

## **Praxisfälle und Erfahrungen zum deutschen Datenschutzrecht**

### **Beitrag zum Südkoreanisch- Deutschen Datenschutzworkshop am 1. November 2004 in Seoul, Korea**

RA Jan Möller,  
Mitarbeiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

#### **I. Einleitung**

Der Datenschutz hat das Ziel, das Recht auf informationelle Selbstbestimmung und damit den Schutz des Persönlichkeitsrechts des Einzelnen in von rasanten Entwicklungen geprägten Lebensbereichen wie beispielsweise der Informations- und Kommunikationstechnik zu gewährleisten. In der Realität sind dabei verschiedene Tendenzen zu beobachten, die es bei der (rechtlichen und technischen) Umsetzung dieses Ziels zu berücksichtigen gilt:

1. Öffentliche Stellen zeigen ein steigendes Interesse an der Überwachung der Bürger und Besucher ihres Landes zu Sicherheitszwecken.
2. Die Wirtschaft ist an genauen Profilen ihrer Kunden und Arbeitnehmer interessiert, um z.B. zielgerichtetes Marketing zu betreiben, präzisere Risikoabschätzungen bei Vertragsabschlüssen vornehmen zu können oder den Workflow des Unternehmens zu optimieren.
3. Öffentliche wie private Stellen bemühen sich, immer mehr Dienste möglichst komfortabel für den Kunden und kostengünstig für die Organisation in den automatisierten Workflow einzubinden.

Zu den vorgenannten Zwecken werden komplexe technische Systeme eingesetzt, die das informationelle Selbstbestimmungsrecht des Einzelnen berühren, die von ihm aber nur schwer zu durchschauen sind (Transparenzdefizit).

Gleichzeitig werden die notwendigen technischen Voraussetzungen (PC, Breitbandanschluss, etc.) für die Nutzung solcher Dienste in immer kostengünstigeren Varianten angeboten und diese Produkte auf Nutzer mit minimalen Vorkenntnissen eingestellt. Diese Voreinstellungen orientieren sich an reibungsloser Funktion der Produkte für bestimmte Aufgaben und in der Regel nicht an der Sicherheit der Nutzerdaten. Dies führt zu vielen unsicheren Systemen mit unzureichend geschulten Nutzern (Wissensdefizit). Die genannten Wissens- und Transparenzdefizite führen dazu, dass viele Bürger nur eingeschränkt in der Lage sind, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

Dieser Beitrag stellt exemplarische Praxisfälle (II.) für die oben genannten Tendenzen vor. In der Folge werden einige Beispiele eines technisch (III.) und am Wettbewerb (IV.) orientierten Datenschutzes umrissen, die den Bürger dazu befähigen sollen, sein Recht auf informationelle Selbstbestimmung auch in einer technisierten Umwelt ausüben zu können. Abschließend wird ein Überblick gegeben, wie in Deutschland verschiedene Datenschutzkontrollinstanzen (V.) zur Umsetzung von datenschutzrechtlichen Vorschriften und von technisch-organisatorischen Maßnahmen beitragen.

#### **II. Praxisfälle**

##### *1. Überwachung und Vorratsdatenspeicherung bei der Erbringung von Telekommunikationsdienstleistungen und Telediensten*

Die nachfolgende Darstellung ist eine Zusammenfassung der Web-Veröffentlichungen des Unabhängigen Landeszentrums für Datenschutz unter <http://www.datenschutzzentrum.de/material/themen/rotekarte/index.htm>. Für detailliertere Informationen wird auf diese Quelle verwiesen.

Seit dem Jahr 1996 werden von Seiten der Sicherheitsbehörden immer wieder Vorstöße unternommen, eine gesetzliche Pflicht zur Vorratsdatenspeicherung sowohl im Bereich der klassischen Telekommunikation (Festnetz, Handy, SMS, Fax usw.) als auch für alle im Internet verfügbaren Daten zu begründen. Zweck sollte es sein, dafür zu sorgen, dass die Geheimdienste und Strafverfolgungsbehörden im Bedarfsfall Daten vorfinden, auf die sie zugreifen können. Einzelheiten sollten nicht auf gesetzlicher Ebene festgeschrieben, sondern von der Bundesregierung durch Rechtsverordnung festgelegt werden.

Für Daten aus dem Bereich der Teledienste gilt zur Zeit genau die gegenteilige Regelung: Grundsätzlich sind alle Daten, die nicht zur Abrechnung gebraucht werden, zu löschen. Insbesondere im Internet sind nach wie vor die meisten Angebote kostenlos, auch bei Bezahldiensten werden zur Abrechnung nur wenige Daten benötigt. Daher müssen die allermeisten Daten gelöscht werden.

Bei einer Speicherpflicht drohen im Gegensatz dazu nahezu unbeschränkte Zwangsspeicherungen durch alle beteiligten Akteure. So hätte ein Webhosting-Provider zu speichern, wer seine Seiten besucht. Access-Provider müssten speichern, wann der Nutzer welche Inhalte abrufen. Damit entstünde ein komplettes Verzeichnis all dessen, wofür sich die Bürger im Netz interessieren, was sie online einkaufen, mit wem sie was chatten oder welche Informationsmedien sie bevorzugen.

