KERSTIN BLOSSEY
(BLOSSEY & PARTNER)

Datenschutzpraxis: Transparenz für mehr Privatsphäre (Teil 1)

Schwierigkeitsgrad:

Von Betroffenen, Informationen, Kennzeichnungs- und Benachrichtigungspflichten, Auskünften, Widersprüchen und dem Jedermannsrecht. Inkognito unterwegs im Geschäftsleben?

IN DIESEM ARTIKEL ERFAHREN SIE...

Grundlagen zur Informationspflicht nach Datenschutzgesetz;

die korrekte Gestaltung einer Einwilligung in die Datennutzung durch Betroffene;

welche praktischen Aspekte zu berücksichtigen sind.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN...

keine spezifischen Vorkenntnisse erforderlich, die Grundbegriffe des Datenschutzes aus den Artikeln der vorherigen Ausgaben sollten geläufig sein. Alternativ kann auf das Glossar von Blossey & Partner (http://blossey-partner.de/showpage.php?SiteID=11&lang=1) zurückgegriffen werden.

Das war einmal. Während viele Stellen ungehindert (und vielfach sehr wohl bemerkt) ihrer Sammelwut frönen, sollen Vorschriften den Verbraucher stärken. So auch der Themenbereich *Auskunft* im unternehmerischen bzw. behördlichen Datenschutz. *Transparenz* sagt das Gebot der Stunde, wenn man den vielen Schlagzeilen zu angeprangertem Datenmissbrauch glauben darf. *Qualitätsmerkmal* sagt der unternehmensbewusste Datenschutzbeauftragte – und macht Geschäftsführern wie Vorständen klar, dass mehr Transparenz durch bewusst gelebten Datenschutz als nicht zu verachtender Wettbewerbsvorteil auf der *Haben*-Seite verbucht werden kann.

Woher sollen wir wissen, dass wir Datenschutz brauchen?

Als Jungunternehmer schlägt man sich besonders anfangs nicht nur mit der Konzeption fürs Geschäft, dem Businessplan, Finanzierungshilfen und der goldrichtigen Geschäftsidee herum, sondern auch mit der Anmeldung bei allen erforderlichen Stellen und der Flut an Vorgaben, die man als Firmengründer und Betreiber nun einmal einzuhalten hat. Wie man von all diesen wichtigen und sinnvollen Regelungen erfährt?

Das weiß niemand so recht zu beantworten. Man hat Glück, wenn man jemanden kennt, der wieder jemanden kennt, der von der einen oder anderen Sache schon einmal gehört hat. Mundpropaganda scheint das Gebot der Stunde, doch sicher sein, dass man keine Vorschrift vergessen hat, gegen die man unwissentlich verstoßen könnte, kann man nicht. Transparenz und eine auffindbare offizielle Anlaufstelle, die zudem kompetente und verbindliche Informationen bereitstellt, das wäre doch schon einmal ein guter Anfang, um Licht ins Dunkel zu bringen.

Woher sollen wir wissen, was der Datenschutz vom Unternehmen fordert?

Im Datenschutz fungiert der betriebliche Datenschutzbeauftragte (DSB) als eine solche kompetente und ansprechbare Informationsschnittstelle im Unternehmen bzw. jeder anderen Personendaten verarbeitenden Stelle. Neben allen anderen Aufgaben soll der DSB für ein gesundes Maß an Transparenz sorgen, sowohl innerhalb der Unternehmensstruktur als auch nach außen. Doch Transparenz, als ein definiertes Maß an Durchblick im weitesten Sinn, ist eine

Anmerkung in eigener Sache:

Dieser Artikel gibt keinen vollständigen Überblick über alle Einzelaspekte, die in der Praxis relevant sein können, sondern greift aufgrund der komplexen Thematik häufige Alltagsfragen auf. Die Inhalte sind außerdem nicht juristisch sondern ganzheitlich-interdisziplinär betrachtet und dargestellt.

bidirektionale Angelegenheit. In einem System wie unserer Wirtschaft bedeutet Kommunikation immer mindestens 1 + n Stellen, die in irgendeiner Form Informationen oder Daten austauschen. Wo das Gleichgewicht der erhaltenen Daten nicht einigermaßen ausgeglichen ist, spricht man in der Regel von einem Informationsdefizit, dem Politik, Wirtschaft und Gesetzgebung so gut wie möglich begegnen wollen, da Wissen auch jenseits des Informationszeitalters immer noch Macht bedeutet. Macht aus Datenschutzsicht bedeuten Spam-Attacken, Wirtschaftsspionage, von Arbeitgeber zu Arbeitgeber weitergereichte Kundendatenbanken, Abhörprotokolle, Kundendaten im Internet zur freien Verfügung sowie der unzureichend verantwortungsbewusste Umgang mit den anvertrauten Personendaten.

