Privacy by Design

Angesichts des rapiden und dramatischen technologischen Wandels gilt es, die besonderen Erfordernisse des Datenschutzes bereits zu einem frühen Zeitpunkt zu berücksichtigen, da neue technologische Systeme oftmals versteckte Gefahren bergen, die sich nur schwer beseitigen lassen, wenn die Grundkonzeption erst einmal feststeht. Daher ist es umso sinnvoller, etwaige Datenschutzprobleme schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen und den Datenschutz von vorneherein in die Gesamtkonzeption einzubeziehen anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme zu beheben. Dieser Ansatz wird als *"Privacy by Design"(PbD)* bezeichnet.

PbD ist nützlich für alle Arten von IT-Systemen, die für die Verarbeitung personenbezogener Daten vorgesehen sind oder eingesetzt werden. PbD sollte eine wesentliche Anforderung sein, die durch alle Produkte und Dienstleistungen zu erfüllen ist, welche Dritten und einzelnen Kunden zur Verfügung gestellt werden (z. B. WiFi-Router, soziale Netzwerke und Suchmaschinen). Viele Nutzer verfügen nur über beschränkte IT-Kenntnisse und sind daher nicht in der Lage, die einschlägigen Sicherheitsmaßnahmen selbst zu ergreifen, um ihre eigenen oder die personenbezogenen Daten Dritter zu schützen. Daher ist im Zusammenhang mit diesen IT-Verfahren stets ein Grundschutz erforderlich (privacy by default). Darüber hinaus müssen Anbieter die Nutzer in die Lage versetzen, ihre personenbezogenen Daten besser zu schützen, indem sie beispielsweise geeignete Datenschutztools bereitstellen (Zugangskotrollen, Verschlüsselung, Vorkehrungen für die anonyme Nutzung).

Der Gedanke, den technischen Datenschutz in IT-Systeme zu integrieren ist nicht völlig neu. Im Erwägungsgrund 46 der Richtlinie 95/46 der Europäischen Union wird z. B. darauf verwiesen, dass sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen sind, um insbesondere die Sicherheit zu gewährleisten. PbD jedoch umfasst mehr als nur die Gewährleistung der Sicherheit. PbD beinhaltet auch den Gedanken, dass Systeme so konzipiert und konstruiert sein sollten dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung oder möglichst baldige Löschung personenbezogener Daten.

Die nachstehenden Beispiele zeigen auf, wie PbD zur Verbesserung des Datenschutzes beitragen kann:

Elektronische Gesundheitskarte

Seit einigen Jahren bereitet sich Deutschland auf die Einführung einer elektronischen Gesundheitskarte vor, einer Chipkarte mit einem integrierten Mikroprozessor, der Zusatzfunktionen ermöglicht, insbesondere die Verifikation der digitalen Identität des Karteninhabers im Rahmen der Telematik-Infrastruktur des Gesundheitssektors. Die Chipkarte wird zunächst die Verwaltungsdaten des Karteninhabers enthalten, die bereits auf der magnetischen Krankenversicherungskarte gespeichert sind. Die Möglichkeit, weitere Daten zu speichern (z. B. Angaben zu in der Vergangenheit verordneten Medikamenten, Informationen für den medizinischen Notfall, elektronische Patientenakte) soll später hinzukommen.

Durch die neue elektronische Gesundheitskarte sollte der Datenschutz für die Patienten sich im Vergleich mit dem bestehenden System zumindest nicht verschlechtern. Ziel ist es vielmehr, die Transparenz für die Versicherten zu verbessern und ihnen umfangreiche Optionen für die Verwendung ihrer medizinischen Daten zu geben. Bei allen Anwendungen, für die sie sich entscheiden, sollen die Karteninhaber die Kontrolle über ihre Daten behalten und in der Lage sein, selbst so weit als möglich darüber zu entscheiden, inwieweit ihre gesundheitsbezogenen Daten auf der Chipkarte und in der Telematik-Infrastruktur gespeichert und wie diese genutzt werden sollen. Die Chipkarte soll mit technischen Merkmalen ausgestattet sein, die den Karteninhabern die Möglichkeit gibt, ihre eigenen Daten und die Zugriffsrechte zu diesen Daten zu verwalten.

