INTEREST

www.datenschuetzer.de

Datenschutz PRAXIS

Datenschutz – rechtssicher, vollständig, dauerhaft.

Ausgabe Juni 2006 | 9 € zzgl. MwSt.

Zertifizierung in vier Schritten

Datenschutz mit Gütesiegel

Ein Ende des technologischen Fortschritts ist nicht in Sicht. Bei all den Verbesserungen und Erleichterungen des täglichen privaten und geschäftlichen Lebens darf der Mensch jedoch nicht auf der Strecke bleiben und bloßes Objekt der Informationstechnologie werden. Aus diesem Grund ist wichtig, dass dem Datenschutz ein entsprechend hoher Stellenwert eingeräumt wird. Gütesiegel machen diesen Stellenwert nach außen für alle sichtbar.

Ob der Einsatz einer Software datenschutzkonform erfolgen kann, überprüft eine Zertifizierung. Ein Datenschutz-Gütesiegel dokumentiert dies nach außen.

Eine Zertifizierung ist eine genaue Überprüfung durch eine unabhängige fachkundige Stelle

Unter Zertifizierung versteht man die Überprüfung von Verfahren durch eine unabhängige Behörde, die über eine besondere Fachkunde verfügt. Prüfungsgrundlage ist ein Katalog von Anforderungen, der bei jeder Prüfung standardmäßig herangezogen wird.

Eine solche unabhängige Zertifizierungsstelle, die mit Anforderungskatalogen arbeitet, ist das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) mit seinem Datenschutz-Gütesiegel für IT-Produkte.

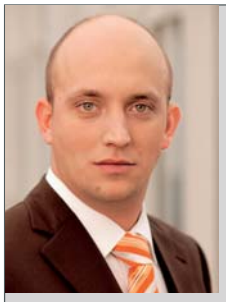
Eine Zertifizierung bringt handfeste Wettbewerbsvorteile

Die Zertifizierung bringt dem Hersteller eines IT-Produkts Wettbewerbsvorteile. Denn er kann sich dadurch maßgeblich von seinen Mitbewerbern abheben.

Auch die Akzeptanz des Produkts bei Verbrauchern wird dadurch erhöht, da sie darauf vertrauen können, dass es mit ihren personenbezogenen Daten sorgsam umgeht.

Fortsetzung auf Seite 8

ISSN-Nr. 1614-6867



Editorial

„Zu Gast im Knast“,

liebe Leser,

diesen Eindruck könnte man bekommen, verfolgt man die Berichterstattung über die ausufernden Sicherheitsmaßnahmen und die Datensammelwut rund um die Fußballweltmeisterschaft.

Verstärkte Grenzkontrollen, Bundeswehr in Lauerstellung, Awacs über den Stadien, Hubschrauber und Phantom-Jets auf Abruf, Speicherung von Personalausweisnummern, Überprüfung aller Helfer und Journalisten durch Polizei und Verfassungsschutz, umfassende Videoüberwachung, RFID-Chips, Speicherung einer Vielzahl persönlicher Daten an einer ebensolchen Vielzahl von Stellen ... Die Liste ließe sich beliebig fortsetzen.

Datenschützer und Bürger haben da nicht mehr viel zu melden. Aber worum ging's eigentlich? Ach ja, da war doch noch was – der Fußball.

Bleibt zu hoffen, dass trotz des Bombardements mit Sicherheitsmaßnahmen die Freude am Sport nicht zu kurz kommt.

Mit besten Grüßen

Ihr Raphael Stange,
Chefredakteur Datenschutz PRAXIS

Notfallhandbuch

Auch im IT-Notfall Daten schützen

Je abhängiger ein Unternehmen von der IT ist, desto dramatischer ist es, wenn Rechner gestört sind oder gar ausfallen. Dann ist Zeit Geld. Beim Support helfen Notfallhandbücher, die Fehlerbeseitigung zu systematisieren. Dabei fällt der Datenschutz in der Hektik leicht unter den Tisch. Weisen Sie daher die Kollegen des Help Desk besonders auf datenschutzkonformes Verhalten in diesen Stresssituationen hin.

Machen Sie sich bewusst, dass IT-Mitarbeiter während eines IT-Notfalls andere Prioritäten setzen als in Normalzeiten. Jegliche Behinderung bei der Fehlersuche empfinden sie als störend. Das betrifft natürlich auch die Maßnahmen zum Datenschutz.

Das Notfallhandbuch bietet Ihnen die Chance, die Anforderungen des Datenschutzes festzuschreiben und in den Notfallabläufen zu berücksichtigen. Dabei ist Ihre Initiative als Datenschutzbeauftragter gefordert.