Information gibt darüber hinaus jedem, der sie erhält, die Möglichkeit, ein Stück weiter zu sehen als jemand, der dieselbe Information nicht zur Verfügung hat. Im Alltag kann das bedeuten, dass Sie kein Impressum auf Ihrer Unternehmens-Website haben – genau wie Ihr Nachbar, der ein anderes Geschäfts in derselben Straße in der Innenstadt betreibt. Während Ihnen eine Abmahnung oder ein saftiges Bußgeld zur Zahlungsaufforderung ins Haus flattert, bleibt Ihr Nachbar ahnungslos – und verschont. Warum? *Dummheit schützt vor Strafe nicht*, sagt der Volksmund, und der Gesetzgeber sieht das genauso, wenn er sich auch etwas gewählter ausdrückt. Sie haben also Pech, Ihr Nachbar Glück. Zufall. Oder ein Informationsdefizit.

Doch genug vom philosophischen Hintergrund. Im Folgenden bringen wir eine gehörige Portion Licht in die Reihe von Aufgaben unternehmerischer Informationspolitik, soweit diese zu den Aufgabengebieten des DSB gehören.

Wozu Transparenz für diejenigen, die uns ihre Daten geben?

Der Datenschutz sagt: *Jeder Mensch hat das Recht, selbst zu bestimmen, wer wann welche Informationen über seine Person und seine Verhältnisse in welchem Umfang und zu welchem Zweck erhält und verwenden darf* (grobe Erläuterung des so genannten

Absicht	Der Betroffene, der seine Einwilligung geben soll, ist zuvor über alle Aspekte der Verwendung seiner Daten klar und vollständig informieren worden, so dass er in der Lage ist zu überblicken, was mit seinen persönlichen Daten gemacht werden wird bei der verarbeitenden Stelle. Im Umkehrschluss muss möglichst weitgehend ausgeschlossen werden, dass der Betroffene seine Einwilligung unabsichtlich, aus Versehen, unbewusst oder auf Grund falscher bzw. unvollständiger Informationen über die Verwendung seiner Daten erteilt. Hierzu gehört auch der folgende BDSG-Grundsatz: *Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben* (§ 4a I Satz 4 BDSG). In der Praxis bedeutet dies, dass ein entsprechender Absatz auf einem Bestell-, Anmelde- oder Kontaktformular vom Rest abgehoben und in direkter unmittelbarer Nähe der zu leistenden Unterschrift platziert werden muss. Das beliebte Jonglieren mit Schriftgrößen bis hin zum Lupenzwang widerspräche dieser Vorschrift. Es versteht sich normalerweise von selbst, dass eine solche Einwilligung vor der beabsichtigten Verarbeitung erfolgen sollte.
Freiwilligkeit	Eine Einwilligung ist nach § 4a BDSG nur dann wirksam, *wenn sie auf der freien Entscheidung des Betroffenen beruht*. So einfach der Satz klingen mag, beschäftigt er die Rechtsprechung doch enorm – und hält damit auch die betrieblichen DSBs ordentlich in Atem, denn kompetente Handlungsempfehlungen sollte auch die aktuelle Rechtsprechung berücksichtigen, um praktikable Lösungen anbieten zu können. Oft wird *freiwillig* pseudonym mit *ohne Zwang* beschrieben, doch erscheint dem Einzelnen Arbeitnehmer oder Verbraucher diese Anforderung aus dem Datenschutz als kaum realisierbar. Gängige Kommentare zum BDSG, wie z. B. Gola/Schomerus, sprechen gar vom Element der *wirtschaftlichen Machtposition*, die eher an Erpressung denn an Freiwilligkeit erinnern mag. Hier hat das Bundesverfassungsgericht deshalb den Aspekt der Verhältnismäßigkeit eingeführt, der sicherlich auch der *Angemessenheit* nach BDSG Rechnung tragen kann. Beispielsweise steht die Veröffentlichung von Mitarbeiterfotos der gesamten Belegschaft in einem Softwarekonzern sicherlich in keinem begründbaren Verhältnis zu den Interessen des Einzelnen, seine Privatsphäre am Arbeitsplatz erhalten zu sehen. Eine solche Veröffentlichung benötigt daher nicht nur die schriftliche Einwilligung jedes betroffenen Mitarbeiters, sondern darüber hinaus die Möglichkeit, diese Einwilligung nicht zu erteilen, weil die Fotoveröffentlichung nicht verhältnismäßig zum Erfolg des Unternehmens beitragen wird.
Nachweisbarkeit	*Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist*, lautet § 4a I Satz 3 und weist damit den Weg in Richtung der Nachweisbarkeit einer freiwillig erbrachten Einwilligung. Wird der erforderlichen Form nicht genüge getan, riskiert die Personendaten verarbeitende Stelle schlimmsten Falls die Zulässigkeit der Datenverwendung und nimmt damit die üblichen Konsequenzen in Kauf: sofortiges Einstellen der Verarbeitung, Bußgelder, Haftstrafen, Schadensersatz, Imageschädigung, Vertrauensverlust, Folgekosten und Aufwand für die Behebung des *Schadens* – und natürlich alle aus diesen Folgen entstehenden Kettenreaktionen für das Unternehmen.
Widerrufbarkeit	Ist eine Einwilligung in die Verwendung persönlicher Daten freiwillig, so erzwingt das beinahe schon die Möglichkeit, diese jederzeit ohne Angabe von Gründen widerrufen zu können. Über dieses Recht – und die damit eventuell zu erwartenden Konsequenzen, z. B. den Verlust eines Profils in einem Online-Forum bei der Löschung der Profildaten – ist der Betroffene bereits vor Erteilung seiner Einwilligung zu informieren.