Die Karte und die Telematik-Infrastruktur müssen so einfach konzipiert sein, dass sie von den Karteninhabern genutzt werden können. Alltagstaugliche Verfahren, die den Durchschnittsnutzer in die Lage versetzen, seine Datenhoheit und Patientenrechte aktive auszuüben, sind eine Grundvoraussetzung für die Einführung der elektronischen Gesundheitskarte und den Betrieb der Telematik-Infrastruktur.

Bei den Bemühungen um die Modernisierung des Gesundheitssektors ist zu berücksichtigen, dass es gilt, die Souveränität der Patienten und ihre Rechte zu stärken und die Einbeziehung der Patienten auszubauen. Konzentrierte sich der Einsatz der IT im Gesundheitssektor ausschließlich auf eine Verbesserung der Kosteneffizienz und eine Beschleunigung der Verarbeitungszeiten ohne dabei gleichzeitig den Datenschutz und die Patientenrechte im Auge zu behalten, so würde er nur geringe Akzeptanz finden und kaum Aussichten auf Umsetzung haben.

Aus diesem Grunde müssen die technischen Verfahren alltagstauglich und für alle Versicherten anwendbar sein, damit diese aktiv ihre Beteiligungs- und Kontrollrechte ausüben können. Damit bieten die elektronische Gesundheitskarte und die Telematik-Infrastruktur die Möglichkeit, den Zugang zu Gesundheitsdaten zu verbessern, die medizinische Behandlung zu optimieren und gleichzeitig die Kontrolle der Patienten über ihre eigenen Daten zu verbessern. Die eingesetzte Technologie muss die Einhaltung der Datenschutzgrundsätze dauerhaft gewährleisten.

Letztlich muss die gesamte technische Infrastruktur primär an dem Nutzen für die Patienten ausgerichtet sein. Sämtliche Komponenten, Schnittstellen, Dienstleistungen und Verfahren in der Gesundheitstelematik müssen optimal funktionieren und den Erfordernissen des Datenschutzes und der Datensicherheit entsprechen.

Alle an der Entwicklung der elektronischen Gesundheitskarte Beteiligten haben sich darauf verständigt, die folgenden Grundsätze zu beachten:

(1) **Datenhoheit:** Der Versicherte hat umfassende Kontrolle über seine Gesundheitsdaten, die in der elektronischen Gesundheitskarte oder in der Telematik-Infrastruktur verarbeitet werden sollen. Die freiwilligen medizinischen Anwendungen können nur mit ausdrücklicher Zustimmung des Versicherten und nur sofern er Zugriff zu diesen Daten gewährt genutzt werden.

(2) **Freiwillige Grundlage:** Gesundheitsdaten sollen nur auf freiwilliger Basis, nach Ermessen des Versicherten gespeichert werden. Die Frage,

ob ein Versicherter den Zugang zu seinen Daten erlaubt oder verweigert, darf nicht dazu führen, dass er bevorzugt behandelt bzw. benachteiligt wird.

(3) **Datenumfang:** Der Versicherte muss in der Lage sein, zu entscheiden, welche Gesundheitsdaten aufgenommen werden und wann sie gelöscht werden sollten.

(4) **Datenzugang:** Der Versicherte muss in der Lage sein, im Einzelfall zu entscheiden, welcher Dienstleistungserbringer (Arzt, Apotheker, Hebamme usw.) Zugang zu welchen Daten haben soll.

(5) **Informationsrecht:** Der Versicherte hat das Recht, seine eigenen Daten zu lesen und über sie und alle sie betreffenden Verfahren informiert zu werden.

(6) **Überprüfungsmöglichkeit:** Der Versicherte muss in der Lage sein, mit Hilfe von Protokollen zu überprüfen wer wann auf welche Daten zugegriffen hat.

Die derzeit in der Erprobung befindlichen technischen Verfahren und die robusten Sicherheitsmechanismen, die in die Chipkarte und die Telematik-Infrastruktur eingebaut wurden, sind darauf ausgerichtet, die Einhaltung dieser Datenschutzgrundsätze und damit auch die aktive Beteiligung der Versicherten zu gewährleisten, was die Gewährung des Datenzugangs und die Verwaltung ihrer medizinischen Daten und Zugriffsrechte angeht.

