Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Ein modernes Datenschutzrecht für das 21. Jahrhundert

Eckpunkte

Vorgelegt am 18. März 2010

Inhaltsverzeichnis

0. Vorwort

Heute ist es nahezu selbstverständlich, jederzeit und aller Orten erreichbar zu sein. Videokameras, die für Sicherheit sorgen sollen, sind ebenso selbstverständlich wie elektronische Helfer in allen Lebenslagen, z. B. Navigationshilfen und elektronische Sensoren, die die Temperatur in Wohn- und Arbeitsräumen regulieren. Diese Entwicklung hin zur allgegenwärtigen Datenverarbeitung hat aber auch ihre Kehrseite: Wir sind nie mehr wirklich allein und können unseren „Datenschatten“ nicht abschütteln, wir haben zudem kaum eine Möglichkeit, diesen überhaupt zu bemerken. Ob von staatlichen Stellen oder Unternehmen – unser Verhalten wird beobachtet, registriert und bewertet. Videoüberwachung folgt uns an allen möglichen Orten, wir können durch Ortungstechnik metergenau lokalisiert werden, Kundenkarten und Internet liefern die Daten für Konsum- und Persönlichkeitsprofile und Auskunfteien haben ein waches Auge auf unsere Zahlungsfähigkeit. Wie soll das Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen Datenverarbeitung ausgestaltet sein? Das heutige Datenschutzrecht gibt hierauf nur noch unbefriedigende Antworten und bedarf der Modernisierung. Datenschutz hat nicht nur eine Schutzfunktion, er beschreibt auch einen Gestaltungsanspruch der Betroffenen: Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Datenschutz ist Grundrechtsschutz und die Wahrung der informationellen Selbstbestimmung eine Funktionsbedingung einer menschenwürdigen Informationsgesellschaft. Als Grundlage einer Diskussion über eine Reform des Datenschutzrechts und als Grundlage für die Fortführung der Diskussion über grundrechtlich verbürgten Datenschutz legt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die nachfolgenden Eckpunkte vor. Bewusst enthält das Papier nur Eckpunkte, die keinen Anspruch auf Vollständigkeit erheben.

1. Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Hierfür sollten für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa ein pauschalierter Schadensersatzanspruch, eingeführt werden. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

2. Grundsätzliche Erwägungen

2.1. Zielbestimmungen und Grundstruktur des Gesetzes

Das Datenschutzrecht hat sich in seiner Grundstruktur in den letzten Jahrzehnten nicht verändert, obwohl sich die technischen Voraussetzungen der elektronischen Datenverarbeitung und der Umfang der dabei anfallenden personenbezogenen Daten und damit die Gefährdung des Persönlichkeitsrechts radikal gewandelt haben. Die Prämissen der Datenschutzgesetze entsprechen immer weniger den Bedingungen der heutigen technologischen und gesellschaftlichen Realität. Dies ist auch nicht verwunderlich, denn die wesentlichen Regelungskonzepte der Datenschutzgesetze stammen im Kern aus der Zeit der Großrechner, in der PCs und Internet noch unbekannt waren.

Eine Vielzahl von Spezialregelungen, die das Bundesdatenschutzgesetz (BDSG) ganz oder teilweise überlagern und verdrängen, haben das Recht für Anwenderinnen und Anwender wie Betroffene unübersichtlich und unverständlich gemacht. Obwohl das Bundesverfassungsgericht immer wieder die Bedeutung des Grundrechts auf informationelle Selbstbestimmung unterstrichen und dieses um das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergänzt hat, tritt die eigentliche Zielsetzung des Datenschutzes immer mehr in den Hintergrund, nämlich der Einzelnen/dem Einzelnen als Ausfluss ihrer/seiner Menschenwürde die Verfügungsmacht über die ihre/seine Person kennzeichnenden und prägenden Informationen zu sichern und sie/ihn nicht zum bloßen Objekt der Informationsverarbeitung anderer werden zu lassen. Die allgegenwärtige Datenverarbeitung bedroht dabei nicht nur die Menschenwürde, sie beschneidet auch die Handlungs- und Verhaltensfreiheit der/des Einzelnen, etwa wenn diese/dieser in einem videoüberwachten Raum ihr/sein Verhalten der Tatsache dieser Dauerbeobachtung anpasst. Die informationelle Selbstbestimmung ist, wie das Bundesverfassungsgericht wiederholt festgestellt hat, eine unverzichtbare Grundbedingung der Demokratie.

Oberstes Ziel einer Modernisierung des Datenschutzrechts muss es deswegen sein, die Betroffenen als Grundrechtsträger wieder in den Mittelpunkt zu rücken und den wachsenden Gefährdungen ihrer Menschenwürde und Handlungs- und Verhaltensfreiheit durch die technische Entwicklung und die moderne Massendatenverarbeitung entgegenzutreten.

Die Datenschutzreform sollte folgende wesentliche Elemente enthalten:

- Neue und konkrete Definition der Schutzziele des Datenschutzes als Grundlage und Maßstab aller datenschutzrechtlichen Regelungen und Maßnahmen:
    - In enger Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts müssen die Schutzziele des Datenschutzes neu und konkreter als bisher definiert und verbindlicher gestaltet werden. So sieht zwar bereits das geltende

Datenschutzrecht beispielsweise eine Zweckbindung für die Verwendung personenbezogener Daten vor. Dieses auch vom Bundesverfassungsgericht als zentraler Grundsatz des Datenschutzrechts hervorgehobene Prinzip wird jedoch in der Praxis immer wieder in Frage gestellt und unterlaufen. Ziel muss es daher sein, dieses bei einer Modernisierung zu stärken und seine Bedeutung erneut zu betonen.

- Ausgangspunkt muss der Schutz der/des Einzelnen vor der Gefährdung (nicht nur konkreter Beeinträchtigung) ihrer/seiner Menschenwürde und Handlungs- und Verhaltensfreiheit durch das Sammeln und Verwenden ihrer/seiner personenbezogenen Daten sein, d.h. von Informationen über sie/ihn, ihr/sein Verhalten, ihren/seinen Aufenthalt und ihr/sein Denken. Dieser Schutz muss sich auch auf die von ihr/ihm genutzten elektronischen Hilfsmittel und Kommunikationsformen erstrecken, die ihre/seine Persönlichkeit abbilden können. Maßgeblich muss dabei die Gefährdung für das Persönlichkeitsrecht und die Eingriffsintensität sein: Je höher das Gefahrenpotenzial ist, desto wirkungsvollere Schutzmechanismen sind erforderlich.
- Der notwendige Schutz ist insbesondere gekennzeichnet durch
    - eine strikte Beschränkung der Datenverarbeitung und -nutzung auf das Erforderliche,
    - eine konsequentere Zweckbindung der einmal erhobenen personenbezogenen Daten (ausführlicher hierzu Abschnitt 2.2.2.),
    - die größtmögliche Selbstbestimmung der Betroffenen und
    - Transparenz der Datenverarbeitung (ausführlicher hierzu: Abschnitt 2.2.4.).
- Die Verwirklichung dieser Schutzziele soll durch folgende Maßnahmen unterstützt werden:
    - ein grundsätzliches Verbot der Profilbildung (ausführlicher hierzu: Abschnitt 2.2.3.) und
    - eine Verpflichtung zur konsequenten Löschung („geregeltes Vergessen“).

  Hierbei kann es grundsätzlich keinen Unterschied machen, ob die Gefährdung von einer öffentlichen oder von einer nicht-öffentlichen Stelle ausgeht.

- Stärkung des BDSG und der Datenschutzgesetze der Länder als allgemeingültige datenschutzrechtliche Grundregelungen:

  Neben dem allgemeinen Datenschutzrecht gibt es in Bund und Ländern eine Vielzahl von spezialgesetzlichen Regelungen, die ganz oder teilweise an die Stelle des allgemeinen Rechts treten, ohne dass dies oft eindeutig geklärt wäre. Nach § 1 Abs. 3 BDSG geht z.B. jede Rechtsvorschrift des Bundes, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden ist, dem BDSG vor. Diese weitgehende Subsidiarität des BDSG trägt maßgeblich zur Unübersichtlichkeit und Unverständlichkeit des Datenschutzrechts bei. Die allgemeinen Regeln des BDSG und der entsprechenden Landesgesetze müssen deswegen als allgemeine Grundregelungen verankert werden, denen spezialgesetzliche Bestimmungen nur noch ausnahmsweise vorgehen, wenn und soweit sie ausdrücklich und eindeutig davon abweichen.

- Gleiche Regeln für öffentliche und nicht-öffentliche Stellen:

  Für die Gefährdung des Persönlichkeitsrechts spielt es keine Rolle, ob diese von einer öffentlichen oder einer nicht-öffentlichen Stelle ausgeht. Die Grundrechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind nicht nur Abwehrrechte gegenüber staatlichen Stellen. Die Rechtsordnung muss den Schutzgehalt dieser Grundrechte vielmehr auch im nicht-öffentlichen Bereich gewährleisten. Die Grundsätze des Datenschutzrechts gelten nach der Europäischen Datenschutzrichtlinie für den öffentlichen und nicht-öffentlichen Bereich gleichermaßen. Deswegen sollten soweit wie möglich gleiche Regeln für öffentliche und nicht-öffentliche Stellen gelten, insbesondere auch bei den Betroffenenrechten. Eine solche Vereinheitlichung würde zudem die Verständlichkeit des Rechts deutlich stärken.