Im IT-Notfall drohen Gefahren für personenbezogene Daten

Oberste Priorität in einem IT-Notfall ist die zügige Wiederherstellung der Verfügbarkeit. Dazu nutzt der IT-Mitarbeiter alle Erfahrungen und Hilfsmittel, die ihm zur Verfügung stehen.

Ein Notfallhandbuch sichert den Datenschutz

Auch der Datenschutz hat Interesse an einer schnellen und sicheren Beseitigung von IT-Störungen. Nur in festgeschriebenen Abläufen für die Fehlerbehebung können die Belange der personenbezogenen Daten berücksichtigt werden.

Drängen Sie also auf die rasche Erstellung eines Notfallhandbuchs, wenn noch keines vorliegt!

Dass dabei die Gefährdung der personenbezogenen Daten im System erhöht wird, mag für viele verständlich sein, für den Datenschutzbeauftragten ist es nicht akzeptabel.

Zugriffsschutz stört IT-Mitarbeiter nur

Der wirksamste Schutz personenbezogener Daten ist der Zugriffsschutz. Im IT-Notfall ist dieser allerdings äußerst hinderlich. Viele IT-Mitarbeiter schalten ihn daher während des IT-Notfalls aus, übersehen aber dabei die wesentlich höhere Bedrohung während der Störungszeit.

Externe Helfer brauchen Berechtigungen, um Fehler zu beheben

Externe Experten können die Fehlerbehebung wesentlich beschleunigen, benötigen jedoch Zugriff auf das System. Dies geschieht oft online, wodurch die Vergabe von Berechtigungen weiter erschwert wird. Die notwendige Sicherheit auch während der Störung beizubehalten, fällt nicht leicht.

„Try and error“ verursacht Datenberge

Eine Fehlersuche ist aufwändig und oft mit Versuch und Irrtum verbunden. Dabei entstehen Hilfs- und Zwischendateien oder Kopien der Datenbestände. Immer wieder finden sich darin auch geschützte sensible Daten. Für Sie gilt es, den Umgang mit solchen Beständen zu regeln.

Bestehen Sie auf der Protokollierung aller Vorgänge

Der Umgang mit personenbezogenen Daten muss penibel protokolliert werden, auch und gerade bei IT-Notfällen. Veränderungen, Datenübertragungen oder Datenträger mit solchen Beständen lassen sich so nachvollziehen und verwalten.

Zu einem sicheren Notfallhandbuch gehört auch der Datenschutz

Die beschriebenen Gefahren für den Datenschutz, also v.a. das Risiko, dass Interne und Externe unbeschränkten Zugriff erhalten, dass das Vorgehen nicht protokolliert wird und dass bei der Fehlersuche neue sensible Daten anfallen, sollten allen Beteiligten deutlich machen, dass ein IT-Notfallhandbuch auch die Einhaltung der Maßnahmen zum Schutz der personenbezogenen Daten gewährleisten muss.

Wenn Bits und Bytes in Gefahr sind, lenkt ein Notfallhandbuch die Rettungsmaßnahmen in geordnete Bahnen.

Um zuverlässig die wichtigsten Punkte abzudecken, hat sich in der Praxis die Aufnahme der folgenden drei Schritte als sinnvoll erwiesen.

1. Ist der Datenschutz betroffen?

Bei jeder als IT-Notfall klassifizierten Störung muss festgestellt werden, ob durch die Störung selbst und/oder durch die Aktivitäten zur Fehlerbeseitigung personenbezogene Daten zusätzlich gefährdet sind.

Für diese Entscheidung müssen die verantwortlichen Mitarbeiter entsprechend der Wichtigkeit des Themas auch die dafür notwendige Zeit bekommen.

2. Wurde der DSB informiert?

Ist der Datenschutz betroffen, muss der Datenschutzbeauftragte informiert werden. Auch diesen Vorgang muss ein IT-Notfallhandbuch festschreiben. Sonst gerät er leicht in Vergessenheit.

3. Ist ein zusätzlicher Ablauf für den Datenschutzbeauftragten beschrieben?

Der Datenschutzbeauftragte muss im IT-Notfall nach der Benachrichtigung zuverlässig reagieren. Im Idealfall schreibt ein Notfallhandbuch also auch fest, welche Handlungsmöglichkeiten dem DSB zur Verfügung stehen, wird ihm eine Störung, die den Datenschutz gefährdet, mitgeteilt.

Dies kann beispielsweise die Einordnung des IT-Notfalls in Risikoklassen sein. Je nach der Einteilung kann der Datenschutzbeauftragte von einer einfachen späteren Kontrolle bis zur persönlichen Überwachung der IT-Notfallaktivitäten zu verschiedenen Instrumentarien greifen.