Derartige gesetzliche Regelungen widersprechen dem vom Bundesverfassungsgericht aufgestellten Grundsatz, dass es keine Vorratsspeicherung zu unbestimmten Zwecken geben darf. Mit einer derartigen Vorratsdatenspeicherung entstünde ein Überwachungspotenzial, das in der realen Welt derzeit kaum ein Gegenstück findet.

Verschiedene Interessenverbände der IT-Wirtschaft lehnen die Einführung einer Speicherpflicht ab, weil diese den IT-Unternehmen beträchtliche Kosten auferlegen würde, die an die Kunden weitergegeben werden müssten und sich damit negativ auf die Wettbewerbsfähigkeit der Unternehmen auswirken würde.

Der vorerst letzte Vorstoß zur Einführung der Vorratsdatenspeicherung auf nationaler Ebene im Rahmen der Änderung des Telekommunikationsgesetzes endete im Mai 2004 mit einem Kompromiss im Vermittlungsausschuss von Bundestag und Bundesrat, der eine umfassende Vorratsdatenspeicherung nicht vorsieht. Derzeit bemühen sich verschiedene Mitgliedsstaaten um die Einführung einer Pflicht zur Vorratsdatenspeicherung auf EU-Ebene. Aktuelle Äußerungen aus dem Bundesrat deuten darauf hin, dass Deutschland diesen Vorschlag nicht unterstützen wird.

## *2. Biometrie in Ausweisdokumenten*

Die nachfolgende Darstellung zur derzeitigen Rechtslage bezüglich der Biometrie in Ausweisdokumenten ist eine Zusammenfassung der Web-Veröffentlichung des Unabhängigen Landeszentrums für Datenschutz abrufbar unter [http://www.datenschutzzentrum.de/material/themen/divers/biometrie\\_ausweis.htm](http://www.datenschutzzentrum.de/material/themen/divers/biometrie_ausweis.htm). Für detailliertere Informationen wird auf diese Quelle verwiesen.

Die Einführung von Ausweispapieren mit biometrischen Merkmalen ist derzeit ein international wie national diskutiertes Thema. Ausländische Staaten (z.B. die USA) fordern für die Einreise das Zurverfügungstellen von biometrischen Daten, z.B. über Reisedokumente. Private Unternehmen (z.B. Betreiber von Flughäfen und Fluglinien) wollen einen Zugriff auf biometrische Ausweisdaten erhalten. Sicherheitsbehörden fordern den Zugriff auf die biometrischen Ausweisdaten z.B. für Strafverfolgungszwecke.

Das deutsche Terrorismusbekämpfungsgesetz vom 09.01.2002 benennt - das Ziel, die Inhaber von staatlichen Ausweisdokumenten mit Hilfe von biometrischen Verfahren eindeutig automatisiert zu identifizieren. Über die computergestützte Identifizierung von Personen mit Hilfe ihrer Ausweisdokumente soll u.a. verhindert werden, dass Personen sich mit gefälschten Papieren bzw. einer anderen Identität ausweisen. Zu diesem Zweck sollen zusätzlich zu Angaben über Körpergröße und Augenfarbe sowie zu Lichtbild und Unterschrift weitere biometrische Merkmale elektronisch gespeichert werden, die im Kontrollfall durch automatisierten Vergleich mit denen des Ausweisnutzenden verifiziert werden sollen.

Das Ausweisdokument darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Inhabers enthalten. Lichtbild, Unterschrift und die weiteren biometrischen Merkmale dürfen ebenso wie die sonstigen alphanumerischen Identifizierungsdaten in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. Bei den alphanumerischen Identifizierungsdaten handelt es sich um eine Seriennummer, Namen, Geburtsangaben, Geschlecht, Größe, Augenfarbe, Wohnort (bzw. Anschrift) und Staatsangehörigkeit.

Wichtig für die Frage der elektronischen Ausgestaltung ist, dass das Dokument eine Zone für das automatische Lesen enthält, die lediglich folgende Daten enthalten darf: Art des Dokuments, Namen, Seriennummer, Staatsangehörigkeit, Geschlecht, Geburtstag, Gültigkeitsdauer und Prüzziffern. Ausdrücklich nicht mit aufgeführt sind die in diesem Zusammenhang mit geregelten biometrischen Merkmale. Daraus kann nur geschlossen werden, dass der Gesetzgeber ausschließen wollte, dass die biometrischen Merkmale automatisiert gelesen werden können. Die gesetzliche Formulierung „Zone für das automatische Lesen“ weist darauf hin, dass der Gesetzgeber davon ausging, dass das Auslesen der Karte über eine direkte Kontaktverbindung zwischen Karte und Lesegerät erfolgt und nicht über Funktechnik (RFID). Gesetzlich ausgeschlossen wird der Einsatz von RFID-Technik nicht. Das Auslesen der sonstigen auf dem Ausweisdokument gespeicherten Identifizierungsdaten mit Hilfe der Funktechnik stößt mangels ausreichender Transparenz der Verarbeitung auf datenschutzrechtliche Vorbehalte. Mit Hilfe dieser Technik wäre eine Datenerhebung ohne Wissen des Ausweisinhabers möglich.