Datenschutz und Datensicherheit sind bei der Konzeption der Verfahren und Technologie berücksichtigt worden. Sämtliche Komponenten, die für die Daten-

sicherheit von wesentlicher Bedeutung sind – und dies umfasst sämtliche für die Datenverschlüsselung und die Überprüfung der Authentizität der Teilnehmer benötigten Komponenten -, müssen gemäß einem in den Gemeinsamen Kriterien festgelegten Sicherheitsprofil zertifiziert sein, um ihre Vertrauenswürdigkeit zu verifizieren.

Alle Nutzer – Patienten, Versicherte und Angehörige der medizinischen Berufe – müssen in der Lage sein, die Systeme sicher und einfach zu nutzen. Verfahren, die gewährleisten sollen, dass die Datensubjekte ihre Rechte aktiv ausüben können, müssen praktisch und alltagstauglich sein, so dass die neue Technologie keine Diskriminierung (z. B. älterer oder kranker Personen) zur Folge hat; unter anderem bedeutet dies, dass

- nicht davon ausgegangen werden kann, dass Versicherte über technische Geräte/Vorrichtungen verfügen;

- Versicherte in der Lage sein müssen, diese Verfahren bequem im Zusammenhang mit einer Behandlung zu nutzen, z. B. in der Arztpraxis oder beim Einlösen eines elektronischen Arzneimittelrezeptes in der Apotheke; und dass

- es möglich sein muss, Anwendungen und Rechte durch Verwendung einer bequemen, standardisierten und leicht verständlichen Schnittstelle zu verwalten.

Die Praktikabilität eines Systems und seine Alltagstauglichkeit sind ein wichtiges Kriterium für die Verwaltbarkeit des Systems und die Gewährleistung eines wirksamen Datenschutzes. Sämtliche Geschäftsabläufe müssen für alle Beteiligten verständlich und möglichst einfach sein. Aus diesem Kriterium ergeben

sich hohe Anforderungen an die Konzeption der Anwendungen für die Versicherten, denn alle Versicherten, nicht nur jene, die über ausgeprägte Erfahrungen im Umgang mit Computern verfügen, müssen in der Lage sein, ihre Rechte auszuüben. Der allgemeine Grundsatz, demzufolge es keine Diskriminierung von Personen mit geringen Computerkenntnissen geben darf, gilt insbesondere im Bereich des Gesundheitswesens. Insbesondere bei der Konzeption von Systemen kommt es darauf an, sicherzustellen, dass die neue Technologie keine Diskriminierung älterer oder kranker Personen mit sich bringt.

Je komplexer ein System und seine Sicherheitsfunktionen jedoch werden (z. B. lange Passwörter oder PINs, unterschiedliche Rechte für unterschiedliche Nutzergruppen), desto höher werden die Ansprüche an die Systemnutzer. Ab einem bestimmten Punkt wird diese Komplexität kontraproduktiv: In der praktischen Anwendung sind die Verfahren dann weniger effektiv und weniger transparent und können unerwünschte Nebenwirkungen und neue Sicherheitsrisiken zur Folge haben.

Daher muss im Vorfeld abgeklärt werden, wie mit bestimmten vorhersehbaren Konstellationen umzugehen ist, in denen Versicherte nicht in der Lage sind, die Sicherheitsfunktionen auf der elektronischen Gesundheitskarte zu bedienen. Dies gilt beispielsweise für körperlich oder geistig Behinderte und für Personen in Extremsituationen, z. B. wenn der Versicherte nicht bei Bewusstsein ist und ein unmittelbarer Zugriff auf bestimmte medizinische Daten dringend erforderlich ist. Eine Lösung könnte darin bestehen, dass die Karteninhaber ihrem Arzt für den Fall, dass sie selbst nicht dazu in der Lage sind, die Befugnis erteilen, ihre Zugriffsrechte zu verwalten. Aber selbst in diesem Fall muss gewährleistet sein, dass das Datensubjekt letztlich darüber entscheidet, wer wann Zugriff auf seine Daten hat.

