KERSTIN BLOSSEY UND
OLIVER KEMPKENS

Chance statt Blockade

Schwierigkeitsgrad:

Dieser Artikel stellt den Unterschied zwischen politischem und unternehmerischem Datenschutz dar. Er zeigt, welche kooperativ--produktiven Ansätze eine durchdachte Datenschutzorganisation im betrieblichen Alltag mitbringt, wenn sie professionell angepackt wird...

Professioneller Datenschutz zeichnet sich durch eindeutige Merkmale aus: Er ist gesetzeskonform und zugleich ökonomisch orientiert, ohne dabei das technische Umfeld und die Unternehmensentwicklung zu vernachlässigen. Datenschutz schafft Balance zwischen den Bedürfnissen des Endverbrauchers – als dem Grundrechtsträger – und den Anforderungen der Unternehmen. Es geht nicht um *Gewinner* und *Verlierer*, wenn der Personendatenbestand in einem Unternehmen, einem Verband, der öffentlichen Hand und anderen zum Datenschutz verpflichteten Stellen gemäß den rechtlichen Vorgaben datenschutzkonform verarbeitet wird. Ganz im Gegenteil.

Voraussetzungen schaffen

Wo immer es einem betrieblichen Datenschutzbeauftragten (DSB) gelingt, diese Erkenntnis zu leben und dadurch für die Belegschaft erfahrbar zu machen, erkennen Fachabteilungen und Aufgabenbereiche eines Unternehmens schnell, dass sie im Team mit einem kommunikativen DSB und mit Hilfe eines durchdachten Datenschutzkonzeptes viele Probleme von vorne herein vermeiden, ihr juristisches Haftungsrisiko reduzieren und darüber hinaus ihr Handlungsspektrum wirkungsvoll erweitern können. Ein paar Beispiele aus der Praxis werden das im Weiteren unter Beweis stellen.

Der intern oder extern bestellte DSB muss weitreichende Fachkenntnis in den verschiedensten Bereichen mitbringen und zugleich mit ihnen in der Praxis umgehen können. Das meint in concreto, der vielseitige Spezialist ist gefragt. Erstmals hat das Ulmer Landgericht mit seinem Urteil aus dem Jahr 1990 (Az.: 5T 153/90-01 LG Ulm, Link: *http://www.udis.de/ulmermodell.htm*) dafür gesorgt, dass der Beruf des DSB überhaupt als solcher wahrgenommen wurde – zumindest im juristischen Bereich. Welche Qualifikation ein professioneller DSB mitbringen muss, konkretisiert derzeit der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. in der Schaffung eines Berufsbildes. Nach über einem Jahr sorgfältiger Recherchen, Erhebungen und Überarbeitungen verfügen DSBs nun über ein praxistaugliches Konzept, das den Datenschutz--Beauftragten als Beruf etablieren wird – ist er das doch längst im unternehmerischen Alltag, wenn auch oft in einer Art schwebendem Zustand ohne die Sicherheit eines definierten Berufsbildes im Rücken. Zur Fachkunde legte das Ulmer Urteil folgende Anforderungen (*Ulmer Modell*) fest:

- Computerexperte;
- Anwendung der Vorschriften der Datenschutzgesetze des Bundes und der Länder und alle anderen den Datenschutz betreffenden Rechtsvorschriften;
- Kenntnisse der betrieblichen Organisation;
- Didaktische Fähigkeiten;
- Psychologisches Einfühlungsvermögen und Führungsqualitäten;
- Organisationstalent und Fähigkeiten in der Methodik;

IN DIESEM ARTIKEL ERFAHREN SIE…

Wie der Unterschied zwischen politischem und unternehmerischem Datenschutz ist.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN…

Voraussetzung für das Verständnis dieses Artikels sind nur Bekanntheit diverser gängiger Begriffe aus der IuK--Umgebung.

- Angemessener Umgang in Konflikten um seine Person, seine Funktion und seine Aufgabe.

Ungesundes Halbwissen kann mittel- und langfristig zu einem porösen Organisations- und Schutz-Fundament führen, welches nicht nur unnötigen rechtlichen Ärger, wie gerichtliche Verfahren und Bußgelder bis zu einer Höhe von EUR 250.000,00 (§ 43 Abs. 3 Bundesdatenschutzgesetzes [BDSG]) bzw. Freiheitsstrafen von bis zu zwei Jahren (§ 44 Abs. 1 BDSG) nach sich ziehen kann. Sondern immer häufiger führen Lücken im Datenschutz- und Datensicherheitskonzept zu öffentlichkeitswirksamen *Pannen*, die unweigerlich und unbestreitbar zu spürbaren Imageeinbußen führen. Dies gilt insbesondere für international tätige Stellen.