Für Pässe und Personalausweise ist geregelt, dass eine bundesweite Datei über biometrische Merkmale nicht eingerichtet wird. Ausgeschlossen ist auch eine „länderübergreifende Vernetzung der lokalen Register“. Der Gesetzgeber hat also ausdrücklich einer zentralen Auswertung biometrischer Daten eine Absage erteilt. Allerdings besteht eine entsprechende Vorschrift für Ausländerdokumente nicht.

Der automatisierte Abruf von Kartendaten beschränkt sich auf die alphanumerischen Identifizierungsdaten und schließt die biometrischen Angaben nicht mit ein. Der automatisierte Abruf ist im öffentlichen Bereich auf die Polizeibehörden und -dienststellen des Bundes und der Länder beschränkt sowie, soweit sie Aufgaben der Grenzkontrolle wahrnehmen, auf die Zollbehörden. Die Nutzung durch andere öffentliche Stellen beschränkt sich auf die Echtheits- und Identitätsprüfung.

Der automatisierte Abruf personenbezogener Daten (inkl. biometrischer Daten) sowie ihre automatisierte Speicherung durch nicht-öffentliche Stellen ist verboten. Ausdrücklich verboten ist die Nutzung der Seriennummer zum Abruf personenbezogener Daten aus Dateien oder zur Verknüpfung von Dateien. Damit soll ausgeschlossen werden, dass die Seriennummer als bereichsübergreifendes Personenkennezeichen verwendet wird.

Eine Nutzung der Ausweise durch ausländische öffentliche oder nicht-öffentliche Stellen ist bisher nicht gesetzlich geregelt. Dies basiert auf der Erwägung, dass die bisherigen Ausweise (von ausländischen Stellen) ausschließlich optisch gelesen werden. Die Offenbarung der Daten erfolgt mit Wissen (und i.d.R. Wollen) der Betroffenen. Soweit diese Offenbarung gegenüber ausländischen Stellen nicht freiwillig (zwangsweise) erfolgt, geschieht dies auf Grund ausländischen Rechts. Durch die Einführung automatisierter Identifizierungsverfahren ergibt sich eine neue rechtliche Situation: Bzgl. der elektronisch auf der Karte gespeicherten und evtl. ausgelesenen Daten besitzt der Karteninhaber in erheblich

geringerem Maße als bei den optisch lesbaren Angaben keine „Datenhoheit“. Dies hat zur Folge, dass rechtliche und technische Vorkehrungen getroffen werden müssen, um ein unzulässiges Auslesen von Daten (z.B. auch durch ausländische Stellen) zu verhindern.

### *3. Übermittlung von Flugpassagierdaten*

Die nachfolgende Darstellung ist eine Zusammenfassung des Dossiers zur Flugdaten-Affäre des Unabhängigen Landeszentrums für Datenschutz im virtuellen Datenschutzbüro unter <http://www.datenschutz.de/feature/detail/?featid=3>

Für detailliertere Informationen wird auf diese Quelle verwiesen.

Am 05.03.2003 ist ein US-Gesetz in Kraft getreten, das allen ausländischen Fluglinien in bzw. aus den USA vorschreibt, ihr Buchungssystem für die US-Zollbehörden zu öffnen. Die Öffentlichkeit erfuhr erst kurz vor diesem Datum, dass es eine Vereinbarung zwischen der EU-Kommission und den USA gibt, in der Einzelheiten des Datenzugriffs durch die USA festgelegt werden. Dabei wurden die Vorschriften der EG-Datenschutzrichtlinie, die gerade bei Datentransfers in Länder außerhalb der EU hohe Voraussetzungen vorschreibt, allem Anschein nach ignoriert.

Die USA hatten in Aussicht gestellt, dass im Falle der Verweigerung der Datenübermittlung die Landrechte entzogen würden. Offenbar haben einige der betroffenen europäischen Fluggesellschaften daraufhin ihre Bereitschaft signalisiert, die Daten zu übermitteln oder dem US-Zoll sogar Zugriff auf die Buchungssysteme zu geben. Besonders weit gehen die dem US-Zoll eingeräumten Rechte den Presseberichten zufolge bei der Lufthansa. Medienberichten zufolge kann diese wegen des von ihr verwendeten veralteten Buchungssystems weder die Zugriffe technisch auf bestimmte Datensätze einschränken noch diese protokollieren.

Das Europäische Parlament hat am 9.10.2003 nach monatelanger Kritik an der Vorgehensweise der EU-Kommission folgenden Beschluss gefasst. Das Parlament verlieh seiner verstärkten Position Ausdruck, indem es der Kommission auftrag, in den Verhandlungen mit den US-Zollbehörden die hinsichtlich der Flugdatenweitergabe geltenden EU-Datenschutzbestimmungen umzusetzen und den gegenwärtigen rechtswidrigen Zustand aufzuheben. Ende 2003 legte die EU-Kommission ein mit den USA ausgearbeitetes Abkommen vor, welches als Rechtsgrundlage dienend die Einzelheiten der Übermittlung von Fluggastdatensätzen an die US-Zollbehörden vorsieht. Da das Europäische Parlament auch dieses Übereinkommen als unvereinbar mit den geltenden EU-Datenschutzbestimmungen erachtet, hat es am 21.04.2004 mehrheitlich die Anrufung des Europäischen Gerichtshofs (EuGH) beschlossen.