Auch der Datenschutz erzeugt Notfälle!

Im IT-Notfallhandbuch wird der IT-Notfall selbst definiert. Nicht jede Störung gehört dazu, erst ab einem gewissen Kostenpotenzial wird die Störung zum Notfall. Durch die Berücksichtigung des Datenschutzes können allerdings einfache Störungen eher zu Notfällen „aufsteigen“.

Funktionieren die zum Schutz der personenbezogenen Daten initiierten Maßnahmen nicht mehr, kann die Unterbrechung der Verarbeitung notwendig werden, auch wenn das System ansonsten technisch funktionsfähig ist.

Abläufe und Definitionen im Notfallhandbuch erhöhen die Sicherheit für die personenbezogenen Daten. Nutzen Sie diese Chance und passen Sie gemeinsam mit dem IT-Management das Notfallhandbuch an!

Reinhard Bleiber

So geht der Datenschutz auch im IT-Notfall nicht unter!

Hat der Mitarbeiter ein erhöhtes Risiko für den Datenschutz erkannt, müssen zusätzliche Maßnahmen greifen. Damit sie aber auch tatsächlich beachtet werden, muss das IT-Notfallhandbuch diese Maßnahmen dokumentieren:

- ✔ **Zugriffsschutz**
  Der Zugriffsschutz muss zumindest für die personenbezogenen Daten unbedingt aufrecht erhalten bleiben. Für den IT-Notfall können dazu z.B. spezielle User mit eingeschränkten Berechtigungen vorbereitet werden.
- ✔ **Verpflichtung auf das Datengeheimnis**
  Anweisungen im IT-Notfallhandbuch müssen festhalten, dass externe Helfer vor dem Einsatz auf das Datengeheimnis verpflichtet werden. Optimal ist es, die Externen bereits vorbeugend zu bestimmen und zu verpflichten.
- ✔ **Ausführliche Protokolle**
  Auch während der Fehlerbeseitigung sind jeder Zugriff und jede Veränderung zu protokollieren. Das Handbuch muss daher ausdrücklich verbieten, die Protokollierungen auszuschalten. Bei Arbeiten auf Systemebene muss für eine ausreichende Dokumentation gesorgt werden.
- ✔ **Sichere Datenvernichtung**
  Protokolle belegen, welche Datenbestände als Sicherungskopien, Zwischen- oder Arbeitsdateien entstanden sind. Eine der letzten Anweisungen muss die sichere Vernichtung solcher Datenbestände anordnen. Auch eine Sicherung der während des IT-Notfalls entstandenen Daten ist notwendig, da sich nur so Veränderungen nachvollziehen lassen.

Scoring-Verfahren, Teil 2

Interessen in Balance

Der Einsatz von Scoring-Verfahren verspricht, Aussagen über das zukünftige Verhalten von Kunden treffen zu können. Für den Datenschutzbeauftragten gilt es, die Interessen zwischen Anbieter und Kunde sorgfältig abzuwägen, gegebenenfalls dessen Einwilligung einzuholen oder die Grenzen des Scorings aufzuzeigen.

Im ersten Teil über Scoring-Verfahren in unserer Mai-Ausgabe haben Sie die wichtigsten Kontrollpunkte bei der Konzeption eines Scoring-Systems sowie die Grenzen der Zulässigkeit bei der Datenerhebung kennen gelernt. Dieses Mal klären wir die Fragen der zulässigen Nutzung von Daten, der Anwendbarkeit des § 6a BDSG, der notwendigen Transparenz sowie zu den Rechten Betroffener.

Erhobene Daten dürfen nicht immer auch für Scoring genutzt werden

Auch wenn Daten im Zusammenhang mit einer Geschäftstransaktion oder anderen Sachverhalten (z.B. Bewerberauswahl) rechtmäßig erhoben worden sind, bedeutet dies nicht automatisch, dass die Daten auch für ein Scoring genutzt werden dürfen. Denn es könnte zu einer Gefährdung des Persönlichkeitsrechts des Betroffenen kommen.

Ziehen Sie daher als Rechtsgrundlage für die Durchführung eines Scorings § 28 Abs. 1 Nr. 2 BDSG (Interessenabwägung) heran.

Nicht erlaubt dürfte in den meisten Fällen die Nutzung der personenbezogenen Daten zur Erfüllung des Vertragszwecks bzw. eines vertragsähnlichen Vertrauensverhältnisses gemäß § 28 Abs. 1 Nr. 1 BDSG sein.