- Integration des Datenschutzes in Produkte und Verfahren:

  Die bisherigen datenschutzrechtlichen Bestimmungen richten sich direkt nur an Anwenderinnen und Anwender und Betroffene, nicht aber an die Herstellerinnen und Hersteller sowie Entwicklerinnen und Entwickler von Produkten und Verfahren. Dadurch bleiben datenschutzrechtliche Belange bei der Entwicklung von Hard- und Software oft unberücksichtigt. Nachträglich aufgepfropfte Datenschutzmaßnahmen sind zudem vielfach ungenügend und unwirtschaftlich. Die technische Integration des Datenschutzes in Produkte und Verfahren, z.B. im Hinblick auf Datenvermeidung oder Datensparsamkeit sowie einfachen und wirkungsvollen Selbstdatenschutz der Nutzerinnen und Nutzer, würde dagegen spätere Datenschutzprobleme vermeiden helfen. Ähnlich wie bei der technischen Betriebssicherheit können Normen und Verfahren einen integrierten technischen Datenschutz fördern und gewährleisten. Dies ließe sich etwa dadurch erreichen, dass Aufsichtsbehörden Anordnungsbefugnisse erhalten, um „Schwarze Schafe“ zu kennzeichnen. Die Verleihung von Gütesiegeln

und die Durchführung von Auditverfahren können wirkungsvolle, marktsteuernde Anreize für besseren Datenschutz setzen. Letztlich tragen auch effektive Betroffenenrechte dazu bei, dass sich datenschutzfreundliche Angebote durchsetzen.

- Verstärkte Grundrechtssicherung durch technische und organisatorische Verfahren:

  Der grundrechtliche Schutz der Privatsphäre erstreckt sich nicht nur auf rechtliche Anforderungen an die Zulässigkeit der Datenerhebung und Datenverarbeitung, er umfasst auch technische und organisatorische Maßnahmen. Dies ergibt sich nicht erst aus dem Urteil des Bundesverfassungsgerichts zur Onlinedurchsuchung und dem neuen Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme. Bereits der Grundsatz der Erforderlichkeit der Datenerhebung zieht technische und organisatorische Maßnahmen zu seiner Umsetzung nach sich.

- Datenschutz als Bildungsaufgabe festschreiben:

  Effektiver Datenschutz muss heute stärker denn je bei den Betroffenen ansetzen. Sie können nur dann verantwortungsbewusst handeln, wenn sie sich der Gefahren für ihr Persönlichkeitsrecht bewusst sind und wissen, wie ihr Handeln sich auf sie selbst und auf andere Menschen auswirkt. Außerdem brauchen sie Kenntnisse darüber, wie sie sich gegen Gefährdungen schützen können, die mit der Nutzung von Informationstechnik verbunden sind. Die Vermittlung des Datenschutzbewusstseins muss als gesamtgesellschaftliche Aufgabe verstanden werden. Entsprechender Regelungen bedarf es deswegen nicht nur in den Datenschutzgesetzen, sondern auch in den Lehrplänen der Schulen und bei sonstigen Bildungseinrichtungen.

- Besserer Schutz für Minderjährige:

  Bei der Wahrnehmung der Datenschutzrechte handelt es sich um Grundrechtsausübung, für die es keine starre Altersregel gibt. Da die datenschutzrechtliche Einwilligung und die Geltendmachung von Betroffenenrechten nicht immer rechtsgeschäftlichen Charakter haben, greift auch der Minderjährigenschutz des Bürgerlichen Gesetzbuchs nicht immer. Unter Umständen treten Elternrechte und eigenständige Rechtsausübung Minderjähriger in Konkurrenz, insbesondere bei der Nutzung des Internets. Gerade hier ist die Gefahr, dass die Gutgläubigkeit und Unerfahrenheit von Kindern und Jugendlichen ausgenutzt wird, besonders groß. Deswegen bedarf es auch im Interesse der Anwenderinnen und Anwender klarer Regelungen, ab wann und unter welchen Voraussetzungen Minderjährige eigenständig einwilligen und ihre Betroffenenrechte wahrnehmen können.

Durch die vorgeschlagenen Maßnahmen werden die Betroffenen und die Gefährdung ihres Persönlichkeitsrechts durch die elektronische Datenverarbeitung mehr ins Zentrum des Datenschutzrechts gerückt. Dies muss Maßstab aller gesetzlichen Regelungen sein.

2.2. Grundsätze des Datenschutzes

Ausgehend von der Zielsetzung der Datenschutzgesetze und der Schutzziele für die Betroffenen sollten konkrete Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung und für alle Anwenderinnen und Anwender von Datenverarbeitung gleichermaßen gelten und sanktionsbewehrt sind.

2.2.1. Datenvermeidung und Datensparsamkeit, Erforderlichkeit

Der Grundsatz, personenbezogene Daten nur insoweit zu verarbeiten, als sie für die Erfüllung einer konkreten Aufgabe erforderlich sind, ist bereits seit langem im Datenschutzrecht verankert. Er muss auch bei der Gestaltung der technischen Systeme berücksichtigt werden. Das Gebot der Datenvermeidung und Datensparsamkeit ist zwar auch im geltenden Datenschutzrecht schon enthalten (z.B. § 3 a BDSG), es hat als allgemeine Zielvorgabe bislang aber kaum Wirkung entfaltet. Vielfach werden aber Datenverarbeitungssysteme und -verfahren angeboten und eingesetzt, bei denen mehr Daten erhoben werden oder einfach nur als Nebenprodukt anfallen, als eigentlich nötig wären. Einmal entstandene Datenbestände stellen aber per se eine Gefährdung des Persönlichkeitsrechts dar, weil sie immer für irgendwelche Zwecke nutzbar sind und entsprechende Begehrlichkeiten wecken. Verstöße gegen den Grundsatz der Datenvermeidung und Datensparsamkeit haben bislang keinerlei Konsequenzen zur Folge.

Zur Stärkung des Grundsatzes der Datenvermeidung und Datensparsamkeit werden folgende Regelungen vorgeschlagen:

- Konkretisierung des verfassungsrechtlichen Grundsatzes der Datenvermeidung und Datensparsamkeit.
- Anspruch der Betroffenen, für den konkreten Zweck nicht erforderliche Daten auch nicht zu erheben und zu verarbeiten, und Anspruch darauf, die von der verantwortlichen Stelle eingesetzten Systeme und Verfahren entsprechend auszurichten.
- Möglichkeit der Sanktionierung bei Nichtbeachtung dieses Grundsatzes.
- Schaffung eines datenschutzfreundlichen Identitätsmanagements: Das Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren.
- Verpflichtung, generell pseudonyme und anonyme Nutzungsmöglichkeiten anzubieten.
- Privacy by Design: Bevor ein neues System zur Erfassung personenbezogener Daten eingeführt wird, sollen die verantwortlichen Stellen sicherstellen, dass Datenschutz-

lösungen von Anfang an fest eingebaut werden und nicht erst in einem späteren Stadium hinzugefügt werden müssen.

Durch eine entsprechende Regelung könnte der Grundsatz der Datenvermeidung und Datensparsamkeit zu einer verbindlichen Norm werden, auf die sich Betroffene berufen können und deren Einhaltung von der Datenschutzaufsicht kontrolliert werden kann.

2.2.2. Grundsatz der Zweckbindung

Der Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind, und sofort zu löschen sind, wenn sie für diesen Zweck nicht mehr erforderlich sind, hat herausragende Bedeutung für die Gewährleistung des Persönlichkeitsrechts. In der datenschutzrechtlichen Praxis kann die Zweckbindung ihre ursprüngliche Schutzfunktion aber immer weniger ausfüllen, weil es häufig an einer klaren Zweckbestimmung bei der ursprünglichen Erhebung der Daten fehlt, zahlreiche Vorschriften unter sehr allgemein formulierten Voraussetzungen Zweckänderungen zulassen und eine zweckfremde Verwendung von Daten vielfach keine Konsequenzen nach sich zieht. Eine konsequente Zweckbindung personenbezogener Daten korrespondiert zudem mit dem verfassungsrechtlichen Gebot zur informationellen Gewaltenteilung.