allgemeinen Persönlichkeitsrechts, das bereits Gegenstand vieler hoch wissenschaftlichen Abhandlungen ist und daher an dieser Stelle nicht weiter ausgelegt werden soll). Damit jeder Mensch dieses Recht auch wahrnehmen kann, muss er eine Reihe von Hilfestellungen bekommen, und zwar immer an den Punkten in seinem Lebensalltag, wo er sich selbst die Zähne ausbeißen würde, ohne etwas zu erreichen.

Aus diesem Grund gibt es unter anderem Regelungen wie das Informati onsfreiheitsgesetz (IFG), das in manchen Bundesländern bereits institutionalisiert und teilweise sogar beim Landesdatenschutzbeauftragten platziert ist, den Verbraucherschutz, die Öffentlichkeit in Form der Presse, Interessenvertretungen und viele weitere Möglichkeiten, sich Hilfestellungen zu holen. Auch dies wollen wir hier nicht weiter vertiefen, da es uns um den betrieblichen Datenschutz, nicht um Verbraucher-Datenschutz gehen soll.

Was genau haben wir im Datenschutz im Sinne der Transparenz zu tun?

Welche Verpflichtungen zur transparenten Informationspolitik hat eine unternehmerische Einrichtung konkret? Wozu sind Arbeitgeber verpflichtet? Und wie kann die Umsetzung aussehen? Im Folgenden sehen wir uns hierzu fünf Kernbereiche aus dem Datenschutz genauer an.

Einwilligung einholen

Nach § 4 BDSG ist eine Verwendung personenbezogener Daten nur zulässig, *soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat*. Der Königsweg zur datenschutzkonformen Verarbeitung personenbezogener Daten ist für Wirtschaftsunternehmen erfahrungsgemäß eine vorliegende formgerechte Einwilligung durch den Betroffenen in die Nutzung seiner persönlichen Daten und muss daher eingeholt werden – auch, wenn das auf den ersten Blick mühsam, zeitaufwändig, teuer oder sinnlos erscheinen mag.

Die gesetzliche Grundlage ist hier eindeutig, und im Umkehrschluss können Sie getrost davon ausgehen, dass jegliche Verwendung personenbezogener Daten, für die Ihnen keine Zulässigkeit nach BDSG vorliegt, gegen geltendes deutsches (und internationales) Recht verstößt. Das bedeutet, dass diverse Verfahren, die nicht direkt mit Personendaten arbeiten, jedoch auf solchen aufbauen, ebenfalls unzulässig sein können und Sie damit Strafen, Imageschäden und Vertrauensverlust bei Ihren Kunden, Interessenten und Verbrauchern.