### *4. Scoring-Verfahren*

Im Bereich der Privatwirtschaft werfen sogenannte Scoring-Verfahren, die zur automatisierten Beurteilung z.B. der Kreditwürdigkeit einer bestimmten Person anhand der Auswertung statistischer Vergleichsdaten verwendet werden, datenschutzrechtliche Fragen auf.

Einerseits werden die Verfahren selbst und die zum Vergleich herangezogenen Datenkategorien als Geschäftsgeheimnisse betrachtet und nicht bekannt gegeben. Damit ist der Betroffene eines Scoring-Verfahrens nicht in der Lage herauszufinden, auf welcher Grundlage ein Urteil über seine Kreditwürdigkeit gefällt wurde. Negative Score-Werte können zu schlechteren Vertragsbedingungen oder der gänzlichen Verweigerung eines Vertragsschlusses führen.

Andererseits sind Scoringsysteme, da sie einen Schluss auf die Zukunft beinhalten und die Bedingungen des konkreten Einzelfalles nicht mit einbeziehen können naturgemäß fehlerbehaftet. In der Kombination mit der oben beschriebenen mangelnden Transparenz der

Verfahren stehen die Betroffenen häufig vor rechtlich negativen Folgen eines Scoring ihrer Person, ohne zu wissen, auf welcher Grundlage diese Einschätzung beruht.

Datenschutzrechtlich sind solche Verfahren an den Vorgaben der §§ 28, 29 und 6a des Bundesdatenschutzgesetzes zu messen. In der Praxis sind jedoch bestimmte Teile dieser Vorschriften aufgrund von Nachweisproblemen nur schwer anzuwenden.

Es ist zu vermuten, dass Transparenzprobleme bei Scoring-Verfahren in Zukunft häufiger auf die Betroffenen zukommen, da solche Verfahren im Rahmen der Automatisierung und Rationalisierung von Entscheidungsprozessen und im Rahmen der Kreditsicherungsvorgaben der Basel II-Vereinbarung in der Privatwirtschaft verstärkt Anwendung finden werden.

### **III. Technischer Datenschutz**

#### *1. Warum technischer Datenschutz?*

Das Recht des Bürgers auf informationelle Selbstbestimmung ist nur schwer umzusetzen, wenn technische Vorgaben z.B. der Software eine datenschutzgerechte Nutzung von Produkten oder Dienstleistungen nicht zulassen. Einen effektiveren Schutz des allgemeinen Persönlichkeitsrechts der Nutzer verspricht daher eine von Beginn an an Datenschutzgesichtspunkten ausgerichtete Gestaltung von Technologie (privacy by design). Eine datenschutzfreundliche Nutzung von Technologie ist darüber hinaus auch durch eine veränderte Konfiguration oder die Verwendung zusätzlicher Produkte oder Dienstleistungen zu erreichen, die dem Betroffenen mehr Transparenz und Entscheidungsgewalt über die eigenen Daten einräumen. Die Information des Betroffenen über solche Möglichkeiten und die Entwicklung entsprechender Applikationen ist die Aufgabe des technischen Datenschutzes. Die nachfolgenden Beispiele sollen die Möglichkeiten technischen Datenschutzes näher illustrieren.

#### *2. Beispiele (Projekte des ULD)*

Die nachfolgende Darstellung ist eine Zusammenfassung der Web-Informationen des Unabhängigen Landeszentrums für Datenschutz unter <http://www.datenschutzzentrum.de/projekte/anon/index.htm>  
Für detailliertere Informationen wird auf diese Quelle verwiesen.

##### **a) Anonymes Surfen im Internet – AN.ON**

Beim Surfen hinterläßt eine Nutzerin oder ein Nutzer Datenspuren im Internet, die jederzeit personenbezogen die Rekonstruktion des Surfverhaltens ermöglichen. Diese Informationen fallen beispielsweise beim Provider oder mithörenden Dritten an. Neben der Möglichkeit, mit Hilfe von Verschlüsselung die Inhalte zu schützen, sollte man durch die Nutzung einer wirksamen Anonymisierung schon die Entstehung von Verbindungsdaten im Sinne des Gebotes der Datensparsamkeit vermeiden. Anonymität im Internet heißt, für alle anderen als die Kommunikationspartner oder Dritte, denen man sich offenbart hat, nicht identifizierbar zu sein. Anfragen an Daten bereit stellende Server bleiben damit verborgen und ermöglichen beispielsweise psychologische Beratungsleistungen oder alle auf einem wirksamen Identitätsmanagement basierenden Kommunikationsbeziehungen zwischen Kunden und Anbietern via Internet.

Eine technische Lösung für anonymes Surfen im Internet bietet ein Anonymisierer. Dies ist ein Programm bzw. eine ganze Kommunikationsarchitektur, die Kommunikationsbeziehungen zwischen Sendern und Empfängern im Internet verschleiert, so daß Sender und/oder Empfänger der Nachricht anonym bleiben und mithörende Dritte die abgefangenen Inhalte nicht mehr den Sendern und Empfängern zuordnen können.