Die folgenden Regelungen sollen die Zweckbindung stärken:

- Eine eigenständige Norm zur Zweckbindung unter den Datenschutzgrundsätzen, die
    - vor jeder Erhebung personenbezogener Daten eine konkrete Zweckbestimmung vorschreibt (Verbot der Vorratsdatenspeicherung),
    - eine strikte Zweckbindung von als „Beifang“ anfallenden Daten ohne gezielten Personenbezug enthält, sofern die vorrangige Löschung oder Sperrung dieser Daten nicht möglich ist,
    - eine strikte Zweckbindung für die Verwendung von Daten zu Zwecken der Datenschutzkontrolle, zur Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebs von Datenverarbeitungssystemen vorsieht.
- Zweckändernde Verwendungen von personenbezogenen Daten dürfen nur in klar definierten Ausnahmefällen zugelassen werden; gesetzlich vorgesehene Zweckbestimmungen dürfen nicht durch die Einwilligung der Betroffenen umgangen werden.
- Verstöße gegen die Zweckbindung müssen bußgeldbewehrt sein.
- Regelmäßiges Verwertungsverbot für Daten, die durch eine rechtswidrige Änderung des ursprünglichen Erhebungszwecks erlangt worden sind.

Eine verbesserte Zweckbindung stärkt die Selbstbestimmung der Betroffenen über den Umgang mit ihren persönlichen Daten und begegnet der zunehmenden Vernetzung unterschiedlicher Datenbestände, die auch vom Bundesverfassungsgericht als große Gefahr für das Persönlichkeitsrecht gesehen wird.

2.2.3. Verbot der Profilbildung

Die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen stellt eine besondere Gefahr für das Persönlichkeitsrecht dar. Auf diese Weise können die Persönlichkeit eines Menschen, sein Verhalten, seine Interessen und Gewohnheiten verfügbar und vorhersehbar gemacht werden, was u.a. eine gezielte Manipulation erlaubt, ohne dass sich die Betroffenen dessen überhaupt bewusst sind. Derartige Profile gibt es bereits in vielen Bereichen, etwa als Konsumentenprofil, Bewegungsprofil, Nutzerprofil im Internet etc. Der rasante technologische Fortschritt in vielen Bereichen lässt Unmengen an personenbezogenen Daten anfallen, oft nur als Nebenprodukt, deren Verknüpfung immer ausgefeiltere Profile möglich macht.

Zum Schutz der Betroffenen halten die Datenschutzbeauftragten des Bundes und der Länder deswegen folgende Maßnahmen für erforderlich:

- Eine gesetzliche Definition der Profilbildung.
- Die Bildung von Profilen sollte nur zulässig sein bei entsprechender konkreter gesetzlicher Grundlage, die dem besonderen Gefährdungspotential von Profilbildung Rechnung trägt, oder bei einer Einwilligung der/des Betroffenen.
- Eine wirksame Einwilligung setzt eine umfassende Information über Umfang und Herkunft der verwandten Daten, Zweck und Verwendung des Profils, verantwortliche Stelle und vorgesehene Löschungsfrist voraus.
- Die Einwilligung muss freiwillig und jederzeit widerrufbar sein. Der Widerruf muss die sofortige Löschung des Profils zur Folge haben, auch bei den Stellen, an die es übermittelt worden ist.

Nur durch eine strikte Reglementierung der Profilbildung kann in diesem besonders sensiblen Bereich die informationelle Selbstbestimmung gewährleistet werden.

2.2.4. Wahrung der Transparenz – Offene Datenverarbeitung

Die moderne Datenverarbeitung ermöglicht in erheblichem Umfang eine für die Betroffenen nicht offensichtliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Das Datenschutzrecht enthält eine Reihe von Vorschriften für eine transparente Datenerhebung (und Weiterverarbeitung), die in der Regel an bestimmte Technologien anknüpfen (Videoüberwachung, Chipkarten usw.). Es fehlt aber an einem übergreifenden technikunabhängigen Konzept. Auf der anderen Seite entstehen in großem Umfang ungezielt – quasi nebenher – bei der Inanspruchnahme informationstechnischer Systeme personenbeziehbare Daten (z. B. Protokoll- oder Verkehrsdaten), bei denen die unmittelbare Herstellung des Personenbezugs nicht intendiert, aber möglich ist. Diese Daten können sensitiv sein, da sie umfassende Auskünfte über die Verhaltensweise der/des Einzelnen geben können. Hierfür gibt es im geltenden Datenschutzrecht keine adäquaten Lösungen.

Ein spezifisches Problem intransparenter Datenerhebung (sowie Verarbeitung und Nutzung) ist die Ortung, d. h. die Feststellung des geografischen Standortes oder der räumlichen Bewegung von Personen oder Gegenständen, die Personen zugeordnet werden können. Hierfür bietet bisher nur das Telekommunikationsrecht eine bereichsspezifische Lösung an.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schlägt vor, zur Wahrung der transparenten Datenerhebung, -verarbeitung und -nutzung eine einheitliche, technikunabhängige Norm zu schaffen. Folgende Eckpunkte müssen dabei berücksichtigt werden:

- Mikrotechnologie und Digitalisierung ermöglichen in zunehmendem Maße die vom Betroffenen unbemerkte Datenerhebung. Daten können ungezielt, fast zufällig und als „Beifang“ der eigentlichen Prozesse erhoben werden. Hier ist für die Betroffenen größtmögliche Transparenz herzustellen. Dies bedeutet, dass die Erhebung personenbezogener Daten für die Betroffenen transparent sein muss und umgekehrt eine von den Betroffenen unbemerkbare Datenerhebung grundsätzlich verboten wird.
- Die Transparenz der Erhebung personenbezogener Daten zeichnet sich dadurch aus, dass die Betroffenen angemessen über die beabsichtigte Erhebung (und weitere Verwendung) der Daten zu informieren sind. Dafür sollten die Transparenzvorschriften einheitlich zusammengefasst werden:
    - Die Datenerhebung muss für die Betroffenen erkennbar sein. Die Funktionsweise und Art der zu erhebenden und verwendenden Daten müssen in verständlicher Form erkennbar gemacht werden.
    - Die Identität der verantwortlichen Stelle ist durch geeignete Maßnahmen erkennbar zu machen.

- Die Betroffenen müssen in geeigneter Weise darüber informiert werden, wie sie ihre Rechte geltend machen können.
- Die verantwortlichen Stellen müssen eine detaillierte Datenschutzerklärung in geeigneter Weise auf aktuellem Stand zugänglich halten.

- In diesem Sinne von den Betroffenen unbemerkt, dürfen Daten erhoben werden, wenn sie ausschließlich zu dem Zweck verarbeitet werden, die Nutzung automatisierter Verfahren und die automatische Kommunikation zwischen Datenverarbeitungsanlagen technisch zu ermöglichen. Dies muss auch für solche Daten gelten, die grundsätzlich geeignet sind, nachträglich auf einzelne Personen bezogen zu werden. Für diese Daten gilt:
  - Das Gebot der Datenvermeidung sollte gestärkt werden.
  - Die Daten sind unmittelbar nach Erfüllung ihres Zwecks zu löschen, ohne dass es auf eine entsprechende Aktivität der Betroffenen ankommt.
  - Die Daten dürfen (nach dem Vorbild von §§ 14 Abs. 4, 31 BDSG) nur für den Zweck der technischen Ermöglichung der Kommunikation verarbeitet und genutzt werden, was durch geeignete technische und organisatorische Maßnahmen abzusichern ist.
  - Die Daten sollten einem Verbot der weiteren Verwendung unterliegen, um Profilbildung und Verknüpfung zu verhindern.
  - Die notwendige Transparenz ist auch hier durch Datenschutzerklärung herzustellen.
  - Zur Unterstützung der o. g. Prinzipien ist der Einsatz datenschutzfreundlicher Technologien vorzuschreiben.
  - Verstöße sind mit wirksamen Sanktionen zu ahnden.
  - Zu prüfen ist, ob und inwieweit das Auskunftsrecht weiterhin auch für diese nur flüchtig gespeicherten Daten gelten soll.
- Die Voraussetzungen, unter denen eine Erhebung gestattet wird, sind technikneutral zu regeln. Nicht auf die Regulierung der einzelnen Techniken, sondern auf die Festlegung von Schutzzielen ist Wert zu legen (siehe Kapitel 3).
- Es ist eine allgemeine und technikunabhängige Regelung zur Verarbeitung von personenbezogenen Lokalisierungsdaten zu schaffen, die sich an den jeweiligen Risiken orientiert:
  - Die Tatsache der konkreten Ortung ist den Betroffenen in verständlicher Form anzuzeigen, etwa durch ein akustisches Signal, sobald die/der Betroffene geortet wurde.

- Beim Einsatz von Tracking-Systemen, also jede Form der Ortung durch Dritte, die Betroffene nicht beeinflussen können, ist die Einwilligung (nach dem Vorbild von § 98 TKG) vorzusehen.

- Selbst bei einer heimlichen, aber nach bereichsspezifischem Recht erlaubten Datenerhebung sind geeignete und effektive Benachrichtigungspflichten vorzusehen.

Es sollte eine allgemeine technikunabhängige Vorschrift zur transparenten Datenerhebung, -verarbeitung und -nutzung geschaffen werden.