Die Aspekte zum oben genannten Stichwort *formgerecht* beschreibt § 4a BDSG. Diese können zusammengefasst werden in folgende Begriffe: Absicht, Freiwilligkeit, Nachweisbarkeit und Widerrufbarkeit (Tabelle 1).

Unter bestimmten Voraussetzungen sieht das BDSG von einer Einwilligung ab, zum Beispiel bei der Sicherstellung gesetzlicher oder staatlicher Interessen, die jenen des Einzelnen im Staat überwiegen (z. B. Strafverfolgung). Auf die Einzelfälle soll hier nicht weiter eingegangen werden, da dies den Rahmen der Abhandlung sprengen würde. Die Einwilligung ist die am häufigsten zutreffende Form für Wirtschaftsunternehmen aller Art. Der Vollständigkeit halber sei erwähnt, dass es Sonderfälle zur Einwilligung in die Datenverarbeitung gibt, zum Beispiel durch vorrangig geltende Gesetze wie unter anderem im Online-Bereich mit dem Telemediengesetz (TMG). Bei der Bereitstellung von Telemedien gilt beispielsweise vorrangig § 12 TMG. Hier ist der betriebliche DSB gefordert, solche Sonderfälle zu erkennen und entsprechend im individuellen Unternehmen zu behandeln.

Benachrichtigung

Nach § 33 BDSG hat jeder Betroffene Anspruch auf eine Benachrichtigung, wenn seine personenbezogenen Daten erstmalig erhoben bzw. verarbeitet werden, ohne dass er davon Kenntnis erlangen würde.

Diese soll vom Timing her mit oder unverzüglich nach der ersten Speicherung erfolgen.

Für diese Benachrichtigungspflicht gibt es eine Reihe von Ausnahmen, die dem geschäftlichen Alltag ebenso Rechnung tragen sollen wie der Privatsphäre des Personals und dem Kunden- bzw. Interessentenkreis.

So ist eine solche beispielsweise nicht erforderlich, wenn der Betroffene auf andere Weise von der Verarbeitung Kenntnis erlangt haben kann.

Das klassische Beispiel aus der Praxis ist hierfür die Veranstaltung von Gewinnspielen aller Art, die zur Gewinnung personenbezogener Adressdaten durchgeführt werden. In diesen Fällen ist eine Benachrichtigung erforderlich, andernfalls wäre eine Nutzung der gewonnenen Daten unzulässig.

Ein gegenläufiges Beispiel wäre die Verarbeitung von Personaldaten durch den Arbeitgeber.

Hier kann das Unternehmen durchaus davon ausgehen, dass der Mitarbeiter sich denken kann, dass seine persönlichen Daten im Rahmen der für die Erfüllung des (Arbeits-)Vertragsverhältnisses erforderlichen Informationen verarbeitet und gespeichert werden, so dass eine ausdrückliche Benachrichtigung nicht erforderlich ist.

Formalismen wie bei der Einwilligung gibt es für die Benachrichtigung nicht, so

Datenschutz-Stilblüte: Das arme Hascherle…

…ist – im Gegensatz zur Überzeugung vieler unserer Datenschutz-Seminarteilnehmer – kein jugendlicher Drogenabhängiger, sondern die Übersetzung des Rechtsbegriffs *Betroffener* in den fränkischen Dialekt.

Er steht für diejenige natürliche Person, deren persönliche Daten verwendet werden und die arm aus Sicht des Gesetzestextes offensichtlich *arm dran sind* – schließlich werden sie allein durch den Umstand, dass ihre Daten verarbeitet werden, automatisch zum *Betroffenen* statt beispielsweise neutraler ausgedrückt zum *Beteiligten*.

Ausblick aufs nächste Heft:

Eine ganze Reihe von Pflichten und Rechten rund um das Datenschutzgesetz führen zu diversen Kennzeichnungs- und Informationsbedürfnissen. Wir beschäftigen uns im nächsten Heft mit Teil 2 des in diesem Heft begonnenen Artikels.

