Evangelische Akademie Villigst
28.-29. April 2014

Datenschutz effektiver gestalten

I. Allgemeines

Der Datenschutz schützt das Allgemeine Persönlichkeitsrecht der Betroffenen. Soweit dabei Arbeitgebern Pflichten auferlegt werden, wird dabei in deren Eigentumsrechte gemäß Art. 14 Grundgesetz eingegriffen. Auch das Allgemeine Persönlichkeitsrecht wird aus Grundrechten, nämlich Art. 2 Abs. 2 Grundgesetz abgeleitet. Es liegt daher ein Konflikt von Grundrechten vor, der durch einen gerechten Ausgleich seitens des Staates behoben werden muss.

Wenn man von Effektivität spricht muss man klären, was man damit meint.
Nachstehend wird unter Effektivität verstanden zum einen die Tatsache, dass Datenschutz auch tatsächlich umgesetzt wird.
Voraussetzung dafür ist dann weiter, dass der Datenschutz und die einzelnen Regelungen auch akzeptiert werden.

Um dies sicher zu stellen folgende Vorschläge:

II. Vorschläge

1. Betrieblicher Datenschutzbeauftragter

Gemäß § 4 f Bundesdatenschutzgesetz muss jedes Unternehmen, bei dem in der Regel mehr als neun Mitarbeiter mit der Verarbeitung personenbezogener Daten befasst sind, einen Datenschutzbeauftragten zu bestellen. Umgekehrt bedeutet dies, dass kleinere Unternehmen unabhängig davon, welche Arten von Daten sie verarbeiten, dies nicht müssen. Eine Ausnahme gilt insoweit nur für Provider, die wiederum unabhängig von ihrer Größe einen Datenschutzbeauftragten bestellen müssen und für Unternehmen, die ohne dass sie die Daten brauchen, um einen Vertrag mit dem Betroffenen zu erfüllen,

mit besonders sensiblen Daten, zum Beispiel Gesundheitsdaten, Gewerkschaftszugehörigkeit, Weltanschauung, Religion, usw. umgehen.

Dies führt zu einer zum Teil unsinnigen Belastung der Wirtschaft, die auch von der Wirtschaft nicht akzeptiert wird.

Eine Gesenkschmiede zum Beispiel mag 14 Arbeitsplätze haben, an denen personenbezogene Daten verarbeitet werden. Das sind dann aber "nur" Daten wie Name, Vorname, Adresse, Geburtsdatum, Religionszugehörigkeit, Datum des Betriebseintritts, verheiratet, Anzahl der Kinder. Die brauchen dann einen Datenschutzbeauftragten.

Ein Arzt, der hochsensible Gesundheitsdaten verarbeitet, benötigt aber nur dann einen Datenschutzbeauftragten, wenn bei ihm in der Regel mehr als neun Personen mit der elektronischen Verarbeitung solcher Daten betraut sind. Das bedeutet, dass praktisch kein Hausarzt einen Datenschutzbeauftragten benötigt, obwohl der weit sensiblere Daten hat als ein produzierendes Unternehmen.

Die Pflicht zur Bestellung eines Datenschutzbeauftragten daher allein an die Größe zu knüpfen ist sinnlos und stellt eine unzulässige finanzielle Belastung von Unternehmen dar.

Und anders herum:

Es gibt keinen vernünftigen Grund, Rechtsanwälte oder Ärzte von der Verpflichtung zur Bestellung eines Datenschutzbeauftragten zu entbinden, nur weil beim Anwalt oder Arzt in der Regel nicht mehr als neun Personen mit der Verarbeitung personenbezogener Daten befasst sind. Diese Berufsgruppen haben erfahrungsgemäß dermaßen wenig Ahnung von dem notwendigen technischen Schritten zum Schutze von Daten und andererseits so besonders sensible Daten, dass genau diese Personenkreise es dringend nötig haben, dass eine ausgebildete Person zur Seite steht, die bei ihnen dafür sorgt, dass die notwendigen Geheimhaltungsmaßnahmen auch tatsächlich durchgeführt werden.