Aus diesem Grunde muss die Konzeption des Systems sorgfältig geplant werden. Die wichtigsten Komponenten des Systems werden derzeit einer umfangreichen Erprobung unterzogen, in deren Rahmen eine Feinabstimmung der Systemspezifikationen im Lichte der gewonnenen praktischen Erfahrungen erfolgt.

Meiner Meinung nach könnte die elektronische Gesundheitskarte zu einem Musterbeispiel dafür werden, wie man Datenschutz und Datensicherheit unter Verwendung datenschutzfreundlicher Technologie gewährleistet, wenn die aufgeführten Konzeptionsgrundsätze konsequent umgesetzt werden. Sowohl das Gesundheitswesen als auch die Rechte der Datensubjekte könnten von der neuen Chipkarte profitieren.

Seit Beginn der Einführung der elektronischen Gesundheitskarte hat es jedoch kürzlich Anzeichen dafür gegeben, dass nicht alle Beteiligten bereit sind, die Kosten für die komplexe Infrastruktur zu tragen, die nach dem Datenschutzgesetz erforderlich ist. So haben bestimmte Kreise der Ärzteschaft sich dagegen gewehrt, neue Hardware zu kaufen, um den Sicherheitsstandards zu entsprechen und stattdessen entsprechende Softwarelösungen gefordert, um so Kosten einsparen zu können. Ich bezweifele, dass es möglich sein wird, die angestrebten und vom Gesetz geforderten Sicherheitsstandards auf diese Weise zu gewährleisten.

Elektronischer Personalausweis

Ein weiteres Beispiel für datenschutzfreundliches Design könnte der neue elektronische Personalausweis der Bundesrepublik Deutschland sein, der Ende 2010 eingeführt werden soll.

Angesichts der datenschutzrechtlichen Kontroverse, die im Zusammenhang mit der Einführung des mit biometrischen Merkmalen ausgestatteten digitalen Reisepasses vor einigen Jahren entstand, mag diese positive Einschätzung gewissermaßen merkwürdig erscheinen. Der elektronische Personalausweis wird nicht nur als offizielles Ausweisdokument dienen, sondern auch die Möglichkeit bieten, die Identität des Ausweisinhabers elektronisch zu überprüfen, und zwar auf eine Art und Weise, die den datenschutzrechtlichen Anforderungen von Anfang an Rechnung trägt. Dank dieser Funktion kann der neue Personalausweis genutzt werden, um die Identität des Karteninhabers bei der Nutzung von Internetdiensten zu verifizieren. Optional wird der neue Personalausweis auch eine Funktion für die elektronische Unterschrift bieten; ebenso wie die Identitätsüberprüfungsfunktion wird die Funktion für die elektronische Unterschrift nur auf ausdrücklichen Wunsch des Ausweisinhabers aktiviert.

Der Personalausweis erfüllt wesentliche Datenschutzanforderungen auch hinsichtlich der biometrischen Merkmale (digitales Gesichtsbild und Fingerabdrücke), auf die ausschließlich Beamte zum Zwecke der Identitätsüberprüfung zugreifen können. Diese biometrischen Merkmale sind elektronisch auf einem besonders gesicherten Teil des Chips gespeichert. Es wurden neue Rechtsvorschriften verabschiedet, um sicherzustellen, dass nur das digitale Gesichtsbild verpflichtend gespeichert wird; die Karteninhaber können selbst entscheiden, ob auch ihre Fingerabdrücke auf dem Chip gespeichert werden sollen.

Privacy by Design bedeutet vor allem Datensicherheit. Bei dem neuen elektronischen Personalausweis wird diese durch den geschützten Zugriff auf biometrische und elektronisch gespeicherte Identitätsdaten und durch gesicherte Übertragungskanäle gewährleistet. Das gesetzlich geforderte Verfahren entspricht diesen Anforderungen weitgehend, und die im Rahmen dieses Systems eingesetzten Komponenten müssen auf der Grundlage einheitlicher Sicherheitskriterien zertifiziert sein.

