KERSTIN BLOSSEY
OLIVER KEMPKENS

Datenschutz

Schwierigkeitsgrad:

Datenschutz ist in aller Munde: Kaum eine technische Abhandlung, die einem breiteren Publikum gerecht werden soll, ohne diesen Begriff. Doch Hintergründe, Fakten und wertvolle Impulse für die Arbeitspraxis bleiben nur allzu oft im Dunkeln. Deshalb widmet HAKIN9 diesem Thema ab sofort eine eigene Rubrik.

Der Begriff *Datenschutz* an sich ist verwirrend, denkbar unkonkret und sogar irreführend. Das belegen allein die vielfältigen Definitionen, die je nach Herkunft ihres Schöpfergeistes sehr unterschiedlich geprägt sein können und selten zufriedenstellend sind. Datenschutz im Sinne des Bundesdatenschutzgesetzes (BDSG) – und darauf als sachlich-rechtliche Grundlage beschränkt sich dieser Artikel – meint weniger den Schutz von Daten als viel mehr den Schutz, von dem was Sinn macht, dem Schutz der Privatsphäre des Menschen. *Daten-Schutz* ist dabei ein ebenso technisch wie organisatorisch zu betrachtender Teilaspekt.

Datenschutz – gesetzliche Anforderung an alle

Mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 23. Mai 2001 wurde die EU-Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr in Deutschland umgesetzt. Dies geschah jedoch erst, nachdem ein Vertragsverletzungsverfahren der EU-Kommission gestartet wurde, da Deutschland nicht innerhalb der Drei-Jahres-Frist die Richtlinie in nationales Recht umgesetzt hatte. Seither sind bundesweit alle Stellen, unabhängig davon ob öffentlich, halböffentlich oder privatwirtschaftlich, zum angemessenen Schutz personenbezogener Daten gesetzlich verpflichtet. Über die Einhaltung des Bundesdatenschutzgesetzes (BDSG) wachen die Bundes- und Aufsichtsbehörden. Zunehmenden Einfluss gewinnen inzwischen die Verbraucherverbände, die nicht zuletzt für wachsende Aufmerksamkeit für die Thematik in den Medien sorgen. Verstöße gegen das BDSG können mit Bußgeldern von bis zu 250.000 Euro und sogar mit Freiheitsstrafen bis zu zwei Jahren (§§ 43, 44 BDSG) geahndet werden.

Den Stein ins bundesdeutsche Rollen brachte das viel zitierte *Volkszählungs-Urteil* von 1983. Anlass war ein Gesetz zur geplanten Totalerfassung der Bundesbürger, das neben den üblichen Stammdaten auch weitere Datenerhebung vorsah. Außer dem Hamburger Senat hielten dieses alle Landesregierungen sowie die Bundesregierung für rechtmäßig. Erst das Bundesverfassungsgericht machte hier mit seinem Urteil vom 15. Dezember 1983 (BVerfGE 65, 1) der Bundesregierung einen kräftigen Strich durch die Rechnung und erklärte das Gesetz kurzerhand für verfassungswidrig, da das Recht auf informationelle Selbstbestimmung der Bundesbürger verletzt würde. So kam es dazu, dass der für 1983 geplante Zensus modifiziert erst 1987 durchgeführt werden konnte. Seitdem ist der Datenschutz in aller Munde, wirtschaftlich wie politisch ein hoch sensibles und fachlich anspruchsvolles Thema, das alle Stellen betrifft, die personenbezogenen Daten nicht zu rein privaten Zwecken automatisiert verarbeiten.

Personenbezogene Daten

Im April 2006 fällte der Bundesgerichtshof ein richtungweisendes Urteil, indem er Kundendaten

IN DIESEM ARTIKEL ERFAHREN SIE…

Was Datenschutz in der Arbeitspraxis meint;

Rahmendaten zum Thema;

Schlüsselfaktoren (nach Bundesdatenschutzgesetz);

Die Bedeutung des betrieblichen DSB;

…dass Datenschutz sogar etwas bringt.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN…

Keine Vorkenntnisse erforderlich.