Die einfachsten Anonymisierer sind so genannte Proxy-Server, die eine Internetanfrage stellvertretend für den Nutzer an den Server weiterleiten. Bei dieser Grund-Form von Anonymisierung, ist die Kommunikation aber sowohl gegenüber dem Provider als auch

gegenüber dem Betreiber des Proxy selbst nicht mehr anonym. Besser geeignet sind echte Anonymisierungs-Architekturen, wie z.B. ein Mix-Netz, das durch die verschlüsselte Weiterleitung von Nachrichten zwischen den Mix-Stationen eine Reidentifizierung der Kommunikation nur noch sehr schwer möglich macht.

Eine solche Anonymisierungslösung stellt der gemeinsam von den Universitäten Dresden, Regensburg, Freie Universität Berlin und dem Unabhängigen Landeszentrum für Datenschutz entwickelte Dienst AN.ON dar ([http://anon.inf.tu-dresden.de/index\\_en.html](http://anon.inf.tu-dresden.de/index_en.html)).

Grundlage ist das Programm Anonymity & Privacy (JAP), das auf einer Idee von David Chaum aus dem Jahre 1981 basiert, mit dem man anonym im Internet surfen kann. Bei der Installation auf dem heimischen Rechner wird ein Proxy vor dem eigenen Webbrowser installiert, der die Serveranfrage verschlüsselt und zum ersten Mix in einer Mix-Kaskade weitersendet. Somit weiß selbst der Provider nicht, welches eigentliche Surfziel vom Sender ausgewählt wurde. Danach versendet dieser Mix die von vielen Nutzern gesammelten und umkodierten Nachrichten in veränderter Reihenfolge weiter zum nächsten Mix der Kaskade. Erst der letzte Mix erkennt die Klaradresse des Empfängers und kann die Nachricht dann tatsächlich zustellen. Durch eine spezielle Form der Kodierung kann sowohl die Anonymität des Senders als auch die des Empfängers gewährleistet werden. Die durch den JAP erreichbare Qualität der Anonymisierung ist daher eine starke Form, die über einfache Proxy-Funktionalität weit hinaus geht.

## b) Identitätsmanagement

Die nachfolgende Darstellung ist eine Zusammenfassung der Web-Informationen des Unabhängigen Landeszentrums für Datenschutz unter <http://www.datenschutzzentrum.de/projekte/idmanage/index.htm> Für detailliertere Informationen wird auf diese Quelle verwiesen.

Identitätsmanagement ist in der realen Welt, ein von den Menschen seit Tausenden von Jahren eingeübtes Handeln. Je nachdem in welcher Situation oder Rolle man sich befindet, verhält man sich anders und gibt unterschiedliche Informationen von sich preis. So gibt sich derselbe Mensch im Beruf anders als im Privatbereich, in dem er oft eher bereit ist, auch persönliche Dinge von sich zu erzählen. Aber auch einzelnen Menschen gegenüber passt man sein Verhalten instinktiv an. Engen Freunden berichtet man persönlichste Angelegenheiten, während der Verkäuferin im Supermarkt möglichst nur die für die Kaufabwicklung unbedingt erforderlichen Daten mitgeteilt werden. Auch dem Kollegen, von dem man weiss, dass er alles weiterberichtet, erzählt man möglichst wenig und wählt eine reserviertere Identität, um einen Missbrauch seiner persönlichen Daten zu vermeiden.

Im Internet ist ein derartiges Verhalten instinktiven Identitätsmanagements schwieriger. Ohne technische Unterstützung ist es kaum noch nachvollziehbar, welche Daten durch welches Internetangebot und welche dahinter stehende Stelle gesammelt werden. Noch schwieriger wird es, die Quantität und Qualität seiner bekanntgegebenen Daten der jeweilige Situation anzupassen. Und selbst wenn der Benutzer meint, mit der Weitergabe persönlicher Daten vorsichtig umzugehen, droht die Gefahr, dass durch die Verbindung verschiedenster Daten, gesammelt von unterschiedlichen Webseiten, neue personenbezogene Daten entstehen.

Identitätsmanagement soll im Alltag überall dort helfen, wo Internetkommunikation stattfindet. Schon heute besitzen zahlreiche Nutzer eine eBay-Identität, die eine eigene Reputation aus zahlreichen Bewertungen durch andere eBay-Nutzer besitzt. Dieses ließe sich auf viele andere Nutzungsarten übertragen. Internetshops begegnet man mit seiner "Käufer"-Identität, die zwar bereit ist, ihre Adresse mitzuteilen, aber Geburtsdaten und Telefonnummern etc. für sich behält. Hierbei könnte wiederum unterschieden werden, ob man als Privatperson oder als Angestellter einer Firma einkauft. Selbsthilfegruppen im Internet will man eventuell zunächst anonym entgegentreten, beim Email-Kontakt mit Freunden aber offen sein.

