität der Daten in diesem Bereich rechtfertigt sich eine detaillierte und klare gesetzliche Regelung, wie dies der Entwurf zum Humanforschungsgesetz vorsieht. Allenfalls wäre zusätzlich, ähnlich dem medizinischen Berufsgeheimnis, auch für die Forschenden ein spezifischer Geheimnisschutz zu schaffen. ■

Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name _____ Vorname _____

Firma _____

Strasse _____

PLZ _____ Ort _____ Land _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: zs.verlag@schulthess.com

Homepage: www.schulthess.com

Schulthess 