Mit Einwilligung ist die Datenverwendung möglich – aber nicht grenzenlos

Möchten Sie dennoch mit diesen Daten arbeiten, können Sie eine Einwilligung einholen. Allerdings darf eine solche Einwilligung den Betroffenen nicht im Übermaß benachteiligen. So ist auch trotz Einwilligung die Verwendung diskriminierender Daten unzulässig.

Welche Daten nun diskriminierend sind, ist wegen des noch nicht verabschiedeten Antidiskriminierungsgesetzes nicht abschließend zu beurteilen.

So wird es sicherlich noch weiterer Diskussionen bedürfen, um beispielsweise die Frage zu klären, ob das Alter des Betroffenen beim Scoring genutzt werden darf. Derzeit ist dies noch erlaubt, wenn die mathematisch-statistische Relevanz des Merkmals „Alter“ für die Scoringbewertung nachgewiesen werden kann.

Nachweis des berechtigten Interesses

§ 28 Abs. 1 Nr. 2 BDSG verlangt zur Durchführung eines Scorings, dass es zur Wahrung berechtigter Interessen des Unternehmens erforderlich ist.

Ein solches berechtigtes Interesse besteht, wenn die statistische Relevanz der verwendeten Daten belegbar ist.

Das Interesse am Scoring ist gegen das schutzwürdige Interesse des Betroffenen abzuwägen

Schutzwürdiges Interesse des Betroffenen gegen ein Scoring überwiegt immer dann, wenn es sich um diskriminierende Daten handelt, wie oben beschrieben.

Es gibt bereits Meinungen, dass der Verwendung von Informationen zum Familienstand (verheiratet, geschieden, ledig, nichteheliche Lebensgemeinschaft und so weiter) schutzwürdige Interessen des Betroffenen entgegen stünden. Begründet wird dies damit, dass das Unternehmen unter wirtschaftlichen Gesichtspunkten private Lebensentscheidungen auswerten würde, die aus Sicht des Betroffenen keine vertragliche Relevanz aufweisen. Ob sich diese enge Auslegung im Rahmen der Interessenabwägung als Meinung durchsetzen wird, bleibt abzuwarten.

Scoring ist möglich bei deutlichem Bezug zum Vertragszweck

Unproblematischer ist die Erhebung von Daten, die einen offensichtlich erkennbaren Bezug zum Vertragszweck haben. Dazu zählt das Einkommen für die Zahlungsbonität oder die Zahl von

Koppelung von Adressdaten mit statistischen soziodemographischen Daten

Nicht einfach ist die Frage zu beantworten, inwieweit bei einer Koppelung von Adressdaten mit statistischen soziodemographischen Daten (z.B. Geomarketingdaten) die Schutzwürdigkeit der Betroffenen überwiegt.

Häufig wird bei derartigen Analysen das Wohnumfeld in eine soziodemographische Dimension gebracht. Die Folge ist, dass der Betroffene diesem Segment unabhängig von seiner tatsächlichen Situation zugeordnet wird. Zweifellos spielt eine Rolle, dass der persönlichkeitsrechtliche Eingriff bei der Ansprache zum Zweck der Werbung eher als sehr gering anzusehen ist.

Für den Adressaten mag es durchaus vorteilhaft sein, wenn er keine unpassenden Angebote erhält und sein Briefkasten nicht überquillt. Datenschutzrechtlich bedenklich kann es jedoch sein, detaillierte Datenprofile der Betroffenen zu entwickeln. Denn wenn das Datenprofil eine bestimmte Komplexitätsgrenze überschreitet, so könnten die schutzwürdigen Interessen der Betroffenen überwiegen.

Unfällen mit dem Auto für den Abschluss einer Kfz-Versicherung. Auch Daten, die der Betroffene durch sein Verhalten leicht beeinflussen kann oder die erst durch sein Handeln entstehen, sind im Rahmen des Scorings nutzbar (z.B. Einhalten von Zahlungsterminen oder häufiger Wohnungswechsel).

§ 6a BDSG „ausschließlich automatisierte Einzelentscheidung“

Nach § 6a Abs. 1 BDSG dürfen Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung oder Nutzung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

Trifft ein Mitarbeiter die Entscheidung, müssen Sie § 6a nicht beachten

Wichtig bei dieser gesetzlichen Regelung ist das Kriterium der „Ausschließlichkeit“ der automatisierten Entscheidung. Wird das Scoring jedoch nur zur Unterstützung bei einer durch einen Mitarbeiter zu treffenden Entscheidung herangezogen, brauchen die besonderen Anforderungen des § 6a nicht beachtet zu werden.