als Geschäftsgeheimnis einstufte und in einem konkreten Fall eine Freiheitsstrafe von sogar fünf Jahren bestätigte (AZ I ZR 126/03). Auch wenn sich die Urteilsbegründung überwiegend auf das UWG als dem in diesem Fall vorrangigen Gesetz stützt, gewinnt doch der Datenschutz hier enorm an Bedeutung für wirtschaftlich orientierte Unternehmen. Kundendaten werden als personenbezogene Informationen im Sinne des BDSG eingestuft und sind mit angemessenem Aufwand ausreichend vor möglichem Missbrauch zu schützen. Eine Haftung kann insofern nicht nur dem beteiligten Personal zugesprochen werden, sondern auch dem so genannten *Herrn der Daten*, also der vertretungsberechtigten Geschäftsleitung, die in diesem Fall ihre Kundendaten unzureichend vor genau solchen Übergriffen geschützt hat. Zusätzlich hätte im obigen Fall auch die Geschäftsleitung der Stelle, die solche Kundendaten angenommen hätte, mit einer Anzeige rechnen müssen.

Den Kopf weiter in den Sand zu stecken, kann vor diesem Hintergrund gerade das leitende Management künftig teuer zu stehen kommen, zumal der behandelte Fall keineswegs als exotisch betrachtet werden kann. Eine sinnvolle und auf die zum Datenschutz verpflichtete Stelle zugeschnittene Datenschutzorganisation kann dagegen mit sehr überschaubarem Aufwand aufgebaut und integriert werden. Hier wird – inzwischen unter anderem auch durch professionelle IT-Sicherheit-Fachleute – zunehmend zur Inanspruchnahme eines kompetenten und vertrauenswürdigen externen Dienstleisters geraten. Die Vorteile liegen vor allem in der Unabhängigkeit eines *Externen* zum Unternehmen, die durch die größere Objektivität unternehmensorientiertere Lösungen erarbeiten kann und darüber hinaus nicht an der üblichen Betriebsblindheit leidet. So gehen nur selten wichtige Aspekte eines angemessenen Sicherheits- und Datenschutzmanagements unter.

Gesetzliche technisch-organisatorische Anforderungen

Für Daten verarbeitende Unternehmen finden sich in der Anlage 2 zu § 9 BDSG die *acht Gebote* des Datenschutzes. Es sind die folgenden Schlagworte, durch deren Beachtung die technischen und organisatorischen Maßnahmen zu treffen sind, um der Wahrung des Persönlichkeitsrechts im Sinne des Gesetzgebers Rechnung zu tragen:

- Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (*Zutrittskontrolle*).
- Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (*Zugangskontrolle*).
- Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (*Zugriffskontrolle*).
- Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (*Weitergabekontrolle*).
- Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (*Eingabekontrolle*).
- Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (*Auftragskontrolle*).
- Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (*Verfügbarkeits-kontrolle*).
- Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (*Datentrennungsgebot*).

Bei der Umsetzung ist insbesondere die Angemessenheit der Maßnahmen im Bezug auf die Daten verarbeitende Stelle, ihre Arbeitsweise und Geschäftsprozesse sowie die Bedürfnisse, die sich aus der individuell tatsächlich gegebenen Infrastruktur (inkl. Personal) ableiten, zu achten. Aus diesem Grund unterscheidet das BDSG technische (EDV, IT etc.) und organisatorische Aspekte (*Faktor Mensch*).

Datenschutz – Wettbewerbsvorteil und Verkaufsargument

Im Gegensatz zu vielen anderen Qualitätsmerkmalen wie etwa dem Qualitätsmanagement, den ökonomi-