Man denke dabei zum Beispiel an die Einwilligungsproblematik im so genannten *Permission Marketing*. §§ 3 Abs. 1, 4a BDSG definieren einen eindeutigen Rahmen, unter welchen Umständen das Unternehmen die personenbezogenen Daten eines Kunden erheben darf. Der Königsweg lautet: hole dir eine Einwilligung des *Betroffenen*, also der Person, deren Daten du verarbeiten möchtest. Dieser Rahmen wird durch weitere Vorschriften, zum Beispiel aus dem Kaufrecht (Bürgerliches Gesetzbuch [BGB]/*Darf die datenschutzrechtliche Einwilligungsklausel in die Allgemeinen Geschäftsbedingungen eingebaut werden?*), dem Wettbewerbsrecht (Gesetz gegen den unlauteren Wettbewerb [UWG]/*In was darf alles eingewilligt werden?*) und natürlich klassischem Datenschutzrecht (BDSG/ *'Opt-in oder Opt-out', oder sogar ‚Double-Opt-in'?*) ergänzt. Wobei die in Klammern genannten Merkmale für eine online-Einwilligung per einfachem Klick als Aktion auf einer Webseite oder per definierter Rückantwort von einer vorher vereinbarten Email-Adresse stehen. Letztere Möglichkeit verhindert mit einfachen Mitteln Aktionen für einen nichtsahnenden Dritten, der dadurch zu Schaden kommen könnte.

Des Weiteren denke man an die Ressourcenverschwendung, die durch unsystematische und undurchdachte Speicherungen von Datensätzen betrieben wird. Diese kann dergestalt ausarten, dass das hochqualifizierte Personal Daten mit unverhältnismäßigem Zeitaufwand und in keiner sinnvollen Relation zum Sucherfolg durchforsten muss. Der operative Geschäftsbereich steht in der Zwischenzeit still, und die Geschäftsführung muss Wartezeiten in Kauf nehmen, bis die erforderlichen Dokumente gefunden werden, bis ihr die Informationen vorgelegt werden können, die sie benötigt, bis gutbezahltes Fachpersonal sich wieder seiner fachlichen Tätigkeit widmen kann. Jedoch auch die technischen Ressourcen werden vergeudet. Fehlende Löschzyklen für Altdaten, für die keine Aufbewahrungsfristen mehr gelten, können die Notwendigkeit einer Erweiterung im Performance-Sektor bedeuten, gegebenenfalls bis hin zum Outsourcing der IT aus Kostengründen – was sich wirtschaftlich in den meisten Fällen als weniger optimale Lösung herausstellt. Darüber hinaus darf die Datenpflege nicht vergessen werden, und selbstverständlich die Verselbstständigung von Backups. Dort sollte der Datenschutzbeauftragte integrativ dem IT-Sicherheitsbeauftragten zur Seite stehen und mit ihm gemeinsam sinnvolle Löschzyklen entwerfen und realisieren.

Nach nur zwei Beispielen aus dem unternehmerischen Alltag können wir festhalten, dass sich der Datenschutz in jedem Fall auf vier Kernbereiche erstrecken und zugleich konzentrieren muss: betriebswirtschaftliche, sozioökonomische, juristische und gelegentlich gern verleugnet, jedoch in der Praxis mindestens genauso wichtig technische. Im Umkehrschluss heißt das, dass der betriebliche DSB sich nicht auf einen der genannten Bereiche fixieren darf, den er bevorzugt. Er muss sich vielmehr entsprechende Zusatzkenntnisse aneignen, um die Aspekte, die ihm ferner liegen, ebenso professionell abwickeln zu können. Tut er dies nicht, muss von einer Gefährdung des Schutzfundaments ausgegangen werden. Die Frage nach der Belegung der Fachkunde sollte ein DSB daher in jedem Fall eindeutig und mit aktuellen Maßnahmen belegen können – in allen vier Disziplinen.