Je mehr das Internet in die unterschiedlichsten Lebensbereiche des Einzelnen vordringt, um so komplizierter wird der Umgang mit verschiedenen Identitäten, der in der "Sekundenwelt"

des Internet für den einzelnen kaum zu bewältigen ist. Hierbei können und sollen Identitätsmanager helfen und die Technik transparent machen. Dies kann von der einfachen Passwort- und Zugangsverwaltung bis hin zum umfassenden situationsbezogenen Pseudonymmanagement gehen. Ziel ist stets die Vereinfachung der Internetkommunikation für den Einzelnen, ohne dass hiermit eine Verringerung der Sicherheit und des Datenschutzes einhergeht.

Erste Ansätze hierfür existieren bereits. Bei Systemen, die auf fremden Servern die Daten des Nutzers speichern, ist jedoch Vertrauen in die dahinter stehende Firma erforderlich. Der Weg hin zu einem intuitiven, selbstgesteuerten Auftreten im Internet ist noch lang, aber zur Verwirklichung des Grundrechts auf informationelle Selbstbestimmung unvermeidbar.

Das ULD ist im Bereich des Identitätsmanagement in verschiedenen EU-Projekten engagiert. Es sieht seine Aufgabe darin, den Weg für tatsächlich datenschutzgerechte Identitätsmanagementsysteme zu bereiten und so eine verfassungskonforme Technikgestaltung zu ermöglichen. Ziel ist das Datenschutztool der Zukunft, das allen Bürgern den selbstbewussten, situationsadäquaten und sozial verträglichen Umgang mit ihrer Identität erleichtern kann.

### c) Automatisiertes Datenschutzmanagement

Die nachfolgende Darstellung ist eine Zusammenfassung der Web-Informationen des Unabhängigen Landeszentrums für Datenschutz unter <http://www.datenschutzzentrum.de/epal> und <http://www.datenschutzzentrum.de/p3p>. Für detailliertere Informationen wird auf diese Quelle verwiesen.

Automatisiertes Datenschutzmanagement mit EPAL und P3P oder vergleichbaren Plattformen soll dazu beitragen das tatsächliche Datenschutzniveau in Organisationen zu erhöhen, indem Datenschutzerfordernisse automatisiert umgesetzt werden.

Die Enterprise Privacy Authorization Language (EPAL) ist eine formalisierte Sprache, um den Schutz personenbezogener Daten innerhalb eines Unternehmens und unternehmensübergreifend darstellen und durchsetzen zu können. Vereinfacht dargestellt werden dabei jedem von dem Unternehmen gesammelten personenbezogenen Daten Informationen beigefügt, anhand derer entschieden werden kann, wie die Daten benutzt werden dürfen. EPAL-Datenschutzinformationen dienen ausschließlich der Festlegung, wer personenbezogene Datenkategorien zu welchem Zweck wie verarbeiten darf und zwar unabhängig davon, welche Datenmodelle eine Software verwendet oder welche Zugriffsrechte dem Nutzer eines EDV-Systems allgemein zustehen.

EPAL soll ein einheitliches Datenschutzmanagement über Applikations-, Abteilungs- und sogar Firmengrenzen hinaus ermöglichen, ohne dabei die dezentrale Struktur der Erhebung, Speicherung, sonstige Verarbeitung oder Nutzung personenbezogener Daten aufzuheben oder zu behindern.

Datenschutzinformationen sollen maschinenlesbar vorgehalten werden, um datenschutzrechtliche Vorgaben, wie z.B. die Voraussetzungen einer Übermittlung oder die Löschung von personenbezogenen Daten für ein konkret vorliegendes Datum automatisiert durchführen zu können.

Durch EPAL sollen Unternehmen in die Lage versetzt werden, die Übereinstimmung ihrer Datenverarbeitung mit ihren Datenschutzerklärungen zu demonstrieren, Kosten für die Einführung und Durchsetzung ihrer Datenschutzzorgaben zu reduzieren und die Abweichungen zwischen existierenden Rechtsstandards und angewandten Verarbeitungspraktiken zu minimieren.

Es dient der Darstellung und Durchsetzung unternehmens- oder behördeninterner, personenbezogener Datenverarbeitung. Adressat von EPAL ist also das Datenschutzmanagement innerhalb eines Unternehmens oder einer Behörde.

Ergänzend zu EPAL existiert bereits P3P ("Platform for Privacy Preferences Externer Link"), eine international – durch das WWW Consortium Externer Link (W3C) - standardisierte, technische Plattform zum Austausch von Datenschutzinformationen im Internet. P3P hilft Internetsurfern auf Webseiten automatisiert und schnell einen Überblick zu gewinnen, welche ihrer personenbezogenen Daten der Webanbieter oder Dritte zu welchen Zwecken verarbeiten.

P3P (Platform for Privacy Preferences) basiert auf einer Formalisierung des Datenschutz-Angebots des Internet-Anbieter und der Datenschutzansprüche des Internetsurfers. Durch die Formalisierung im P3P-Format werden die Informationen maschinenlesbar; die Überprüfung, ob ein Anbieter den Datenschutzansprüchen des Nutzers genügt, wird damit automatisierbar.