Die gezielte heimliche Datenerhebung wird nur in Ausnahmefällen z. B. zur Strafverfolgung erlaubt, im Übrigen grundsätzlich untersagt. Das Verbot wird durch Verwertungsverbote und Sanktionen abgesichert.

2.3. Beteiligung mehrerer Stellen an der Datenverarbeitung/Cloud Computing

Das BDSG kennt – ebenso wie eine Reihe von Landesdatenschutzgesetzen – keine ausdrückliche Regelung für eine gemeinsame Verarbeitung personenbezogener Daten durch mehrere Stellen. Anders als die Europäische Datenschutzrichtlinie kennt das BDSG beim Begriff der verantwortlichen Stelle nicht die Möglichkeit einer gemeinsamen Verantwortlichkeit mehrerer Stellen („joint controllership"). Eine wachsende Bedeutung kommt in der Praxis zentralen IT-Verfahren zu, an denen verschiedene Stellen von Bund und Ländern, mehrere Länder oder gar nicht-öffentliche Stellen beteiligt sind.

Es ist außerordentlich schwierig, solche Verfahren gesetzeskonform zu betreiben, weil die klassischen Instrumente Auftragsdatenverarbeitung oder Übermittlung nicht passen und zudem völlig unterschiedliche und z. T. einander widersprechende datenschutzrechtliche Normen des Bundes und der Länder beachtet werden müssten. Außerdem sind u. U. zahlreiche Kontrollbehörden für die datenschutzrechtliche Kontrolle nebeneinander zuständig.

Weitere Fragen wirft auch die verteilte und häufig grenzüberschreitende Datenverarbeitung auf, wie es z. B. beim Cloud Computing oder beim Binnenmarktinformationssystem IMI der Fall ist. Solche Konstellationen sind mit dem Datenschutzrecht nicht befriedigend in Einklang zu bringen. Das Instrument der Auftragsdatenverarbeitung lässt sich in der Praxis nicht umsetzen. Legt man die Funktionsübertragung (mit Übermittlung von Daten zwischen den beteiligten Stellen) zugrunde, ist die Verteilung der Verantwortlichkeiten nicht befriedigend zu regeln.

Aus diesen Gründen sollte das Konzept der Zuweisung von Verantwortlichkeiten neu gefasst werden:

- Der Begriff der verantwortlichen Stelle ist an dem Vorbild von Art. 2 lit. d) der EG-Datenschutzrichtlinie zu orientieren.
- Die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung ist bei der Beteiligung mehrerer Stellen durch entsprechende Vorschriften von den tatsächlichen Einflussmöglichkeiten und der Interessenlage der Betroffenen abhängig zu machen (Prinzip der Accountability). Die datenschutzrechtliche Verantwortlichkeit kann demnach z. B. auch nach einer Übermittlung fortbestehen, wenn die wirtschaftlichen bzw. tatsächlichen Einwirkungsmöglichkeiten auf die Empfänger dafür vorhanden sind.

Für gemeinsame Verfahren müssten folgende Anforderungen berücksichtigt werden:

- Festlegung materieller und formeller Anforderungen an die Zulässigkeit gemeinsamer Verfahren (Abwägung mit den schutzwürdigen Belangen Betroffener; bei Verfahren mit erheblicher Bedeutung ggf. gesonderte Rechtsgrundlage).
- Integration der Vorschriften zu den Abrufverfahren (§ 10 BDSG) als eine Form des gemeinsamen Verfahrens.
- Einführung spezifischer technischer und organisatorischer Sicherungen (z. B. zwingende Vorabkontrolle).
- Verpflichtung, die Verantwortlichkeiten für die Umsetzung der fachlichen und technischen Vorgaben eindeutig festzulegen.
- Verpflichtung, die Verantwortlichkeiten für die Rechtmäßigkeit der Datenverarbeitung zu dokumentieren.
- Verpflichtung, sowohl das anwendbare Datenschutzrecht als auch die zuständigen Datenschutzkontrollbehörden zu regeln.
- Sicherstellung, dass die Betroffenen gegenüber jeder beteiligten Stelle ihre Rechte geltend machen können.

Die Neufassung des Begriffs der verantwortlichen Stelle sowie die Einführung des Prinzips der nachhaltigen Verantwortlichkeit („Accountability“) ermöglichen vor allem bei der Beteiligung mehrerer Stellen an der Datenverarbeitung eine interessengerechte Verteilung der Verantwortlichkeit. Jede Stelle ist verantwortlich, wenn und soweit sie in tatsächlicher Hinsicht über Mittel und Zwecke der Datenverarbeitung verantwortlich bestimmen kann. Die Betroffenen können ihre Rechte gegenüber jeder verantwortlichen Stelle geltend machen.

2.4. Datenverarbeitung im Auftrag

Bei der Einbeziehung Dritter im Rahmen der Auftragsdatenverarbeitung hat der Gesetzgeber durch die letzten Änderungen des § 11 BDSG Präzisierungen und Klarstellungen vorgenommen, deren Auswirkungen zunächst abzuwarten sein werden. Ungelöst ist allerdings nach wie vor die Frage der zulässigen Auftragsdatenverarbeitung, wenn die Daten bei der Auftraggeberin/beim Auftraggeber durch Berufsgeheimnisse i. S. v. § 203 StGB geschützt sind. Da die Weitergabe der Daten an die Auftragnehmerin/den Auftragnehmer zwar keine datenschutzrechtliche Übermittlung, wohl aber eine Offenbarung des Geheimnisses darstellt, gibt es hierfür keine Rechtsgrundlage. So kann die Inanspruchnahme von IT-Dienstleistungen durch Ärztinnen und Ärzte, Rechtsanwältinnen und Rechtsanwälte und Steuerberaterinnen und Steuerberater, aber auch durch Versicherungen in vielen Fällen nur auf die Einwilligung der Betroffenen gestützt werden. Gleiches gilt z.B. für die externe Archivierung von Patientenakten in Krankenhäusern, sofern das Landeskrankenhausrecht hier keine ausdrückliche Befugnis enthält.

Ein weiteres Problem ist die Auftragsdatenverarbeitung bei besonders sensitiven Daten (§ 3 Abs. 9 BDSG), wenn die Auftragnehmerin/der Auftragnehmer ihren/seinen Sitz in einem Drittland außerhalb der EU hat. Da hierfür die Übermittlungsvorschriften zu beachten sind (vgl. § 3 Abs. 8 Satz 3 BDSG), ist eine Auftragsdatenverarbeitung unter diesen Umständen – anders als in anderen Mitgliedstaaten der EU – kaum möglich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält folgende Schritte für notwendig:

- Schaffung einer eng begrenzten Offenbarungsbefugnis z.B. in § 11 BDSG und den vergleichbaren Vorschriften der Landesdatenschutzgesetze, um eine Strafbarkeit der Berufsgeheimnisträgerinnen und -träger auszuschließen.
- Einbeziehung der Auftragnehmerinnen und Auftragnehmer in die strafrechtliche Sanktionierung bei Verstößen gegen das Berufsgeheimnis (etwa durch Gleichstellung mit den Berufsgehilfen in § 203 Abs. 3 Satz 2 StGB).
- Schaffung der notwendigen strafprozessualen Begleitmaßnahmen (Zeugnisverweigerungsrecht, Beschlagnahmeschutz).

Für die Auftragsdatenverarbeitung in Drittländern ist eine spezifische Norm zu schaffen, die diese nicht von den Übermittlungsvoraussetzungen, sondern vom angemessenen Datenschutzniveau im Drittland abhängig macht.

Die Schaffung einer Offenbarungsbefugnis für eine Auftragsdatenverarbeitung durch Berufsgeheimnisträger würde es auch diesen Berufsgruppen in begrenztem Umfang ermöglichen, insbesondere IT-Dienstleistungen durch Dritte durchführen zu lassen.

Die Möglichkeit, grundsätzlich auch sensitive Daten in Drittstaaten außerhalb der EU im Auftrag verarbeiten zu lassen, würde Wettbewerbsnachteile deutscher Unternehmen gegenüber anderen europäischen Unternehmen beseitigen und insofern Chancengleichheit herstellen.

3. Technischer und organisatorischer Datenschutz

Das Recht auf informationelle Selbstbestimmung kann nur gewährleistet werden, wenn es durch besondere Vorkehrungen für die technische Durchführung und Organisation der Erhebung, Verarbeitung und Nutzung personenbezogener Daten gesichert wird. Angesichts der weit fortgeschrittenen Digitalisierung der automatisierten Datenverarbeitung und ihrer Allgegenwart, angesichts der Verkettbarkeit personenbezogener Daten kommt technischen und organisatorischen Schutzvorkehrungen eine immer größere Bedeutung zu. Die besten rechtlichen Verarbeitungsbeschränkungen sind praktisch wertlos, wenn ihre technische und organisatorische Absicherung fehlt oder mangelhaft ist.