Eine weitere Rahmenbedingung ist die interdisziplinäre Teamarbeit im Unternehmen. Datenschutz wird erfahrungsgemäß nur dann das entscheidende Plus an unternehmerischer und Rechts-Sicherheit bringen, wenn Geschäftsführung (als Ausrichter des operativen Geschäfts), IT-Verantwortliche (als technischer Pol), Betriebsrat (als Personalpol), und der betriebliche Datenschutzbeauftragte (als kompetente Kommunikationsschnittstelle) an einem gemeinsamen Strang – und natürlich möglichst in dieselbe Richtung! – ziehen. In Zeiten hoch qualifizierter Fachkräfte, die sich zudem durch ein hohes Maß an Führungs- und Teamfähigkeiten im Gesamtbetrieb auszeichnen, kann ein so interdisziplinär aufgestelltes Team alltagstauglich umsetzen, was der Gesetzgeber in den EU-Richtlinien 95/46/EG (*EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* vom 24.10.1995) und 2002/58/EC (*EU-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation* vom 12.06.2002) und entsprechender nationaler Umsetzung, in Deutschland in Form des BDSG, in Handlungsprinzipien gefasst hat. Darüber hinaus kann ein solches Team ungeahnte Synergien freisetzen, die nicht zuletzt dem gesamten Unternehmen inklusive seiner nach außen wirkenden Geschäftsbeziehungen als Harte Währung in Form eines zusätzlich gelebten Qualitätsmerkmales *Datenschutz und Datensicherheit* Vorteile im Wettbewerb bringt, andererseits neue Qualitätsmerkmale aus anderen Geschäftsfeldern für das eigene Unternehmen schafft.

Säulen des Datenschutzes

Die Grundprinzipien des Datenschutzes bieten ungeahnten integrativen Charakter und werden bei durchdachter und *sauberer*

Tipps für modernen Datenschutz

- Sparen Sie nicht an der Fachkunde/der Qualifikation;
- Sorgen Sie für ein ausreichendes Zeitbudget;
- Erarbeiten Sie ein umfassendes Konzept;
- Schaffen Sie ein kooperatives Klima zwischen IT, Betriebsrat, Management und DSB, um den Datenschutz nicht als *betrieblichen Blockierer* zu betrachten;
- Externe Dienstleister unterstützen Sie jederzeit durch Zuarbeit, Know-How oder einen externen DSB;
- Nutzen Sie den Mehrwert, den Datenschutz Ihnen bietet.

Anwendung sehr schnell vom Bremsklotz zum Startblock.

Als Grundprinzipien sieht das BDSG folgende Aspekte vor, die zu realisieren sind:

- Datenvermeidung & Datensparsamkeit gemäß § 3a BDSG;
- Datenverfügbarkeit gemäß § 9 Anlage zu 9, Satz 1 Ziffer Z BDSG;
- Verarbeitungskontrolle gemäß § 4 BDSG;
- Datenweitergabe und Datentrennung gemäß § 4 BDSG.

Die weiter oben angesprochenen Löschzyklen personenbezogener Altdaten, die nicht mehr gebraucht werden und nur noch nach den Vorschriften aus der Abgabenordnung aufbewahrt werden, spielen für alle Beteiligten eine Rolle und befolgen dabei selbst das Grundprinzip der Datensparsamkeit. Doch was heißt *Datensparsamkeit* eigentlich? Per definitionem bedeutet dies, dass sich die *Gestaltung und Auswahl von Datenverarbeitungssystemen […] an dem Ziel auszurichten [haben], keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht* (Quelle: § 3a BDSG).

Praktische Konkordanz

So erreicht der IT'ler durch den aufgesetzten installierten Löschzyklus höhere Performance im Ressourcenmanagement, was sich wiederum auf die operativen Kosten auswirkt. Der Betriebsrat ist gegebenenfalls *froh*, dass Daten seiner Mitarbeiter (endlich?) pseudonymisiert oder gar gelöscht wurden, weil sie gar nicht benötigt wurden, und nicht zuletzt hat der DSB einem hohen Gut des deutschen Datenschutzrechtes Rechnung tragen können. Dabei obliegt dem DSB durchaus die Möglichkeit, praxisorientierte Ergebnisse herbeizuführen, denn auch technisch-organisatorische Maßnahmen stehen immer in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck.