Aber Privacy by Design bewirkt mehr als nur die Gewährleistung des Datenschutzes; Privacy by Design bedeutet auch, die Erhebung und Verarbeitung personenbezogener Daten auf ein Minimum zu beschränken (Grundsatz der Datensparsamkeit). In Bezug auf den neuen Personalausweis könnte dies bedeuten, dass die Möglichkeit ausgeschlossen wird, ereignis- und ortsbezogene Daten zu speichern, so dass kein datenbezogenes Profil „auf“ dem Personalausweis erstellt werden kann. Weder in der Vergangenheit durch Beamte erfolgte Überprüfungen biometrischer Daten noch Geschäftskontakte, bei denen die Identitätsüberprüfungsfunktion genutzt wurde, ließen sich aus der entsprechenden Zone des Chips ablesen und schon gar nicht durch die andere Zone auslesen und speichern. Dadurch wird verhindert, dass Daten generiert werden, wenn der neue Personalausweis für verschiedene Zwecke verwendet wird und dass sie genutzt werden, um Bewegungs- oder Verhaltensprofile abzuleiten.

Ein gutes Beispiel für Privacy by Design wäre die Möglichkeit, im Rahmen der elektronischen Identitätsüberprüfungsfunktion unterschiedliche Pseudonyme für unterschiedliche Dienstleistungsanbieter verwenden zu können. Der Karteninhaber sollte die Möglichkeit haben, zu wählen, welchen Namen er gegenüber welchem Unternehmen bzw. gegenüber welcher Behörde verwendet (Privacy by Design als Rollenstrategie). Wichtig ist auch, dass der neue Personalausweis eine Funktion zur Überprüfung des Alters des Ausweisinhabers umfasst. Be-

stimmte Dienstleistungen kann man erst ab einem bestimmten Alter (z. B. 18 Jahre) in Anspruch nehmen, und diese Funktion ermöglicht es, das Alter des Ausweisinhabers zu verifizieren, ohne seinen Namen, seine Adresse oder sein genaues Geburtsdatum preiszugeben.

Privacy by Design bedeutet auch, dass man die künftige Missbrauchsanfälligkeit ursprünglich sicherer Technologien gründlich analysiert und bewertet. In diesem Zusammenhang sollte zum Beispiel auch die Gültigkeitsdauer von Zertifikaten nicht zu lang gewählt werden. Bei der Konzeption technischer Systeme gilt es auch zu bedenken, dass die immer leistungsfähiger werdenden Rechnersysteme in einigen Jahren in der Lage sein werden, Verschlüsselungen und Zugangskodes zu entschlüsseln, die heute noch als unüberwindbar gelten. Weitere Sicherheitslücken ergeben sich vielleicht erst im Verlauf der Zeit. Daher müssen die Systeme so ausgelegt sein, dass bestimmte Sicherheitsvorkehrungen zu einem späteren Zeitpunkt optimiert oder hinzugefügt werden können.

In einem weiteren und abstrakteren Sinne und über die Anforderungen gemäß Paragraph 3a und 9 des Bundesdatenschutzgesetzes hinaus, bedeutet Privacy by Design auch, dass man technologische, wirtschaftliche und gesellschaftliche Entwicklungen und das Zwischenspiel zwischen ihnen vorwegnimmt, um den Datenschutz für Morgen bereits in die IT von heute einzubauen oder, wo dies nicht möglich ist, die Lebensdauer der eingesetzten Technologien und Verfahren zu begrenzen.

Elektronischer Entgeldnachweis (ELENA)

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit wurde in einem sehr frühen Stadium in die Planung eines Projektes einbezogen, das seit dem 1. Januar 2010 unter dem Namen ELENA bekannt ist, eine Abkürzung, die für Elektronischer Entgeldnachweis steht. ELENA ist eine Datenbank, in der sämtliche Einkommensdaten der in Deutschland Erwerbstätigen gespeichert und verwendet werden, um elektronische Entgeldnachweise zu erstellen, die im Bedarfsfall an die Sozialbehörden weiter geleitet werden, wenn z. B. bestimmte Sozialleistungen beantragt werden.
ELENA wurde geschaffen, um das vorherige Verfahren zu ersetzen, bei dem der Arbeitgeber ein bestimmtes amtliches Formular verwendete, um bestimmte Einkommensdaten und andere Daten über den Beschäftigten, der Sozialleistungen beantragte, anzugeben. Die Daten werden zur Berechnung von Sozialleistungen wie z. B. des Kindergeldes benötigt. Viele dieser Daten müssen als sensitiv gelten und könnten leicht missbraucht werden, so dass ihrer Sicherheit besonderes Augenmerk zukommt.