EPAL und P3P sollen sich als Backend-Frontend-Lösung ergänzen. Um z.B. die automatisierte Erstellung von P3P-Datenschutzerklärungen aus EPAL-Datenschutzinformationen zu ermöglichen, werden P3P-Grundstrukturen in EPAL mit eingearbeitet.

#### **IV. Datenschutz als Wettbewerbsvorteil**

Datenschutz kann für Behörden und Unternehmen mehr sein, als nur die Erfüllung gesetzlicher Anforderungen. Der Bürger und Kunde vertraut Organisationen eher, wenn diese sich um seine Rechte kümmern und dies auch kommunizieren. Vertrauen wiederum ist die Basis jeder guten Geschäftsbeziehung.

Im Datenschutz kann ein Datenschutz-Audit oder ein Datenschutz-Gütesiegel eine solche vertrauensbildende Maßnahme darstellen. Das ULD bietet seit dem Jahr 2002 Datenschutz-Audits und Datenschutzgütesiegel auf gesetzlicher Grundlage an.

##### *1. Datenschutz-Gütesiegel*

Die nachfolgende Darstellung zum Gütesiegel ist eine Kurzfassung der Darstellung des Unabhängigen Landesentrums für Datenschutz abrufbar unter <http://www.datenschutzzentrum.de/guetesiegel>

Durch ein schleswig-holsteinisches Gütesiegel wird bescheinigt, dass die Vereinbarkeit eines Produktes mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde. Ein Gütesiegel können informationstechnische Produkte, also Hard- und Software, sowie Datenverarbeitungsverfahren erhalten. Voraussetzung ist zusätzlich, dass sie zur Nutzung durch öffentliche Stellen geeignet sind.

Zur Erlangung eines Gütesiegels beauftragen Hersteller- oder Vertriebsfirmen Sachverständige oder eine sachverständige Prüfstelle ihrer Wahl, die beim Unabhängigen Landeszentrum für Datenschutz akkreditiert ist. Diese führen die Prüfung des Produkts in rechtlicher und technischer Hinsicht durch und übersenden die schriftliche Dokumentation der Prüfung an das ULD. Ergibt die Nachprüfung durch das ULD keine Hinderungsgründe, so wird das Gütesiegel vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein für die geprüfte Programmversion verliehen. Angesichts des Tempos der Veränderungen der Informationstechnik werden Gütesiegel in der Regel auf zwei Jahre befristet verliehen. In einem vereinfachten Rezertifizierungsverfahren wird nach Ablauf des Siegels oder bei kleineren Veränderungen des Produkts überprüft, ob das Produkt oder seine Nachfolgeversion den aktuellen Vorschriften entspricht.

Inhaltlich wird vom Gutachter die Vereinbarkeit des Produkts mit den Vorschriften über Datenschutz und Datensicherheit überprüft. Besonderer Wert wird auf die Gesichtspunkte der Datenvermeidung und Datensparsamkeit, Datensicherheit und Revisionsfähigkeit sowie auf die Gewährleistung der Rechte der Betroffenen gelegt. Das ULD stellt einen

Anforderungskatalog für die IT-Produkte zur Verfügung, der gleichermaßen rechtliche und technische Aspekte beinhaltet. Dieser wird regelmäßig fortgeschrieben. Das ULD prüft in erster Linie die Schlüssigkeit des Gutachtens und die methodisch einwandfreie Vorgehensweise des Sachverständigen oder der sachverständigen Prüfstellen. In Zweifelsfällen kann auch das zu zertifizierende Produkt in Augenschein genommen werden.

## *2. Datenschutz-Audit*

Die nachfolgende Darstellung zum Datenschutz-Audit ist eine Kurzfassung der Darstellung des Unabhängigen Landeszentrum für Datenschutz abrufbar unter <http://www.datenschutzzentrum.de/audit>

Ein Datenschutzaudit ist die förmliche Prüfung des Datenschutzkonzepts einer öffentlichen Stelle durch das Unabhängige Landeszentrum für Datenschutz (ULD).

Alle öffentlichen Stellen in Schleswig-Holstein können entweder für ihre gesamte Datenverarbeitung, für abtrennbare Teile hiervon oder für einzelne Datenverarbeitungsverfahren ein Datenschutzaudit beantragen.

Das Datenschutzaudit wird durch das Unabhängige Landeszentrum für Datenschutz durchgeführt.

Grundlage des Audits ist eine schriftliche Vereinbarung der jeweiligen Behörde mit dem Unabhängigen Landeszentrum für Datenschutz. Danach erfolgen Bestandsaufnahme, Festlegung der Datenschutzziele, Einrichtung eines Datenschutzmanagementsystems, Begutachtung durch das ULD und schließlich die Verleihung des Datenschutzauditzeichens. Ein Datenschutzaudit wird für höchstens drei Jahre verliehen. Verlängerungen sind in einem vereinfachten Verfahren möglich.

Das Audit ist auch für Behörden oder Behördenteile möglich. Es ist primär darauf gerichtet, den Datenschutz zu verbessern und durch eine geeignete Organisation nachhaltig zu gewährleisten.