Die Konzeption des BDSG und vieler Landesdatenschutzgesetze wird diesen Anforderungen indes nicht mehr gerecht. Die in der Anlage zu § 9 BDSG aufgeführten einzelnen Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes stammen noch aus der Zeit der Großrechnertechnologie und lassen sich nur noch mit Mühe auf die heutige Welt vernetzter und ubiquitärer Systeme übertragen. Es ist zu erwarten, dass sie für die weitere Entwicklung der IuK-Technologien noch weniger geeignet sein werden.

Im geltenden Recht finden sich nur punktuelle Lösungsansätze hinsichtlich der konzeptionellen Absicherung vor Datenschutzrisiken beim Einsatz automatisierter Verfahren. Dies betrifft auch Verfahren, bei denen eine Verarbeitung personenbezogener Daten nicht von vornherein intendiert, aber (ggf. zu einem späteren Zeitpunkt) möglich ist.

Die Konferenz der Datenschutzbeauftragten schlägt deshalb eine grundsätzliche Reform der Regeln zum technischen und organisatorischen Datenschutz vor, die folgende Aspekte berücksichtigen müsste:

- Die bisher in der Anlage zu § 9 BDSG beschriebenen Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes („10 Gebote“) sind durch die Definition elementarer Schutzziele zu ersetzen. Diese sollten folgende Bedingungen erfüllen:
    - Die Schutzziele sollten einfach, verständlich und praxistauglich sein.
    - Die Schutzziele sind an den Vorgaben des Datenschutzes zu messen, müssen längere Zeit Bestand haben und dürfen sich trotz aller Überschneidungen nicht allein an den Vorgaben der IT-Sicherheit orientieren.
    - Aus den Schutzzielen sollten sich die konkret in der Praxis zu treffenden Maßnahmen ableiten lassen. Die Maßnahmen müssen in einfachen, flexiblen und praxistauglichen Verfahren – durch Software unterstützt – umgesetzt werden können. Sie können die Basis für die Kriterien eines Datenschutzaudits bilden.

- Die Schutzziele müssen technologieunabhängig definiert werden.
- Die Schutzziele sind nachhaltig. Lediglich die Maßnahmen sind dem Stand der Technik anzupassen.
- Die Schutzziele sind so zu fassen, dass grundsätzliche rechtliche Anforderungen (z. B. Datenvermeidung/Datensparsamkeit, Zweckbindung oder Betroffenenrechte wie Berichtigung oder Löschung) technisch umgesetzt werden können.

- Entsprechend den genannten Anforderungen sind folgende Schutzziele aufzunehmen:
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität
  - Transparenz
  - Nichtverkettbarkeit (als technische Sicherung der Zweckbindung)
  - Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte)
- Die Umsetzung der Schutzziele durch technische und organisatorische Maßnahmen ist konzeptionell abzusichern:
  - Vor der Freigabe von Verfahren sind grundsätzlich die Risiken für das Recht auf informationelle Selbstbestimmung zu analysieren und die zur Beherrschung der Risiken zu treffenden Maßnahmen in einem Sicherheitskonzept zu beschreiben; das Sicherheitskonzept ersetzt nicht die Vorabkontrolle, sondern ist deren Bestandteil. Es kann zudem wichtige Grundlage eines Datenschutzmanagements sein.
  - Risikoanalyse und Sicherheitskonzept sind nach dem Stand der Technik regelmäßig fortzuschreiben.
- Die Umsetzung der Schutzziele muss konzeptionell zu einem möglichst frühen Zeitpunkt ansetzen:

  Technische und organisatorische Maßnahmen sind im Sinne eines vorgelagerten Systemdatenschutzes schon dann zu treffen, wenn in einem Verfahren die Möglichkeit besteht, dass personenbezogene Daten verarbeitet werden oder dass dies zu einem späteren Zeitpunkt intendiert ist.
- Angesichts der hohen Komplexität informationstechnischer Systeme ist eine gesetzliche Verpflichtung der verantwortlichen Stellen zu schaffen, den Betroffenen Methoden und Mittel des Selbstdatenschutzes zur Verfügung zu stellen; der Staat hat die

Verpflichtung, die informationelle Selbstverantwortung und das Prinzip des Selbstdatenschutzes zu fördern.

- Die Regelungsvorschläge gelten – wie bisher – gleichermaßen für den nichtöffentlichen und wie den öffentlichen Bereich.

Mit den o. g. Regelungsvorschlägen werden einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen, das Recht auf informationelle Selbstbestimmung durch technischen und organisatorischen Datenschutz zu sichern. Durch die technologieunabhängige Definition der Schutzziele ist die Nachhaltigkeit gewährleistet, sodass keine fortlaufenden Anpassungen notwendig werden und das Recht nicht permanent der Technik hinterherhinkt.

Defizite bei der Umsetzung der technischen und organisatorischen Maßnahmen können durch dokumentierte Risikoanalysen und Sicherheitskonzepte abgebaut werden.

Mit den Vorschlägen kann der Einsatz datenschutzfreundlicher Technologien – auch zur Stärkung der Eigenverantwortung und des Selbstdatenschutzes der Betroffenen – gefordert und gefördert werden.

4. Betroffenenrechte

4.1. Mehr Transparenz in der Datenverarbeitung

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Doch nur wenn sie oder er ihre/seine Rechte einfach und effektiv geltend machen kann, wird sie/er diese auch nutzen. Das derzeitige Recht kennt zwar bereits eine Reihe von Rechten auf Auskunft, Berichtigung und Löschung. Es kommt aber darauf an, dass die Betroffenen diese Rechte unkompliziert geltend machen können. Hierzu kann auch eine regelmäßige Benachrichtigung über die gespeicherten personenbezogenen Daten (Datenbrief) einen Beitrag leisten.

Die Konferenz der Datenschutzbeauftragten fordert, das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Erweiterung der Informationspflichten (etwa nach § 4 BDSG):
    - Die Verantwortlichkeit für die Datenverarbeitung muss gegenüber den Betroffenen klar und eindeutig offengelegt werden.
    - Die Kerninformationen müssen an prominenter Stelle platziert werden, statt mehrseitige, kleingedruckte Einwilligungserklärungen zum Datenschutz zu verwenden.
- Umgekehrt bedeutet dies als Pflicht für die verantwortliche Stelle: Dokumentation der Herkunft und der Empfänger von Daten sowie Protokollierung von Datenbankzugriffen.
- Vereinfachte Auskunftsrechte der Betroffenen:
    - Leichter Zugang zu Informationen über gespeicherte personenbezogene Daten („Mein XYZ“); Bereitstellung technischer Mittel zur Erleichterung der Wahrnehmung von (Datenschutz-)Rechten.
    - Generelle Einführung eines Rechts auf elektronische Auskunftserteilung/Einsichtnahme für die Betroffenen.
    - Auskunftsrecht der Betroffenen auch hinsichtlich der Zusammenführung ihrer Daten mit anderen Daten.
    - Erstreckung des Auskunftsrechts auf die Nutzung, soweit sie vom Zweck der Datenerhebung abweicht.
- Aufklärung über Risiken und Information über Datenpannen auch im öffentlichen Bereich.

- Auskunfteien und Detekteien sollten die Auskunft nicht mehr unter Berufung auf überwiegende Geschäftsgeheimnisse verweigern dürfen.

4.2. Echte Einwilligung statt faktischem Zwang

Die allgegenwärtige Datenverarbeitung ist aus der Informationsgesellschaft nicht mehr wegzudenken. Die Einwilligung der Betroffenen ist im Allgemeinen in der Privatwirtschaft eine wichtige Ermächtigungsgrundlage für eine Datenverarbeitung. Um wirksam zu sein, muss sie insbesondere freiwillig und informiert erteilt werden. Angesichts der immer komplexer werdenden Welt der allgegenwärtigen Datenverarbeitung ist dies fast schon Illusion. Es kommt darauf an, den Betroffenen die immer umfassenderen Datenverarbeitungen nicht zu verheimlichen, sondern einfach und verständlich die wichtigsten Konsequenzen zu erläutern, damit die Betroffenen sich bei Interesse vertiefter informieren können, im Übrigen aber ein Verständnis für die Welt der Informationsgesellschaft entwickeln und sich selbstbestimmt darin entfalten können.