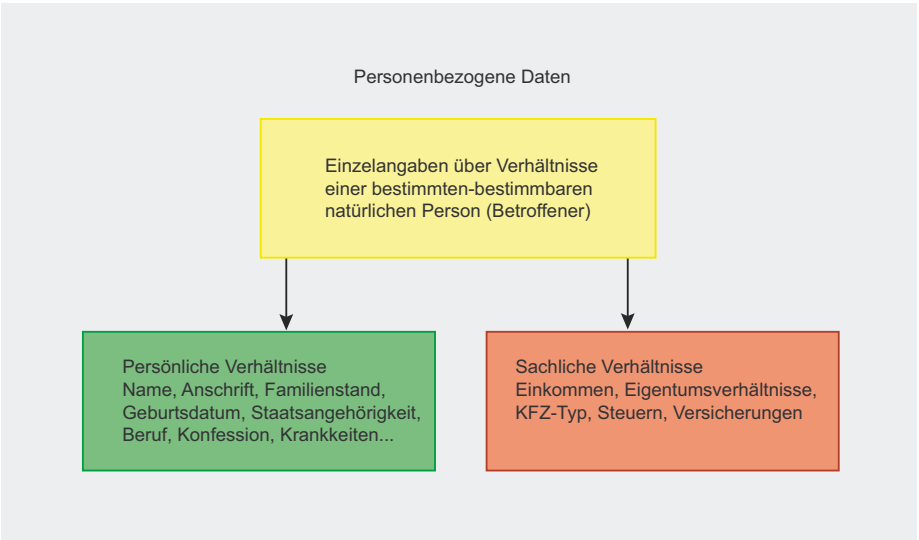

Abbildung 1. *Was sind personenbezogene Daten?*

schen Anforderungen nach z.B. Basel II oder sogar den Börsenansprüchen in Form des Sarbanes-Oxley-Act (SOX) oder der IT Infrastructure Library (ITIL) hat Datenschutz den Vorteil, dass alle Stellen ihm rechtlich verpflichtet sind. In der Praxis bedeutet dies, dass Partner wie Kunden zunehmend nach Datenschutz fragen oder diesen sogar als Basis für eine Geschäftsbeziehung voraussetzen werden, ähnlich wie das im Qualitätsmanagement längst Standard ist. Während Qualitätssicherung im Grundsatz zunächst ein *nice-to-have* darstellt, kann die Unterlassung von Datenschutzmaßnahmen rechtliche Konsequenzen nach sich ziehen. Doch Datenschutz bringt zusätzliche Vorteile, wenn er sinnvoll realisiert wird:

- *Transparenz* – Übersichtliche Geschäftsprozesse, die kommuniziert und gelebt werden, sind entscheidender Qualitätsfaktor für die Vertrauensbasis zu Personal, Kunden und Partnern. Man denke dabei nur an das Beschwerdemanagement von Unternehmen. Viele Beschwerden könnten richtig kanalisiert und zur Zufriedenheit aller Beteiligten zügig und erfolgreich bearbeitet werden, wenn die Fragestellungen an die richtigen Ansprechpartner adressiert würden bzw. werden könnten. Eine klare Unternehmensrichtlinie (z.B. im Datenschutz eine *Privacy Policy*) kombiniert mit einem entsprechenden Link auf der Homepage können objektiv die Personal- und Kundenzufriedenheit erhöhen. Ein durchdacht umgesetztes *Permission Marketing*, als die geregelte Einwilligung des Kunden in die ebenfalls geregelte Nutzung seiner persönlichen Daten, kann durch eine konsequente rechtlich zulässige Formulierung und Anwendung des so genannten *Sternchentextes* (also des *Kleingedruckten*) eine rechtlich und operativ anwendbare Datenbank von Adressen heranwachsen. Auch hier gewinnt gerade die gelebte Transparenz (ganz im Gegenteil zu dem versteckten oder gar verschwiegenen buchstäblich Kleingedruckten!) sehr viel mehr Nutzdaten und reduziert zugleich den Misstrauens- oder Unzufriedenheitsgrad bei Kunden und Interessenten.
- *Prozessoptimierung* – Jeder kennt das Problem. Die Festplatte wächst und wächst, die Ressourcen nebst Performance schwinden. Und warum das Ganze? Man sammelt, speichert, verarbeitet und vervielfältigt Daten – ohne jemals etwas davon wieder zu löschen. Dies ist häufig eine Frage von Unstrukturiertheit und Unsicherheit. Dabei liegt die Lösung auf der Hand: definierte Löschzyklen. Wann, wie, in welchem Umfang und auf welcher gesetzlichen Grundlage? Aus datenschutzrechtlicher Sicht gibt das Gebot der Datensparsamkeit hier nützliche Hilfestellung: Stehen weder unternehmerische Zweckbindung noch vorgeschriebene Aufbewahrungsfristen noch andere gesetzliche Vorschrift (z.B. aus der GoBS, Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme) entgegen, sind Daten zu löschen. Eine weitere Rolle spielt die Wirksamkeit der Löschung. Hier gibt es eine richtige Auswahl:
  - *Richtlinien des BSI zum Geheimschutz von Verschlußsachen beim Einsatz von IT (VSITR)* – Dabei werden die Daten erst negativiert überschrieben und dann beim letzten Vorgang noch mal mit *010101*- überschrieben, um schlussendlich gelöscht zu werden.
  - *Standard 5220.22-M des US-Verteidigungsministeriums* – Die Daten werden erst zweimal überschrieben, beim dritten Mal mit zufälligen Daten überschrieben, um anschließend gelöscht zu werden.
  - *Bruce Schneier-Algorithmus* – Die Schneier-Methode wurde aus einem Kartenspiel mit 54 Karten (52 Farbwerte + 2 Joker) entwickelt. Kurz nach Veröffentlichung wurde jedoch eine gravierende logische Schwachstelle bekannt.
  - *Peter Gutmann-Algorithmus* – Bei der Gutmann-Methode werden die Daten nach einem speziellen Algorithmus 35-mal überschrieben und anschließend gelöscht. Dies gilt als die sicherste, wenn auch zeitaufwendigste Methode, um Daten endgültig zu löschen.