Es wäre sogar zu überlegen, hier eine "Verantwortliche Person" einzuführen, die persönlich für die Einhaltung des Datenschutzes unterschreibt und damit auch die persönliche Haftung für Datenschutzvorfälle übernimmt. Solche Personen gibt es bereits beim Gesetz über die Elektromagnetische Verträglichkeit (CE-Kennzeichnung) und im Medizinrecht.

Auch die europäische Grundverordnung - Datenschutz in ihrem jetzigen Vorschlagsstadium wäre zu korrigieren. Die spricht zwar zurzeit noch unverbindlich davon, dass bei besonders sensiblen Daten auch ein Datenschutzbeauftragter in Betracht kommt, knüpft ansonsten aber immer noch an die Mitarbeiterzahl und zwar in diesem Fall von 250 Mitarbeitern und mehr an. Ob dabei Mitarbeiter gemeint sind, die mit der elektronischen Datenverarbeitung befasst sind oder überhaupt nur 250 Mitarbeiter, zum Beispiel auch aus der Produktion, lässt sich den Unterlagen nicht entnehmen.

2. Ergänzung des Katalogs der sensiblen Daten

In § 3 Abs. 9 BDSG sind besonders sensible Daten definiert, wie zum Beispiel Gesundheit, Religion, usw. An diese Qualifikation knüpfen sich zum Teil erhöhte Datenschutzpflichten, zum Beispiel die Vorabkontrolle aber auch erhöhte Anforderungen an die technisch-organisatorischen Maßnahmen.

Nach Auffassung des Unterzeichners sollten hier auch Finanzdaten aufgenommen werden, weil die mindestens genauso wie Daten über die Religionszugehörigkeit die Stellung der Person im sozialen Umfeld erheblich gefährden können.

3. Genauere Gesetze

Ein wichtiger Teil des Datenschutzes ist im Datenschutzrecht lediglich mit einem einzigen Paragraphen geregelt. Nur § 32 BDSG regelt nämlich den Arbeitnehmerdatenschutz. Das dann natürlich nur in rudimentärer Weise.
Im Januar 2013 zog die Bundesregierung einen Gesetzentwurf zur Regelung des Arbeitnehmerdatenschutzes (§§ 32-32 l BDSG-E) wieder zurück, weil der Entwurf sowohl von der Arbeitgeberseite also auch von der Arbeitnehmerseite als völlig

inakzeptabel bezeichnet wurde und das, obwohl mit dem Entwurf lediglich die aktuelle Rechtsprechung des Bundesarbeitsgerichtes abgebildet werden sollte. Das führt heute dazu, dass weite Teile des Datenschutzrechts für Arbeitnehmer für einen Datenschützer überhaupt nicht feststellbar sind. Der muss vielmehr die Rechtsprechung des Bundesarbeitsgerichtes laufend überprüfen, um hier wichtige Auskünfte geben zu können. Eine unzumutbare Aufgabe – zumindest für Nichtjuristen.

4. Bessere Gesetze

Manche Datenschutzgesetze sind so unsäglich schlecht formuliert, dass man sie beim besten Willen nicht verstehen kann. Im Anhang zu dieser Ausarbeitung findet sich der Text von § Abs. 28 Abs. 3 BDSG. Der ist auch für Fachleute unverständlich und obendrein auch noch handwerklich falsch, weil eine Verweisung den ebenfalls gemeinten Satz 5 nicht erwähnt.

Die Vorschrift regelt den Umgang von Daten in der Werbung. Wer daher heute in der Werbung tätig ist muss diese Vorschrift beachten. Tut er dies nicht, muss er mit Bußgeldern bis zu 300.000 € rechnen.
Es ist aber dem Bürger nicht zuzumuten, das Risiko von Bußgeldern bis 300.000,00 € einzugehen, weil er ein Gesetz nicht umgesetzt hat, das selbst von Fachleuten unterschiedlich verstanden wird.

Akzeptanz setzt Transparenz und damit Verständlichkeit voraus. Solche Regelungen bewirken das Gegenteil.