Die Konferenz der Datenschutzbeauftragten fordert, das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Die Einwilligung muss durch aktives Tun (ankreuzen, Haken setzen etc.) erteilt werden, eine formularmäßige Einwilligung, etwa durch Unterschrift unter allgemeine Geschäftsbedingungen oder umfangreiche Datenschutzerklärungen, genügt nicht.
- Die Geltungsdauer einer Einwilligung wird zeitlich begrenzt, da Betroffene nach einer gewissen Zeit die Konsequenzen nicht mehr einschätzen können oder im Bereich der Werbung die Daten häufig „wandern“ und die Betroffenen unter Umständen Mühe haben, eine einmal erteilte Einwilligung gegenüber allen „Nutznießern“ zu widerrufen.
- Anspruch auf Nachweis der Einwilligung, um den Betroffenen eine wirksame Durchsetzung ihrer Ansprüche zu ermöglichen.
- Der Widerruf sollte nur bei der Stelle eingelegt werden müssen, die die Daten erstmalig weitergegeben hat. Diese hat den Widerspruch dann an die Empfänger der Daten weiterzugeben.
- Das Koppelungsverbot im Bereich der Werbung sollte strenger formuliert werden. Der Abschluss eines Vertrages darf bereits heute nicht davon abhängig gemacht werden, dass die oder der Betroffene in die Weitergabe ihrer oder seiner persönlichen Daten an Dritte zu Werbezwecken einwilligt, es sei denn, die Datenweitergabe ist gerade Gegenstand des Vertrages. Dieses Verbot sollte ausgeweitet und nicht auf

marktbeherrschende Unternehmen beschränkt werden. Soweit das Koppelungsverbot von dem Merkmal der „Marktbeherrschung“ abhängig ist, besteht die Gefahr, dass nicht marktbeherrschende Unternehmen dies als Ermutigung zur Koppelung verstehen. Darüber hinaus sollte das Koppelungsverbot über den Bereich der Werbung hinaus ausgedehnt werden.

- Der Widerruf der Einwilligung darf nicht durch einen Medienbruch erschwert werden („Wieso darf zwar die Einwilligung elektronisch erklärt werden, nicht aber der Widerspruch zur Werbenutzung?“).

Eine derart reformierte Einwilligungserklärung versetzt die Betroffenen wieder in die Lage, ihre Daten selbst zu kontrollieren und sich verständig in der Informationsgesellschaft zu bewegen.

5. Datenschutz im Internetzeitalter

Das Internet ist weder rechtsfreier Raum noch harmlose Spielwiese. Es gehört zur Lebenswirklichkeit in der Informationsgesellschaft. Immer stärker wird der Druck, Teil des globalen Netzes zu sein – ob nun freiwillig in sozialen Netzwerken oder unfreiwillig als Objekt der Bewertung, Kritik, aber auch Verleumdung. Die Konferenz der Datenschutzbeauftragten fordert daher, die Stärkung des Datenschutzes im Internet als gesellschaftliche Aufgabe zu verstehen, die von allen relevanten gesellschaftlichen und staatlichen Akteurinnen und Akteuren getragen werden muss.

Ein modernes Datenschutzrecht muss internetfähig sein. Die globale Struktur des Internets und neue Dienste, wie z.B. Street View und Soziale Netzwerke, setzen nationalen Regelungsansätzen und -strategien jedoch enge Grenzen. Die Globalisierung ist allerdings keine Entschuldigung für nationale Passivität. Es ist daher ein mehrdimensionaler Ansatz zur Stärkung des Datenschutzes zu verfolgen: Nationale Regelungen sollten möglichst durch internationale Vereinbarungen flankiert werden, so dass ein weitgehend deckungsgleiches inhaltliches Grundniveau des Internet-Datenschutzes entsteht, dem sich Anbieter von Diensten nicht ohne weiteres durch Flucht in das Ausland entziehen können. Gleichzeitig müssen vollzugsfähige Strukturen geschaffen werden, die es ermöglichen, dass gemeinsam anerkannte Standards auch international durchgesetzt werden können.

Bei der Fortentwicklung des Internetrechts ist ein rechtlicher Rahmen zu schaffen, der die grundsätzlich unbeobachtete Kommunikation und Nutzung des Internets gewährleistet. Zudem hält die Konferenz die Entwicklung von besonderen Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz für erforderlich. Angesichts der weltweiten Vernetzung und dauerhaften Verfügbarkeit von Inhalten im Netz besteht im Internet eine besondere Gefährdungslage, der nur durch internetspezifische Instrumente begegnet werden kann. Im Einzelnen schlägt die Konferenz vor allem vor, das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Einführung eines Mediennutzungsgeheimnisses, das die grundsätzlich unbeobachtete Inanspruchnahme elektronischer Dienste garantiert.
- Stärkung der Möglichkeit zur anonymen und pseudonymen Nutzung und Bezahlung von Online-Angeboten.
- Verbesserte Informationspflichten für Anbieter:
    - Wichtigste Datenschutzinformation an prominenter Stelle des Webauftritts: Ort der Datenspeicherung, zuständige Datenschutzbehörde

    - Verpflichtung, die Nutzerinnen und Nutzer über alle Änderungen der Datenschutz- und Geschäftsbedingungen vorab in Kenntnis zu setzen und diese zu dokumentieren.

- „privacy first“ oder „privacy by default“, d.h. Grundeinstellung von Internetdiensten müssen ein Optimum an Datenschutz bieten, Abweichungen hiervon sind von den Nutzenden im Sinne einer Opt-In-Lösung selbstverantwortlich zu wählen.
- Verpflichtung der Anbieter, den Betroffenen neben der Möglichkeit zur elektronischen Erteilung der Einwilligung auch einen elektronischen Zugriff auf ihre Daten und die elektronische Ausübung von Widerspruchs-, Berichtigungs- und Kündigungsrechten ohne diskriminierenden Medienbruch zu ermöglichen.
- sichere und datenschutzfreundliche Authentifizierung von Nutzerinnen und Nutzern, soweit dies zur elektronischen Ausübung ihrer Rechte erforderlich ist.
- erleichterte Durchsetzung von Nutzerrechten, etwa durch nutzerfreundliche Festlegung des anwendbaren Rechts und des Gerichtsstandes entsprechend dem im Verbraucherschutzrecht maßgeblichen Internationalen Privatrecht (Rom I- und II-Verordnungen; Urteil des Bundesgerichtshofs v. 2.3.2010 – VI ZR 23/09 – Klage gegen eine Internetveröffentlichung der New York Times).
- besondere Regelungen zum Datenschutz bei Diensten, die sich an minderjährige Nutzerinnen und Nutzer richten.

Zusätzliche Anforderungen an die Zulässigkeit von Internetveröffentlichungen (im Unterschied zur herkömmlichen Veröffentlichung), nämlich

- Verpflichtung der Anbieter, Nutzerinnen und Nutzer auf mit der Veröffentlichung personenbezogener Daten verbundene Risiken hinzuweisen.
- Veröffentlichung personenbezogener Daten im Internet durch öffentliche Stellen grundsätzlich nur, soweit die entsprechende Rechtsgrundlage diese Veröffentlichungsform ausdrücklich mit einbezieht.
- Aufnahme von „Verfallsdaten“ für personenbezogene Daten bei deren Veröffentlichung im Internet, zumindest wenn Betroffene eigene Daten ins Netz stellen und ein solches Verfallsdatum setzen wollen.
- gesetzliche Verpflichtung der Anbieter von Suchmaschinen, von Website-Anbietern verhängte „Indexierungsverbote“ und Verfallsdaten zu beachten.
- Pflicht zur Verwendung verfügbarer technischer Schutzmechanismen zur Gewährleistung der Datensicherheit, insbesondere zum Schutz vor dem unbefugten massenhaften Herunterladen von personenbezogenen Daten.

Die Bundesregierung wird darüber hinaus aufgefordert,

- im Rahmen internationaler Vereinbarungen die Anforderungen des Datenschutzes zur Geltung zu bringen.
- sich auf internationaler Ebene dafür einzusetzen, dass es zu verbindlichen Absprachen im Rahmen der Vereinten Nationen für ein möglichst hohes Datenschutzniveau und dessen Durchsetzung im Internet kommt.
- die internationalen Standardisierungsvorhaben damit zu verknüpfen.
- verstärkt Forschungsmittel zur Verbesserung des Datenschutzes in globalen Netzen vorzusehen, insbesondere zur Unterstützung und Stärkung der Rechte Einzelner im Cyberspace, z.B. zur Umsetzung von Verfallsdaten und zur Entwicklung eines „digitalen Radiergummis“ für Betroffene.

Auch im Internet muss die/der Einzelne ihr/sein Recht auf informationelle Selbstbestimmung durchsetzen können.

6. Eigenkontrolle der verantwortlichen Stellen

Das gegenwärtige Datenschutzrecht ist vielfach noch geprägt durch Verbotsnormen, die selten zu Kontrollen führen und deren Sanktionen bei festgestellten Verstößen nicht ausreichen. Aufgrund sehr geringer Kontrolldichte führt dies zu erheblichen Vollzugsdefiziten. Ein modernes Datenschutzrecht muss deswegen die Elemente der Eigenkontrolle stärken. Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden, etwa als Vorteil im Wettbewerb, und nicht nur als von außen aufgezwungene Beschränkung. Daneben müssen interne Mechanismen bei den verantwortlichen Stellen entwickelt und gestärkt werden, die die Einhaltung des Datenschutzes sicherstellen, ohne dass es einer ständigen Kontrolle von außen bedarf.

Die Konferenz der Datenschutzbeauftragten fordert das bestehende Datenschutzrecht um folgende Punkte zu ergänzen:

- Ausführungsgesetz zum Datenschutzaudit:

  Die Einführung eines freiwilligen bundesweiten Datenschutzaudits für Verfahren und Produkte der elektronischen Datenverarbeitung, mit dem die Einhaltung aller relevanten Datenschutzvorschriften bestätigt und darüber hinaus besonders datenschutzfreundliches Verhalten ausgezeichnet werden, wäre ein wirksames Mittel, Datenschutz zum Wettbewerbsvorteil zu machen.