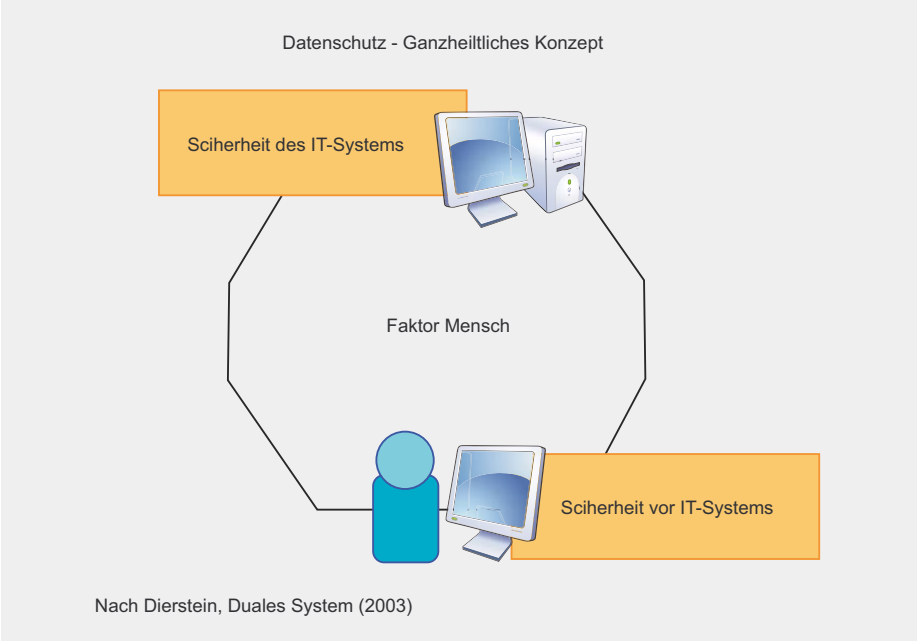

Abbildung 2. *Ganzheitlicher Datenschutz*

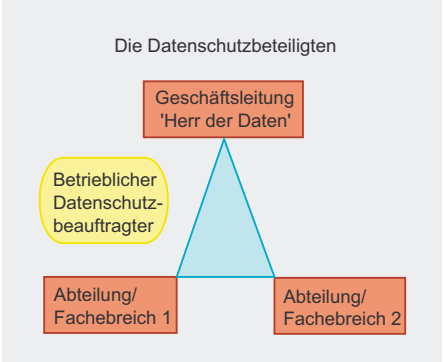

Abbildung 3. *Stabsstelle Datenschutzbeauftragter*

- *DSX-Methode der kanadischen Bundespolizei* – Dabei wird die Festplatte im ersten Durchgang mit dem Bitmuster *00*, im zweiten Durchgang mit dem Bitmuster *11*, danach mit einem Textmuster überschrieben, das aus der Versionsnummer der Software sowie Datum und Uhrzeit der Löschung besteht. Zu beachten ist jedoch, dass das Überschreiben von Festplatten mit der DSX-Methode von der kanadischen Regierung nicht als Methode zum Vernichten vertraulicher, geheimer oder streng geheimer Daten zugelassen ist.
- *Sensibilisierung der Mitarbeiter* – Vertrauliche Daten, Geschäftsgeheimnisse und – im Datenschutz einzig relevant – personenbezogene Informationen können nur durch ein gesundes Verantwortungsbewussts ein des Personalstabs wirksam geschützt werden. Ein solches Verhalten kann der Arbeitgeber nicht voraussetzen, wie neben vielen anderen auch ein Bruce Schneier (Spezialist für Sicherheitsmanagement) ebenso wie ein Kevin Mitnick (ehemaliger, verurteilter Cracker, der heute ebenfalls als Sicherheitsberater tätig ist) in ihren vielfältigen Abhandlungen immer wieder eindrucksvoll berichten. Vielmehr müssen die Beschäftigten quer durch alle Hierarchien und Aufgabenbereiche mit Hilfe gezielter und regelmäßiger Maßnahmen der Sensibilisierung geprägt werden. Wird eine angemessene Datenschutzorganisation nicht gelebt, können Strafen gemäß BDSG und vor allem Imageverlust und die Kosten für die interne Schadensbehebung nicht wirksam verhindert werden.