5. Mehr Kontrolle

Die typische Antwort eines Unternehmens bei einem Angebot von Datenschutzleistungen lautet, dass man abwarte, bis man erstmals Kontakt mit dem Landesdatenschutzbeauftragten habe. Dann werde man sich wieder melden. Warum solle man heute für etwas Geld ausgeben, was für den Ertrag des Unternehmens überhaupt keine positive Auswirkung hat sondern nur Kosten ausgelöst.

Aus der Sicht des Unternehmens ist das ökonomisch vollkommen richtig.

Rechtlich allerdings ist diese Auffassung falsch. Denn zum einen brauchen manche Unternehmen überhaupt keinen Datenschutzbeauftragten. Zum anderen ist aber umgekehrt ohne hin jedes Unternehmen unabhängig von seiner Größe verpflichtet, ein Verfahrensverzeichnis vorzulegen. Jedes Unternehmen muss sich daher bereits jetzt mit den bei ihm vorhandenen personenbezogenen Daten beschäftigen und ein solches Verfahrensverzeichnis dem Landesdatenschutzbeauftragten zusenden.

6. Auswüchse beseitigen

Akzeptanz setzt auch Augenmaß bei der Anwendung des Datenschutzrechtes durch die entsprechenden Behörden voraus.

So wird bei der Erhebung von Daten durch einen Arbeitsvermittler im Internet zwar auch zugelassen, dass die Eingabe der Daten durch den Arbeitsuchenden als Einwilligung ausreichen soll. Dann wird aber für die Weitergabe dieser Daten an potentielle Arbeitgeber wiederum die schriftliche (!) Zustimmung des Arbeitnehmers verlangt. Das führt einen Medienbruch herbei mit der Folge, dass ein Großteil der Interessenten hier schon gar nicht mehr reagieren wird. Wer im Web seine Daten eingibt, weil er einen neuen Arbeitsplatz sucht und von dem Headhunter dann per Brief eine Aufforderung bekommt, dem noch einmal schriftlich zuzustimmen, hält dieses Unternehmen für steinzeitlich, zumindest aber für überflüssig formell und wird deswegen möglicherweise dieses Unternehmen nicht weiter benutzen. Hinzu kommt die oft schon zu weitgehende Mühe, die schriftliche Einwilligung zurücksenden zu müssen.

Den Gipfel hat Österreich erreicht, wo jeder Ausfuhr von Daten, und zwar nicht nur von Daten natürlicher Personen, vor ihrer Ausfuhr aus dem Land durch eine entsprechende Behörde genehmigt werden muss.

7. Löschen von Daten

Ein besonderes Anliegen ist das Löschen von Daten. Das Augenmerk liegt immer nur auf den Mengen von Daten, die im Augenblick eingehen. Die aber addieren sich über die Zeit zu einem Vielfachen dessen, was man eigentlich als eingehend im Blick hat. Gerade da aber liegen dann auch relevante Informationen. Warum muss also ein

Rechtsanwalt zum Beispiel noch wissen, dass Herr Müller sich vor 18 Jahren von seiner Ehefrauen hat scheiden lassen?

Es gehört daher zu den wichtigen Aufgaben eines Datenschutzbeauftragten, für eine Löschung der Daten zu sorgen.

8. Datenschutz im Internet

Auch hier gewinnt das Recht auf Löschung von Daten besondere Bedeutung. Dies erst recht, weil es da nicht nur um den Zugriff der verantwortlichen Stelle geht sondern die Gefahr einer Weitergabe und daher unkontrollierten Kenntnisnahme durch ganz andere Unternehmen und Behörden besteht.

Die weltweit diskutierten Gefährdungen durch NSA/Facebook/Google können dabei auf nationaler Ebene nicht gelöst werden.

Technisch wäre zu überlegen, hier ein europäisches Netz/eine europäische Cloud einzurichten, um wenigstens den Umgang mit solchen Daten für die Unternehmen handhabbar zu machen.