- Aufstellung verbindlicher Datenschutzkonzepte:

  Eine Verpflichtung der verantwortlichen Stellen, für ihre Verarbeitung personenbezogener Daten ein Datenschutzkonzept zu entwickeln und der Aufsichtsbehörde auf Verlangen vorzulegen, würde diese zwingen, sich mit der Thematik umfassend für ihren jeweiligen Betrieb auseinanderzusetzen, Schwachstellen aufzudecken und entsprechende Vorkehrungen zu treffen. Hierzu sollte auch die bereits bestehende Verpflichtung zur Vorabkontrolle ausgebaut werden, insbesondere sollte festgeschrieben werden, dass die Durchführung der Vorabkontrolle schriftlich zu dokumentieren ist.

- Stärkung der behördlichen/betrieblichen Datenschutzbeauftragten:

  Die behördlichen und betrieblichen Datenschutzbeauftragten sind ein wichtiges Element der Eigenkontrolle, soweit sie ihre Aufgaben unabhängig, kompetent und mit ausreichenden Möglichkeiten wahrnehmen können. Deswegen sind Regelungen erforderlich, die zumindest

  - sie in ausreichendem Umfang von anderen Aufgaben freistellen,
  - ihre interne Beteiligung bei allen datenschutzrelevanten Vorgängen zwingend vorsehen,

- sie als Ansprechpartnerinnen und -partner für Datenschutz nach innen und außen bekannt machen,
- die Unabhängigkeit und Qualität externer Datenschutzbeauftragter etwa durch Festlegung von Mindestanforderungen bei der Beauftragung stärken und
- eine Berichtspflicht einführen.

Mit diesen Maßnahmen kann die Verwirklichung des Datenschutzes in den verantwortlichen Stellen selbst verbessert und die externe Kontrolle entlastet werden. Das Audit würde den Datenschutz zum Wettbewerbsfaktor machen und auf diesem Wege stärken.

7. Datenschutzaufsicht

Den Datenschutzaufsichtsbehörden kommt für die Verwirklichung eines effizienten Datenschutzes eine herausragende Rolle zu, da sie nicht nur die Einhaltung der datenschutzrechtlichen Bestimmungen kontrollieren, sondern die verantwortlichen Stellen im Vorfeld auch beraten und die Parlamente und die Öffentlichkeit über datenschutzrechtliche Probleme und Lösungswege informieren. Die Stärkung der Aufsichtsbehörden ist deswegen zugleich auch eine Verbesserung des Datenschutzes. Es gibt neben der vielfach unzureichenden personellen Ausstattung aber weitere Punkte, die eine wirkungsvolle Datenschutzaufsicht beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten folgende gesetzgeberische Maßnahmen für erforderlich:

- Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.

- Das mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.08.2009 (BGBl. I S. 2814) eingeführte Anordnungsrecht in § 38 Abs. 5 BDSG ist zwar ein erster Schritt. Dieses muss jedoch effektiver ausgestaltet und den üblichen Grundsätzen des Verwaltungsvollzugs angepasst werden.

- Mitwirkungspflicht der kontrollierten Stelle gegenüber Kontrollen der Aufsichtsbehörde:

  § 38 Abs. 4 BDSG sieht bislang nur das Recht der Aufsichtsbehörde vor, die zu kontrollierende Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Ohne aktive Mitwirkung der zu kontrollierenden Stelle, wie sie etwa § 24 Abs. 4 BDSG für die Tätigkeit des Bundesbeauftragten vorsieht oder § 5 des Gesetzes zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung, gehen solche Kontrollen aber oft ins Leere, wenn z. B. vor Ort niemand da ist, der Fragen beantwortet, die Datenverarbeitungssysteme und -verfahren erläutert oder die technischen Voraussetzungen für wirksame Prüfungen schafft.

- Ausweitung der Informationspflicht bei Datenpannen auf öffentliche Stellen.

- Anordnungsbefugnisse auch für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit:

  Durch die jüngsten Gesetzesänderungen haben zwar die in § 38 BDSG erwähnten Aufsichtsbehörden ein Anordnungsrecht bei Datenschutzverstößen erhalten, es fehlt

aber eine vergleichbare Regelung für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in den Bereichen, in denen er nicht-öffentliche Stellen nach dem Telekommunikationsgesetz und dem Postgesetz kontrolliert.

- Ausdehnung der Zeugnisverweigerungsrechte und Beschlagnahmeschutzvorschriften auf Informationen und Unterlagen, die die Aufsichtsbehörden bei Berufsgeheimnisträgerinnen und -trägern erlangt haben:

  Die gesetzlich vorgesehene Datenschutzkontrolle von Berufsgeheimnisträgerinnen und -trägern durch die staatlichen Aufsichtsbehörden wird von diesen teilweise mit der Begründung verweigert, dort erlangte Kenntnisse und Unterlagen unterlägen bei den Aufsichtsbehörden nicht in gleicher Weise dem strafverfahrensrechtlichen Zeugnisverweigerungsrecht und Beschlagnahmeschutz wie bei den Berufsgeheimnisträgerinnen und -trägern selbst. Deswegen sei eine solche Kontrolle nicht zulässig. Aus diesem Grunde bedarf es entsprechender Vorschriften im Strafgesetzbuch und im Datenschutzrecht, wie sie für externe betriebliche Datenschutzbeauftragte schon geschaffen wurden.

- Strafantragsbefugnis für die Datenschutzaufsichtsbehörden in § 205 StGB:

  Nicht selten erhalten die Aufsichtsbehörden Kenntnis von Datenschutzverstößen, die zugleich eine Strafbarkeit nach den §§ 201 - 204 StGB begründen können. In der Praxis scheitert die Strafverfolgung aber zum Teil daran, dass der nach § 205 StGB erforderliche Strafantrag nicht gestellt wird. Deswegen sollte auch den Aufsichtsbehörden diese Möglichkeit eingeräumt werden, wie in § 44 BDSG für den nicht-öffentlichen Bereich bereits geschehen.

Durch diese Maßnahmen würden die Möglichkeiten der Aufsichtsbehörden deutlich gestärkt, ihre Kontrollaufgaben wirksam wahrzunehmen.

8. Sanktionen

Die erheblichen Vollzugsdefizite im Datenschutz sind unter anderem auch darauf zurückzuführen, dass Verstöße gegen datenschutzrechtliche Bestimmungen vielfach folgenlos bleiben. Gründe hierfür sind zum einen nicht ausreichende Sanktionsmöglichkeiten und zum anderen praktische Probleme bei der Verhängung von Bußgeldern oder der Strafverfolgung. So sind z. B. immer noch wichtige Datenschutzvorschriften nicht bußgeldbewehrt, Haftungsansprüche werden nur selten geltend gemacht, weil die Anspruchsteller nicht nur den Datenschutzverstoß nachweisen müssen, sondern auch ein Verschulden der verantwortlichen Stelle und eine konkrete Schadenshöhe. Außerdem fallen aufgrund fehlender Zuständigkeitsregelungen oft Datenschutzaufsicht und zuständige Bußgeldbehörde auseinander. Deswegen sind inhaltliche und verfahrensrechtliche Änderungen erforderlich, damit Daten verarbeitende Stellen aufgrund erhöhten Risikos von sich aus intensiver auf die Einhaltung der geltenden Datenschutzvorschriften achten.

Um die Sanktionsmöglichkeiten und ihren Vollzug effizienter zu gestalten, hält die Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende Maßnahmen für erforderlich:

- Einführung einer Gefährdungshaftung auch für nicht-öffentliche Stellen:
  - Nach § 8 Abs. 1 BDSG besteht eine verschuldensunabhängige Haftung für Datenschutzverstöße nur bei öffentlichen Stellen. Da die Gefährdung des Grundrechts auf informationelle Selbstbestimmung aber bei nicht-öffentlichen Stellen in mindestens gleicher Weise besteht, sollte auch für diesen Bereich eine vergleichbare Gefährdungshaftung eingeführt werden. Die Geltendmachung von Schadensersatzansprüchen scheitert vielfach daran, dass die Betroffenen zwar einen Datenschutzverstoß nachweisen können, aber kein Verschulden.
  - Konkretisieren sich in der elektronischen Datenverarbeitung immanente Risiken, kann dies nicht zu Lasten der Betroffenen gehen.
- Einführung eines pauschalierten Schadensersatzes für Datenschutzverstöße:

  Nach geltendem Recht kann nach einem Datenschutzverstoß nur dann Schadensersatz verlangt werden, wenn der/dem Betroffenen ein konkret bezifferbarer Schaden entstanden ist, den sie/er nachweisen muss. Immaterielle Schäden können nach § 8 Abs. 2 BDSG nur bei schweren Verletzungen des Persönlichkeitsrechts und nur gegenüber öffentlichen Stellen geltend gemacht werden. Allerdings ist dies im Einzelfall u. U. auch nach den allgemeinen Haftungsregelungen des Bürgerlichen Gesetzbuchs möglich. Ein pauschalierter Anspruch (unbeschadet weiterer Ansprüche bei nachweisbar höheren Schäden) würde dieses Problem lösen und zugleich die An-

strengungen der verantwortlichen Stellen erhöhen, von sich aus Verletzungen des Datenschutzes zu verhindern.