Der betriebliche Datenschutzbeauftragte

Bei der Umsetzung der gesetzlichen Vorgaben nach BDSG hilft der betriebliche Datenschutzbeauftragte (DSB), seine Aufgaben ergeben sich aus §§ 4f und 4g BDSG. Danach ist jede Stelle, in der Daten automatisiert verarbeitet werden, zur Umsetzung geeigneter Datenschutzmaßnahmen verpflichtet. Sind mehr als neun Personen überwiegend mit der automatisierten Verarbeitung bzw. mehr als 20 Personen mit jeder anderen Verarbeitung oder Nutzung personenbezogener Daten beschäftigt, ist ein DSB von der verantwortlichen Stelle sogar formal (schriftlich) zu bestellen.

Dabei werden hohe fachliche wie persönliche Anforderungen an die Qualität des DSB gestellt, zuletzt definiert durch das so genannte *Ulmer Urteil* von 1991, das neben dem (an sich schon umfangreichen) Fachwissen zusätzlich Kenntnisse in der EDV und IT, der Betriebswirtschaft und dem Sozialwesen verlangt. Darüber hinaus muss der DSB teamfähig sein und zugleich eigenverantwortlich handeln und Leitungsfunktion übernehmen können. Er muss die entsprechenden Inhalte auf allen strukturellen Ebenen kommunizieren können und ausreichend didaktische Fähigkeiten mitbringen, um Sensibilisierungsmaßnahmen nicht nur durchführen sondern auch planen und auf ihre nachhaltige Wirkung hin optimieren können. Analytisches Denken und methodisches Handeln werden vorausgesetzt. Auf Grund dieser vielfältigen Anforderungen sieht der Gesetzgeber vor, dass die Funktion des DSB in Alternative zu einem internen Mitarbeiter auf einen *Externen* übertragen werden kann.

Die Vorteile liegen auf der Hand. Entscheidet man sich für einen Dienstleister, der ein ganzes Datenschutzteam zur Verfügung hat, profitiert man direkt vom Know-how aller Teammitglieder, die Stellvertretung des externen DSB ist in der Regel gesichert und ein Dienstleister kann durch die Konzentration auf Datenschutz als sein Kerngeschäft alle anfallenden Aufgaben wesentlich schneller, effizienter und damit für die Daten verarbeitende Stelle kostengünstiger erledigen. Hinzu kommt der angenehme Nebeneffekt, dass ein externer Berater einen zusätzlichen Blickwinkel, nämlich von außen, einbringt. Weiterbildung und aktuelles Fachwissen können vorausgesetzt werden, und seine Qualität ist zum Beispiel durch Nachweise seiner Fachkunde und entsprechende Referenzen durchaus messbar.

Der DSB ist per legem weisungsfrei in seinem Handeln als Datenschutzbeauftragter und hierin zugleich ohne Weisungsbefugnis, hat also eine Stabstelle inne und übernimmt normalerweise eine rein beratende Rolle, wie die folgende Abbildung zeigt:

Aus diesem Grund ist die Übertragung der Rolle des DSB auf interne Mitarbeiter in bestimmten Positionen oder Funktionen nicht zielführend und daher nicht zulässig – oder zumindest umstritten und somit für einen reibungslosen effektiven Datenschutz nicht zu empfehlen. Hierzu gehören fast immer Beschäftigte aus dem oberen Management, der Personalabteilung, der IT und dem Betriebsrat. Wichtig ist bei der Auswahl eines internen Mitarbeiters als DSB auch der Aspekt, dass Datenschutz immer auch interdisziplinäres Schnittstellenmanagement ist und daher erfordert, dass der DSB sich gut auf die anderen Abteilungen, fremde Fachbereiche, Verhandlungen

Tipp

Je nach Anwender bzw. Schutzbedarf der Daten sollte neben einer Löschung per Software auch eine physische Löschung, etwa in Form einer wirksamen Zerstörung des Datenbestandes durch Magnetisierung oder auch des Datenträgers selbst erwogen werden.