Das Problem der Nutzung von Google als international dominierende Suchmaschine bleibt dabei natürlich ungelöst. Zumindest wäre aber für einen Schutz der Unternehmensdaten und deren Verarbeitung gesorgt, wenn dies in Europa erfolgen würde.

Auch da müssen wir damit rechnen, dass europäische Geheimdienste davon erfahren. Aber zumindest besteht bei dann auch staatlich streng kontrollierten europäischen Rechenzentren die begründete Hoffnung, dass Unternehmensdaten wenigstens nicht als Geschäftsgeheimnisse weitergegeben werden.

Ansonsten bleibt nur zu hoffen, dass die Landesdatenschutzbeauftragten ihre beschränkten Machtmittel gegenüber diesen Weltkonzernen weiter gezielt einsetzen. Denn auch Bußgelder von nur 300.000,00 € tun solchen Unternehmen weh, weil sie nämlich für jeden Fall der Verletzung verhängt werden können, also auch mehrfach oder

vielfach verhängt werden können. Dann bleibt allerdings immer noch das Problem der Vollstreckbarkeit, wenn nämlich Facebook zum Beispiel keinen einzigen Sitz in Europa hat.

Eine technische Möglichkeit, Datenschutz effektiver zu machen ist die Verschlüsselung, die auch in der Anlage zu § 9 Bundesdatenschutzgesetz neuerdings ausdrücklich angesprochen ist.

IV. Ausblick

Die zu treffenden Maßnahmen müssen im Verhältnis stehen und wie in der Einleitung dargelegt einen Ausgleich schaffen zwischen dem Allgemeinen Persönlichkeitsrecht des Betroffenen und den Eigentumsrechten der Unternehmen.

Dabei ist bei unterschiedlichen Altersschichten auch eine unterschiedliche Einstellung zu den eigenen Daten festzustellen. Jüngere, insbesondere Studierende, geben ihre personenbezogenen Daten trotz der Kenntnis der Gefährdungen durch NSA/Facebook/Google weiter unbefangen in die sozialen Netzwerke ein, legen daher offensichtlich weniger Wert auf den Schutz ihrer Privatsphäre, als dies Ältere tun.

Vor einer Definition dessen, was getan werden muss, muss daher eine Analyse stehen, wo denn die für den Betroffenen subjektiv definierte Grenze verläuft, ab der für den Betroffenen die Nutzung seiner Daten nicht mehr akzeptabel wird.

Dabei muss diese Selbsteinschätzung des Betroffenen aber nicht die abschließende und verbindliche Grenze sein. Schließlich ist der Staat auch dafür da, Wertungen zu treffen und durchzusetzen, die dem Einzelnen vielleicht im ersten Moment nicht einsichtig sind. Gleichwohl ist natürlich die Auffassung des Betroffenen selbst ein wesentliches Indiz für die Abwägung der Grundrechte.

Unabhängig davon, dass der Staat möglicherweise weitere Gesetze formuliert, kommt es aber trotzdem auf das Verhalten des Betroffenen an. Denn wenn der trotz entsprechender verhältnismäßiger Gesetze an NSA/Facebook/Google weiter personenbezogene Daten eingibt, muss er weiter damit rechnen, dass Missbrauch

betrieben wird. Also besteht der erste Schritt einer Verbesserung des Datenschutzes darin, einen der wichtigsten Grundsätze des Datenschutzes nicht nur bei der verantwortlichen Stelle sondern bei dem Betroffenen selbst zu berücksichtigen, nämlich die Datensparsamkeit. Der beste Datenschutz ist immer noch derjenige, der darauf verzichtet, personenbezogenen Daten überhaupt bekannt zu machen.

Gerade, weil zwar Deutschland und die Europäische Union einen hohen gesetzlichen Datenschutzstandard haben, aber fast alle anderen Staaten der Welt sich um den Datenschutz wenig oder gar nicht kümmern, bleibt der Einzelne aufgerufen, selbst für den Schutz seiner Daten zu sorgen.

Rechtsanwalt Göbel, im April 2014

§ 28 BDSG

…

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen-oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Abs. 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen-oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Abs. 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hin zu speichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1,2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4a Abs. 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass sie Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.