Wochenrückblick zu den Datenschutz-Schlagzeilen in der Online-Presse:

Das Redaktionsteam von Blossey & Partner stellt jede Woche neu die Schwerpunktthemen rund um Datenschutz für Sie zusammen unter *http://www.blossey-partner.de* (*News*, unten rechts). Gucken Sie doch mal rein, das Archiv reicht inzwischen bis 2005 zurück und bietet sogar eine einfache Suchfunktion. Viel Spaß beim Stöbern.

ist etwa keine Schriftform vorgeschrieben. Bedenkenswert ist bei dieser vermeintlichen Freiheit für den Unternehmer jedoch durchaus die Nachweisbarkeit seiner Erfüllung der Datenschutzanforderung, weshalb sich eine formale Vorgehensweise im *Ernstfall* sicher vielfach empfiehlt, wenn sie wirtschaftlich und organisatorisch angemessen ist.

Eine Benachrichtigung ist übrigens auch dann erforderlich, wenn der Betroffene einer weiteren Nutzung seiner persönlichen Daten widersprochen hat und er in einer Liste (z. B. einer entsprechend sparsam ausgeführten Sperrdatei), aufgeführt wird, die verhindern soll, dass etwa bei der erforderlichen Rückspielung eines Backups die Kennzeichnung der Sperrung oder gar der komplett gelöschte Datensatz plötzlich wieder verfügbar ist und wieder zur werblichen Ansprache genutzt wird. Natürlich kann der Betroffene auch dem Eintrag in dieser Liste widersprechen, womit das Unternehmen dann aber die ordnungsgemäße Unterlassung der weiteren Nutzung seines Datensatzes nicht mehr sicherstellen und der Betroffene diese nicht mehr ohne weiteres voraussetzen kann.

Wissenswert ist generell auch der Umfang der Informationspflicht, die sich durch alle Einzelregelungen des BDSG wie ein roter Faden zieht: Der Betroffene ist jeweils sowohl über die Art der Daten, die Erhebung, Verarbeitung oder Nutzung, die Zweckbestimmung sowie über die Identität der verantwortlichen Stelle zu informieren.

Die beiden eben behandelten Aspekte sind nur zwei von mehreren grundlegenden zur Informationspolitik nach Datenschutzgesetz. Lesen Sie in der nächsten Ausgabe die Fortsetzung, wo es dann schwerpunktmäßig um das Auskunftsrecht des Betroffenen, das so genannte Jedermannsrecht sowie um das Verfahrensregister gehen wird, das jede personenbezogene Daten verarbeitende Stelle haben muss.

Fazit: Informationspolitik als nutzbringender Mehrwert

Die meisten Gründe, die zu einer Verarbeitung personenbezogener Daten im Unternehmen führen, sind berechtigt, wie die langjährige Praxiserfahrung in unterschiedlichen Branchen und Firmengrößen gezeigt hat.

Jedoch sind diese Gründe und das jeweilige Verfahren sowie seine Durchführung und die beteiligten organisatorischen wie technischen Schnittstellen durch den DSB sorgfältig zu prüfen. In den meisten Fällen ist die Einwilligung ein sehr praktischer Weg, um mit wenig organisatorischem Aufwand ein hohes Maß an Zulässigkeit zu erreichen – und somit drohende Risiken zu vermeiden.

Es lohnt sich also durchaus für jedes Unternehmen, seine Politik bezüglich der Gewinnung und Behandlung von personenbezogenen Daten zu überdenken, entsprechende Einwilligungsmechanismen und Datenschutzhinweise zu etablieren und zu implementieren.

Kerstin Blossey

Kerstin Blossey ist Dipl. Informations-Wirtin (FH) und Gründerin von Blossey & Partner, einer aufstrebenden Unternehmensberatung, das sich auf den betrieblichen/behördlichen Datenschutz spezialisiert hat. Zum stetig wachsenden Kundenkreis, der von einem derzeit fünfköpfigen Team betreut wird, zählen deutsche ebenso wie international angesiedelte mittelständische Unternehmen, Konzerne und Einrichtungen aus so unterschiedlichen Branchen wie Medien, Softwareindustrie, Automotive, Wirtschaft, Gesundheitswesen, Tourismus und der öffentlichen Hand. Die Autorin selbst betreute als externe Datenschutzbeauftragte unter anderem BEA Systems bis zu deren Übernahme durch Oracle im August 2008.