Exkurs

Insbesondere die zurzeit diskutierte Vorratsdatenspeicherung kann schnell zu einem Bumerang werden, wenn man das Thema unterschätzt. Die Bundesregierung plant mit der Novellierung des Telekommunikationsgesetzes, Internetprovider und Telekommunika-tionsnetzbetreiber zu verpflichtet, sämtliche entstandenen Verkehrsdaten ihrer Kunden für eine Dauer von sechs Monaten präventiv vorzuhalten, um den Behörden bei möglicher Strafverfolgung zu unterstützen. Diese aus strafrechtlicher Sicht möglicherweise sinnvolle Änderung stellt für die Unternehmen nicht nur große technische Anfoderungen. Auch neu anzuschaffende Speicher-, Verarbeitungs- und Abrufressourcen sind bereit zu stellen, Geschäftsprozesse sind entsprechend anzupassen und Maßnahmen wie die Veränderung oder Neuschaffung definierter Löschzyklen, Datentrennungswege oder auch wirksame Zugangs- sowie (physische) Zutrittsbeschränkungen müssen realisiert und gelebt werden.

auf allen Ebenen und Krisensituationen einstellen können muss und deeskalativ handeln können muss, soll er nachhaltige Ergebnisse erzielen.

Alleinstellung und Qualitätsmerkmal – ein Ausblick

Im öffentlichen Leben ebenso wie an manchem unbeobachteten Stammtisch ranken sich die Diskussionen um die Einführung des *ePasses II*, die zweite Stufe des biometrischen Reisepasses, der neben einem digitalen Foto nun auch den digitalen Fingerabdruck enthält. An die Übermittlung von Fluggastdaten der Europäischen Union an das US-amerikanische Luftfahrtbundesamt haben sich die meisten schon gewöhnt. Die Ablösung des guten alten Barcodes durch die viel flexibler einsetzbaren und dabei intelligenten Funketiketten (RFID, Radio Frequency Identification) nimmt langsam massentaugliche Formen an. Die spätestens mit dem neuen Geldwäschegesetz lückenlos nachvollziehbaren Wege des Geldverkehrs scheinen niemanden weiter zu interessieren, der Zugriff entsprechend berechtigter Stellen auf die Meldelisten der Geldinstitute wird teilweise sogar geleugnet oder ist selbst den betreffenden Mitarbeitern völlig unbekannt und unvorstellbar. In den Unternehmen geht es um Outsourcing, ITIL und – oft nicht zuletzt – Vorratsdatenspeicherung. Behörden, öffentlicher Dienst und das Gesundheitswesen erörtern die praktischen Möglichkeiten der Zusammenarbeit, insbesondere wenn es um das Zusammenlegen digitaler Datenbanken und Akten geht. Die Einführung einer lebenslangen und 20 Jahre darüber hinaus währenden eindeutig zuordenbaren Steuernummer ist ein erster Schritt hierin. Die trendige *Geschäftsidee*, Gästen ausgewählter Diskotheken in Berlin, auf Mallorca und anderenorts einen Funkchip in den Oberarm zu injizieren, mit dem sie nicht nur jederzeit kontaktlos identifizierbar sind, sondern der zugleich als bargeldloses Zahlungsmittel eingesetzt wird, unterstützt die Entwicklung eines ID-Implantats. Heute bezahlen die Gäste der Diskotheken noch für so einen Chip, der ihnen zusätzlich Einlass in die VIP-Lounge gewährt. Morgen ist das vermutlich Pflicht für alle registrierten Bürgerinnen und Bürger, weil dadurch alles so viel bequemer wird, so viel praktischer erscheint und so viel einfacher für die Organe, denen wir die Entwicklung und Lenkung unserer Gesellschaft anvertrauen.