## **V. Kontrolle datenschutzrechtlicher Vorschriften in Deutschland**

Die Kontrolle datenschutzrechtlicher Regelungen ist in Deutschland auf verschiedene Stellen verteilt. Eine Aufteilung ergibt sich dabei aus der föderalen Struktur der Bundesrepublik Deutschland. Außerdem wird bei der Aufsicht über die verantwortlichen Stellen nach öffentlichen und nicht-öffentlichen Stellen unterschieden. Für diese gelten teilweise unterschiedliche Rechtsvorschriften.

Für die Datenschutzkontrolle in den öffentlichen Stellen der Bundesländer sind die Landesbeauftragten für den Datenschutz, für die Kontrolle in den öffentlichen Stellen des Bundes der Bundesbeauftragte für den Datenschutz zuständig.

Die Datenschutzkontrolle im nicht-öffentlichen Bereich (z.B. Wirtschaft, Vereine) obliegt den Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich der Länder. Diese hoheitliche Aufgabe ist teilweise den Landesbeauftragten für den Datenschutz, teilweise den Innenministerien und teilweise anderen öffentlichen Stellen angegliedert worden.

Für bestimmte inhaltliche Bereiche bestehen Sonderzuständigkeiten, so liegt z.B. dass Telekommunikationsrecht in der ausschließlichen Zuständigkeit des Bundesbeauftragten für den Datenschutz.

Das Unabhängige Landeszentrum für den Datenschutz (ULD, <http://www.datenschutzzentrum.de>) wird von dem Landesbeauftragten für den Datenschutz im Bundesland Schleswig-Holstein geleitet. Es nimmt außerdem die Aufgaben der Aufsichtsbehörde für den nicht-öffentlichen Bereich in Schleswig-Holstein wahr. Daneben betreibt das ULD das Innovationszentrum Datenschutz und Datensicherheit (<http://www.uld-i.de>), das interdisziplinär (unter Beteiligung von Juristen, Informatikern, Soziologen,

Betriebswirtschaftlern etc.) neue Ansätze zur Gewährleistung des informationellen Selbstbestimmungsrechts der Bürger entwickelt. In diesem Rahmen sind die zuvor vorgestellten Projekte zum technischen Datenschutz und zum Datenschutz-Audit und – gütesiegel durchgeführt worden.

Neben den dargestellten Datenschutzaufsichtsbehörden, die mit Kontrollbefugnissen und der Möglichkeit zur Verhängung von Bussgeldern ausgestattet sind, setzt das deutsche Datenschutzrecht zusätzlich auf eine Selbstkontrolle der verantwortlichen öffentlichen und nicht-öffentlichen Stellen.

Dafür besteht für nicht-öffentliche Stellen mit einem bestimmten Umfang oder einer bestimmten Intensität an personenbezogener Datenverarbeitung die Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen. Dieser soll ein betriebliches Datenschutzmanagement aufbauen und betreiben. Zu seinen Aufgaben gehört neben der Beratung der Geschäftsleitung und der Betroffenen in Fragen des Datenschutzes, die Führung eines Verzeichnisses aller personenbezogener Datenverarbeitungsverfahren der verantwortlichen Stelle, die Schulung der Mitarbeiter in Datenschutzfragen, die Vorabkontrolle besonders invasiver Datenverarbeitungsverfahren vor ihrer Einführung und die regelmäßige Kontrolle der Umsetzung der Datenschutzvorschriften im Unternehmen. Die Pflichtbestellung eines betrieblichen Datenschutzbeauftragten, der fachkundig und zuverlässig sein muss, stellt sicher, dass das notwendige Datenschutzwissen auch in den Unternehmen und Vereinen vorhanden ist und ein kompetenter Ansprechpartner zur Verfügung steht.

Parallel zu den betrieblichen Datenschutzbeauftragten können in öffentlichen Stellen behördliche Datenschutzbeauftragte bestellt werden.

Neben den genannten Kontrollinstanzen besteht für bestimmte Personen und Gruppen die Möglichkeit Datenschutzverstöße auf zivilrechtlichem Wege als Verstöße gegen das Wettbewerbsrecht oder gegen das Verbraucherrecht (eingeschränkt) zu verfolgen.

Allen genannten Kontrollinstanzen ist gemein, dass sie die gesetzlich garantierten Datenschutzrechte der Bürger nicht selten gegen die entgegenstehenden Interessen der verantwortlichen Stellen (z.B. des eigenen Unternehmens oder der eigenen Behörde, gegen ganze Wirtschaftskreise oder gegen Regierungsstellen) durchsetzen müssen. Für eine effektive Rechtsdurchsetzung ist daher eine unabhängige Stellung der Datenschutzkontrollinstanzen unablässig. Für die betrieblichen Datenschutzbeauftragten wird dies im deutschen Datenschutzrecht durch eine direkte Unterstellung unter die Geschäftsleitung und einen funktionalen Kündigungsschutz gewährleistet.

Aufsichtsbehörden für den Datenschutz müssen ihre Entscheidungen weisungsungebunden treffen können, um eine Einflussnahme von Regierungsstellen oder Lobbyistenvereinigungen zu Lasten des Grundrechts der Bürger auszuschließen. Auch eine indirekte Einflussnahme über Personalentscheidungen oder das Budgetrecht sollte organisatorisch vermieden werden.