- Anspruch der Betroffenen gegen die verantwortliche Stelle, auf die Beseitigung von durch unrichtige oder unrechtmäßige Datenübermittlung entstandene negative Folgen hinzuwirken:

  Werden unrechtmäßige oder unrichtige Daten an Dritte übermittelt, kann das für die Betroffenen fatale Folgen haben. Falsche Angaben einer Kreditauskunftei (etwa aufgrund einer Verwechslung oder eines unrichtigen Datenbestandes) können dazu führen, dass den Betroffenen Kredit-, Handyverträge oder Konten gekündigt werden. Weisen diese den Irrtum nach, berichtigt die Kreditauskunftei zwar ihren Datenbestand, mit den eingetretenen Folgen bleiben die Betroffenen aber allein und müssen selbst versuchen, die Kündigungen rückgängig zu machen oder andere Folgen zu beseitigen. Die vorgeschlagene Maßnahme würde hier die Verursacherinnen und Verursacher in die Pflicht nehmen. Eine solche Regelung würde darüber hinaus das Eigeninteresse von Auskunfteien steigern, die Richtigkeit ihres Datenbestandes zu überprüfen und Irrtümer zu vermeiden.

- Erweiterung der Bußgeldtatbestände, insbesondere für
  - unbefugtes Nutzen von Daten,
  - unzulässige Beobachtung, Registrierung und Zweckänderung durch automatisierte Verfahren (z.B. Videoüberwachung),
  - das Unterlassen von technisch-organisatorischen Maßnahmen:

    Noch immer gibt es eine Reihe von wichtigen Datenschutzbestimmungen, deren Nichtbeachtung nicht mit einem Bußgeld geahndet werden kann. Hierzu gehören insbesondere das unbefugte Nutzen von Daten und die Gefährdung elektronischer Datenverarbeitungssysteme durch Unterlassen der erforderlichen Schutzmaßnahmen, die etwa in § 9 BDSG und der Anlage dazu vorgesehen sind. Diese Lücken sind im Interesse eines effizienten Datenschutzes zu schließen.

- Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten konzentrieren:

  Die Datenschutzgesetze enthalten zwar eine Vielzahl von Bußgeldtatbeständen, vielfach aber keine eigenständige Zuständigkeitsregelung für deren Verfolgung, sodass insoweit die allgemeinen Regelungen des Ordnungswidrigkeitenrechts gelten. Deswegen sind häufig weder die Datenschutzaufsichtsbehörde, die den Datenschutzverstoß festgestellt hat, noch eine andere zentrale, landes- oder bundesweit agierende Stelle zuständig, sondern die jeweils fachlich zuständige oberste Landes- bzw. Bundesbehörde, die aber wegen der geringen Fallzahlen häufig ihre Zuständigkeit für die Ahndung von Datenschutzverstößen gar nicht kennt, keine Erfahrung im Datenschutz

hat und keine Übung in der Durchführung von Ordnungswidrigkeitenverfahren. Deswegen kommt es in vielen Fällen zu keiner Verfolgung von datenschutzrechtlichen Ordnungswidrigkeiten, obwohl die Voraussetzungen dafür vorliegen.

- Verfolgung von datenschutzrechtlichen Straftaten auch von Amts wegen, wenn ein besonderes öffentliches Interesse gegeben ist:

  Nach geltendem Recht setzt die Verfolgung von Straftaten im Datenschutzrecht einen Antrag voraus, den nur die oder der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit oder die Datenschutzaufsichtsbehörde stellen können. Es häufen sich die Fälle, in denen Strafverfolgungsbehörden, die von sich aus auf entsprechende Straftaten gestoßen sind, eine/einen Antragsberechtigte/Antragsberechtigten suchen müssen, um die Vergehen verfolgen zu können. Deswegen sollte in den Fällen, in denen ein besonderes öffentliches Interesse an einer Strafverfolgung gegeben ist, eine Verfolgung auch von Amts wegen möglich sein.

Durch die aufgeführten Maßnahmen könnte das datenschutzrechtliche Sanktionssystem sehr viel wirkungsvoller auf Datenschutzverstöße reagieren. Damit ließen sich die Vollzugsdefizite verringern, weil die betroffenen Stellen größere Anstrengungen zeigen würden, Datenschutzverstöße gar nicht erst entstehen zu lassen.

9. Vereinfachung und bessere Lesbarkeit des Gesetzes

Das BDSG ist in Aufbau, Wortlaut und Regelungstechnik kaum noch verständlich und nachvollziehbar. Selbst für Fachleute ist es inzwischen schwierig, für konkrete Sachverhalte das Recht korrekt anzuwenden. Normale Anwender, die nicht über eigene Rechtsabteilungen oder spezialisierte Fachanwälte verfügen, sind hier vielfach überfordert.

Auch für die Bürgerinnen und Bürger, die sich selbst anhand des Gesetzes über ihre Rechte und die Möglichkeiten, diese durchzusetzen, informieren wollen, werden fast unüberwindbare Verständnishürden aufgebaut. Die Vollzugsdefizite im Datenschutz gehen zu einem Teil auf die Unverständlichkeit der Regelungen zurück. Deswegen muss das BDSG einfacher und verständlicher gestaltet werden. Hierzu können auch Änderungen bei den Definitionen gehören, die zusätzliche Spezialvorschriften entbehrlich machen.

Neben bereits aufgeführten Maßnahmen, wie z. B. einer möglichst weitreichenden Vereinheitlichung der Vorschriften für den öffentlichen und den nicht-öffentlichen Bereich, hält die Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende Punkte für erforderlich:

- Neue Definition des Begriffs „Verarbeiten“, die sowohl das Erheben wie das Nutzen von personenbezogenen Daten umschließt:

  Die derzeitige Begrifflichkeit des BDSG umfasst gesondert das „Erheben“ (§ 3 Abs. 3), das „Verarbeiten“ (§ 3 Abs. 4) und das „Nutzen“ (§ 3 Abs. 5) von personenbezogenen Daten. Aufgrund dieser unterschiedlichen Terminologie werden in zahlreichen Bestimmungen des BDSG immer alle drei Begriffe hintereinander aufgezählt, was Lesbarkeit und Verständnis beeinträchtigt. Die Europäische Datenschutzrichtlinie definiert „Verarbeiten“ hingegen so (Art. 2b), dass „Erheben“ und „Benutzen“ mit umfasst werden.

- Einheitliche Anwendung des Datenschutzrechts für alle Formen der Verarbeitung personenbezogener Daten:

  Im Gegensatz zum öffentlichen Bereich gilt das BDSG im nicht-öffentlichen Bereich nur für den Einsatz von Datenverarbeitungsanlagen und nicht automatisierte Dateien, nicht aber für personenbezogene Daten in normalen Papierakten. Diese Unterscheidung ist im Blick auf die Schutzziele nicht sinnvoll und verliert aufgrund des technologischen Fortschritts zunehmend an Bedeutung. Sie sollte aufgegeben werden, was das Gesetz auch vereinfachen würde.

- Aufnahme von „genombezogenen Daten“ in die Definition der besonderen Arten personenbezogener Daten:

Personenbezogene Daten, die sich aus genetischen Untersuchungen und Analysen ergeben, sind besonders sensibel, aber durch die Definition der besonderen Arten personenbezogener Daten nur so weit erfasst, wie es sich dabei um Gesundheitsdaten handelt. Der besondere Schutz für diese Datenkategorie sollte auf alle genombezogenen Daten erweitert werden, zumindest soweit sie nicht offensichtlich sind, wie etwa das Geschlecht.

- Definition der „öffentlich zugänglichen Daten“ und spezielle Regelungen für den Umgang damit:

  Die Datenschutzgesetze des Bundes und der Länder sehen vielfach vor, dass für den Umgang mit personenbezogenen Daten, die öffentlich zugänglich sind oder aus öffentlich zugänglichen Quellen stammen, geringere Anforderungen gelten oder die Schutzvorschriften gar nicht zur Anwendung kommen. Dies muss mit Blick auf das Internet überdacht werden. Zum einen ist der Begriff „öffentlich zugänglich“ einschränkend zu definieren, etwa indem eine entsprechende Zweckbestimmung durch den Betroffenen selbst oder aufgrund gesetzlicher Regelung (öffentliche Register) erforderlich ist, zum anderen bedarf es spezieller Regelungen zur Interessensabwägung und zur Zweckbindung.

Die vorgeschlagenen Maßnahmen würden das Datenschutzrecht lesbarer und verständlicher machen und zur Vereinfachung beitragen.