Wie Georg Orwell schon 1949 in seinem Utopieroman *1984* skizzierte und das Volkszählungsurteil bereits 1983 versuchte, uns allen klar zu machen: Wir alle, vom obersten Vorstandsvorsitzenden bis zum letzten Menschen in der sozialen Kette, sind irgendwo und irgendwann Endverbraucher und Betroffene im Sinne des Bundesdatenschutzgesetzes. Technischer und gesellschaftlicher Fortschritt ist wichtig, doch entscheidend ist bei allem, was der Mensch schafft, dass er seine Menschlichkeit bewahrt. Dies gelingt nur, wenn die unbegrenzten Möglichkeiten, die heute theoretisch aller Welt offen stehen, sinnvoll genutzt werden. Ohne definiertes Maß und Ziel richtet sich jeder Organismus irgendwann zugrunde. Das ist der Lauf der Dinge, der Lauf der Zeit – ein wiederkehrender Zyklus von Aufstieg, Stagnation und Zerfall.

Übersetzt man diese Erkenntnisse, die so alt sind wie die Menschheit selbst, auf den betrieblichen Datenschutz, so entdeckt man, dass dieser so aktuell wie nie ist. Datenschutz in aller Munde, auf der einen Seite die *Datenschützer*, die den Verbraucherschutz stärken und prägen, auf der anderen Seite die *Datenschutzberater*, die sich dem Consulting mit betriebswirtschaftlichen und juristischen Zielen verschrieben haben. Im Schulterschluss erwirken sie gemeinsam einen sinnvollen Umgang mit personenbezogenen Daten und persönlichen Informationen und tragen damit dazu bei, dass unser aller urpersönlichste Würde und Privatsphäre ein geachtetes und geschütztes Gut unserer aufgeklärten fortschrittsorientierten Gesellschaft bleiben.

Wer das erkannt hat, erkennt, dass Datenschutz ein echter Mehrwert für alle Beteiligten ist, ein echtes Qualitätsmerkmal für die verarbeitende Stelle, ein Signal der Wertschätzung an Kunden, Interessenten, Geschäftspartner und Beschäftigte, ein echter Beitrag mit hohem Stellenwert zur Entwicklung unserer Wirtschaft, Forschung und Gesellschaft.

Lesen Sie in der nächsten Ausgabe, welche *Synergieeffekte im Datenschutz* zu finden sind und warum man als Unternehmen darauf nicht verzichten kann.

Datenschutz – Historischer Abriss

- 1970: Hessen erlässt als erstes Bundesland ein Datenschutzgesetz; Kernpunkte sind *Daten und Ergebnisse*, die durch maschinellen und personellen Schutz gesichert werden sollten. Das Jedermannsrecht wurde jedoch schon zementiert.
- 1977: Erstes Bundesdatenschutzgesetz (BDSG).
- 1980: Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data; Die OECD erließ Handelsrichtlinien zur Harmonisierung der europäischen und amerikanischen Entwicklung.
- 1981: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten; Erstes Europäisches Datenschutzabkommen zur Herstellung eines einheitlichen Datenschutzes.
- 1983: Volkszählungsurteil 1983; Erste Etablierung des Rechts auf informationelle Selbstbestimmung.
- 1987: Hessen schafft erstes Datenschutzgesetz.
- 1990: Das novellierte BDSG tritt in Kraft; Neben einer modernen Begriffsdefinition werden datenschutzrechtliche Richtlinien (so z.B. zur Datensparsamkeit) definiert, sachliche und räumliche Anwendungsbereiche benannt und eine Trennung von öffentlichen und nicht-öffentlichen Stellen implementiert.
- 1995: Europäische Datenschutzrichtlinie 95/46/EG; Festsetzung eines Mindeststandards mit der Pflicht zur Übernahme in nationales Recht.
- 2001: Neufassung des BDSG (Gesetz zur Änderung des BDSG); Übernahme der europäischen Richtlinie in nationales Recht.

Kerstin Blossey
Kerstin Blossey ist 1969 in Erlangen geboren und Gründerin von Blossey & Partner (ehemals KSB4 Consulting), einem aufstrebenden Unternehmen, das auf Dienstleistungen rund um deutschen und internationalen Datenschutz für Medien, Wirtschaft und die öffentliche Hand spezialisiert hat.

Oliver Kempkens
Oliver Kempkens ist 1983 in Essen geboren und studiert Jura an der Ludwigs-Maximilians-Universität in München. Neben seinem Studium arbeitet er freiberuflich im Bereich Datenschutzes und Mediation.