Um dies zu gewährleisten wurden bei der Entwicklung der Verfahren und Anwendungen besondere datenschutzrechtliche Bestimmungen des Zehnten Buches des Bundessozialgesetzbuches und des Bundesdatenschutzgesetztes sowie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegte Spezifikationen berücksichtigt. Darüber hinaus wurden die folgenden datenschutzrechtlichen Grundsätze beachtet:

1. Verschlüsselung sämtlicher Übertragungskanäle und sämtlicher Dateien in der Datenbank;
2. räumliche, organisatorische, technische und personelle Trennung zwischen der zentralen Datenbank und der für die Registrierung der Teilnehmer und die Verarbeitung ihrer Daten zuständigen Stelle;

3. strikte Trennung zwischen der Daten speichernden Stelle und der für die Verwaltung des Hauptschlüssels zuständigen Stelle. Der Deutsche Bundestag hat mir, dem Bundesbeauftragten für Datenschutz und Informationsfreiheit, die Zuständigkeit für die Verwaltung des Hauptschlüssels übertragen;
4. Protokollierung sämtlicher Datenbanktransaktionen, -abfragen usw., um sämtliche Datenverarbeitungsoperationen für eine Prüfung durch die datenschutzrechtlichen Aufsichtsbehörden zu dokumentieren;
5. unverzügliche und gezielte Löschung von Daten, wenn sie nicht mehr benötigt werden;
6. interne technische Trennung und Isolierung sämtlicher an dem System beteiligten Organisationseinheiten und Festlegung eines inneren und äußeren Sicherheitsschutzes, jeweils mit eigenen physischen Barrieren und Überwachungsmechanismen;
7. grundsätzliche Erfordernis von zwei Unterschriften für die Datenabfrage (die abfragende Stelle und das Datensubjekt müssen der Datenabfrage in jedem Fall zustimmen, indem sie eine Signaturkarte vorlegen, die eine gesetzlich vorgeschriebene qualifizierte Signatur trägt);
8. ausschließlich die hierzu befugten Behörden und ihre Bediensteten sind (vorbehaltlich inhaltlicher und zeitlicher Einschränkungen) berechtigt, diejenigen Informationen aus der Datei abzurufen, die sie zur Erfüllung ihrer jeweiligen Aufgaben benötigen;
9. technische Maßnahmen, um zu gewährleisten, dass Daten nur für die Zwecke verwendet werden, für die sie ursprünglich erhoben wurden und dass insbesondere die Sicherheitsbehörden, die Finanzbehörden, der Zoll u. ä. keinen Zugang erhalten.

Die Integration dieser datenschutzrechtlichen Grundsätze in dieses komplexe System und damit die Wahrung der Datenschutzrechte des Einzelnen konnten

nur dadurch gewährleistet werden, das die Datenschutzbehörden bereits in einem frühen Stadium in die Planung einbezogen wurden.

Obwohl den Erfordernissen des Datenschutzes Rechnung getragen wurde, gab es in den Monaten vor seiner Einführung zunehmend Kritik an ELENA. Die Kritik konzentrierte sich zunächst auf die Menge der Daten, die von nun an, wenn auch in verschlüsselter Form, zentral gespeichert werden sollen und die zuvor nur durch die Arbeitgeber verwaltet wurden. Diese Kritik war zumindest teilweise nachvollziehbar und berechtigt.
Obwohl die Systemkonzeption die oben beschriebenen, äußerst wirksamen und technisch komplexen Schutzmaßnahmen umfasst, hatte man nur kursorisch geprüft, inwieweit tatsächlich eine Notwendigkeit zur Erhebung der verschiedenen Daten bestand. Die bis dahin für die Entgeltmeldungen verwendeten Papierformulare bildeten im Wesentlichen die Ausgangsbasis für die Datenerhebung; dies führte dazu, dass alle im Rahmen des konventionellen Verfahrens erhobenen Daten auch in das neue ELENA-System aufgenommen wurden. Es wurde jedoch deutlich, dass berechtigte Zweifel an der Notwendigkeit bestimmter Datenfelder bestanden. Diese Erfahrung zeigte, dass Privacy by Design nicht auf die Gewährleistung der Datensicherheit und auf technische Datenschutzfunktionen (wie die Nutzung elektronischer Signaturkarten und Datenverschlüsselung) reduziert werden sollte und dass ein solcher Prozess einer Entwicklung unterliegt und neuen Erfordernissen Rechnung tragen muss.