Nicht nur der datenschutzrechtliche Grundsatz der Datensparsamkeit *überlappt* den IT-Sicherheitsbereich, auch die Grundsätze wie z.B. Verarbeitungskontrolle und Datentrennung tangieren diesen. Es sei der Fall gegeben, dass ein interner Prozess dergestalt läuft, dass der Kunde in seinem persönlichen Web-Access im Front-End andere Daten als seine eigenen wiederfindet. Erbost wendet er sich an das Unternehmen, das die Anfrage bestenfalls direkt an den DSB weiterleitet, so es entsprechend der gesetzlichen Vorschriften einen DSB bestellt hat. Dieser wird nun versuchen, den Sachverhalt zu nachvollziehen, die Ursache und damit das Problem zu eruieren und Möglichkeiten für eine möglichst einfache Lösung zu finden. Hierzu wird er in der Regel immer den Kontakt zu den IT-Fachleuten des Unternehmens suchen, da niemand besser die individuellen Systeme kennt und versteht. Regelmäßige Audits sensibler Systeme, Sicherheitsübungen und die gesetzlich vorgeschriebenen Vorabkontrollen (§ 4d Abs. 5 BDSG) können solche Aktionen planbar und damit berechenbar machen. Teure und oft unbedachte aktionistische Reaktionen lassen sich so vermeiden – zum Besten des Unternehmens. Hiervon profitieren alle Beteiligten: Der Betroffene bekommt eine vernünftige Antwort im Sinne des BDSG, bzw. die Information, dass ein solcher Vorfall sich nicht wiederholen wird. Die IT kann sich in einem etwas ruhigeren Fahrwasser und damit noch souveräner bewegen, die Geschäftsleitung braucht sich keine Gedanken über drohende Bußgelder und Haftstrafen machen.

Fazit: Effektive Rollenverteilung im Unternehmen

Abschließend bleibt festzuhalten, dass es für alle Beteiligten der unterschiedlichsten Unternehmensbereiche lohnenswert ist, zielorientiert im Sinne des Unternehmens zu (ver)handeln. Sie verfolgen unterschiedliche Interessen, die letztlich in der Praxis durchaus unter einen Hut zu bringen sind. Hier tritt die Bedeutung der Fähigkeit zum interdisziplinären Schnittstellenmanagement, das wir seit Jahren propagieren, wieder deutlich hervor. Der professionelle DSB hat hier eine gute Handlungsmöglichkeit. Hierbei sei an das Beispiel aus dem Bestseller *Das Harvard-Konzept* (*Harvard Negotiation Project*) von Roger Fisher, William Ury und Bruce Patton erinnert, indem die Mutter eine Orange an ihre beiden Töchter verteilen möchte. Beide Töchter erheben Anspruch auf die Orange. Die Mutter könnte sie einer Tochter geben, dann wäre die andere unglücklich. Oder sie halbiert die Frucht, dann wären beide Töchter unzufrieden. Schlau, wie die Mutter jedoch ist, fragt sie nach. Daraufhin meint Tochter A, sie wolle einen Kuchen backen und brauche dafür die Orangenschale. Tochter B wiederum möchte nur das Fruchtfleisch essen. Die Entscheidung der Mutter nach dieser kommunikativen Interaktion ist keine Überraschung: Tochter A bekommt die Schale für ihren Kuchen, Tochter B das Fruchtfleisch zum Essen. Die Übertragung auf den unternehmerischen Fall: der praxisorientierte professionelle Datenschutz sucht den Gewinn für alle, indem er genau hinsieht, welche Bedürfnisse alle Beteiligten haben. Die Konsequenz: Niemand muss mehr die Rolle des Sündenbocks zwischen allen Stühlen spielen, sondern jeder kann sich ganz den Aufgaben, die seiner hohen Fachkompetenz entsprechen, widmen.

Moderner Datenschutz birgt also die Chance in sich, dass der betriebliche DSB vom klischeebedingt misstrauisch beäugten Kontrollfreak zum geldwerten integrativen Partner wird, der das Unternehmen intern nach Kräften interdisziplinär unterstützt und nach außen in der Öffentlichkeit ernsthaft und glaubwürdig vertritt und kein potemkinsches Dorf entstehen lässt. Der Betriebsrat bekommt einen noch integrativeren Standpunkt. Das heißt präzise, durch die Einbindung seiner Kompetenz wird der Ablauf im Unternehmen für alle Beteiligten (Mitarbeiter, Kunden, Öffentlichkeit...) transparent, inklusive Bullauge für die eigenen Mitarbeiter. Denn im Zweifel sind wir alle Endverbraucher.

Lesen Sie in der nächsten Ausgabe in der Rubrik Datenschutz, was genau Permission Marketing bringt, und warum das auf Dauer richtig was bringt.

Kerstin Blossey
Kerstin Blossey ist 1969 in Erlangen geboren und Gründerin von Blossey & Partner (ehemals KSB4 Consulting), einem aufstrebenden Unternehmen, das sich 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.
Kontakt mit den Autoren: datenschutzpraxis@blossey-partner.de