Das Beispiel ELENA zeigt auch, dass PbD sich nicht auf die Entwicklung cleverer technischer Lösungen und deren Integration in Systeme beschränken sollte. Ebenso wichtig ist es, schon früh im Planungsprozess zu prüfen, ob und wie die Mengen personenbezogener Daten auf das absolut erforderliche Minimum beschränkt werden können. Die Tendenz, zunehmend komplizierte bürokratische

Systeme in der Informationstechnologie exakt abzubilden, wird auch bei anderen IT-Prozessen deutlich und stellt den Datenschutz mitunter vor große Probleme. Diese Gefahr besteht selbst dann, wenn große Anstrengungen unternommen werden, um den Datenschutz zu gewährleisten und Datenmissbrauch zu verhindern.

Der Grundsatz des *Privacy by Design* sollte für Technologieentwickler und –hersteller ebenso verbindlich sein wie für diejenigen, die für die Daten verantwortlich sind und über die Beschaffung und den Einsatz von IT-Systemen zu entscheiden haben. Sie sollten verpflichtet sein, dem technologischen Datenschutz bereits in der Planungsphase von IT-Verfahren und –Systemen Rechnung zu tragen. Die Anbieter von IT-Systemen und -Dienstleistungen sollten als Datenverantwortliche zeigen, dass sie alle erforderlichen Maßnahmen getroffen haben, um diesen Erfordernissen zu genügen.

Bei Entscheidungen über die Konzeption eines Verarbeitungssystems, seine Beschaffung und seinen Betrieb sollten die nachstehend aufgeführten allgemeinen Zielsetzungen beachtet werden:

- **Datenvermeidung**: Datenverarbeitungssysteme sollten so ausgelegt und ausgewählt werden, dass keine oder möglichst wenig personenbezogene Daten erhoben, verarbeitet und verwendet werden.
- **Kontrollierbarkeit:** Ein IT-System sollte den Datensubjekten die wirksame Kontrolle über ihre personenbezogenen Daten geben. Die Zustimmungs- bzw. Widerspruchsmöglichkeit sollte durch technologische Mittel unterstützt werden.

- **Transparenz**: Sowohl die Entwickler als auch die Betreiber von IT-Systemen haben sicher zu stellen, dass die Datensubjekte detailliert über die Funktionsweise der Systeme informiert werden.
- **Vertraulichkeit der Daten:** IT-Systeme sind so zu konzipieren und zu sichern, dass nur entsprechend autorisierte Stellen Zugriff auf personenbezogene Daten haben.
- **Datenqualität**: Die Datenverantwortlichen müssen die Datenqualität durch technische Mittel unterstützen. Einschlägige Daten sollten im Bedarfsfall für rechtmäßige Zwecke zugänglich sein.
- **Möglichkeit der Trennung**: IT-Systeme, die für verschiedene Zwecke eingesetzt werden können oder in einer Mehrbenutzerumgebung betrieben werden (d. h. virtuell verbundene Systeme wie z. B. data warehouses, cloud computing) müssen sicherstellen, dass Daten und Prozesse, die für verschiedene Aufgaben oder Zwecke verwendet werden, sicher voneinander getrennt werden können.

Aus der zunehmenden Bedeutung, die dem Datenschutz bei der Entwicklung und beim Betrieb von IT-Systemen zukommt, ergeben sich zusätzliche Anforderungen an IT-Spezialisten. Aus diesem Grunde muss der Datenschutz wichtiger Bestandteil der Ausbildung von IT-Spezialisten sein.