Kein allgemeiner Auskunftsanspruch

Es besteht kein allgemeiner Anspruch auf Auskunft, aus welchem Grund der Abschluss eines Vertrages oder der Abschluss zu einem bestimmten Tarif abgelehnt wird. Der Auskunftsanspruch nach § 34 Abs. 1 Nr. 1 BDSG bezieht sich auf die über den Betroffenen gespeicherten Daten. Wird der Scorewert gespeichert, dann ist der Betroffene auf Anfrage auch über den Scorewert und dessen Aussage zu informieren.

Machen Sie die Zweckbestimmung der Datenerhebung deutlich

Machen Sie im Rahmen des Vertragsabschlusses mit dem Betroffenen die beabsichtigte Zweckbestimmung der Datenerhebung auch für das Scoring deutlich (Unterrichtungspflichten gemäß § 4 BDSG). Informieren Sie ihn auch darüber, wenn bereits im Bestand des Unternehmens befindliche oder später hinzukommende Daten zum Scoring herangezogen werden.

Die Interessenabwägung kann auch beim Scoring ein schwieriger Job für den Datenschutzbeauftragten sein.

Einen weiter gehenden Informationsanspruch hat der Betroffene, wenn es sich bei dem Scorewert in Wirklichkeit um eine automatisierte Einzelentscheidung nach § 6a BDSG handeln sollte. In diesem Fall muss er darüber informiert werden, dass die Ablehnung aufgrund des Scorewertes erfolgt ist.

Sein Auskunftsrecht erstreckt sich dann auch auf den logischen Aufbau des Scoring-Verfahrens. Dabei müssen jedoch nicht der Aufbau des Scorewerts und die Gewichtung aufgedeckt werden (Betriebsgeheimnis).

Scoring für Werbung ist problemloser

Weniger problematisch sind Scoringauswertungen für Zwecke der Werbung und des Marketings. Dies geschieht häufig zur Optimierung der Werbeansprache, indem vorhandene Kunden unterschiedlichen Klassen zugeordnet werden.

Auch wenn die Klassifizierung durch allgemeine Erfahrungswerte angereichert wird, die Gruppierungen beispielsweise nach Alter, Vornamen, Geschlecht, Beruf oder Wohngegend ermöglichen, so ist hiermit im Allgemeinen keine besondere Gefährdung des informationellen Selbstbestimmungsrechts verbunden.

Dies gilt insbesondere dann, wenn solche Klassifizierungen zur Kanalisierung des Werbematerials dienen. Oft sehen sie es die Betroffenen sogar positiv, weil sie nicht mit Werbebotschaften belästigt werden, die an ihrem Bedarf vorbeigehen.

Eine Einwilligung ist nötig, wenn Nachteile zu erwarten sind

Je nach beabsichtigter Nutzung der errechneten Scoreergebnisse wird die Frage aufkommen, ob unter der Abwägungsklausel nach § 28 Abs. 1 Nr. 2 BDSG diese Datenverarbeitung im Rahmen des Scorings noch zulässig ist. Eine Einwilligung der Betroffenen ist sicherlich dann Voraussetzung, wenn ihnen dadurch unmittelbare und nennenswerte Nachteile entstehen.

Beim Scoring ist der DSB gefragt

In unseren beiden Artikeln zum Scoring haben wir gezeigt, dass bei der Konzeption und Einführung derartiger Systeme der DSB intensiv eingebunden werden sollte.

Nicht alle Zweifelsfragen können als geklärt angesehen werden, da die datenschutzrechtliche und auch die politische Diskussion über das Scoring gerade erst am Anfang stehen. Diskussionsgrundlage ist dabei eine Studie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) zu den Chancen und Risiken von Kredit-Scoring-Systemen.

Harald Eul

Harald Eul ist Datenschutzberater und Vorstandsmitglied der GDD, Bonn

Datenschutzgerechte Unternehmensausgliederung

Alles geregelt – nichts gemacht

Die Bandbreite beim Facility Management reicht von der internen Haus- und Netzwerktechnik über das Energiemanagement und die Sicherheitstechnik bis zur Zugangskontrolle oder zu den Überwachungsanlagen. Sollen diese Arbeiten aus dem Unternehmen ausgegliedert werden, gilt es, eine oft symbiotische Einheit datenschutzgerecht zu trennen. Keine leichte Aufgabe.

Durch Ausgliederung entstehen neue Unternehmen, die sich dem offenen Wettbewerb stellen müssen. Kostenreduzierung, Verschlankung, Auslagerung lautet die Devise.

Die kaufmännische Lösung

Die kaufmännischen Regularien sind schnell erstellt, die Vertragsbedingungen vorgegeben und im Facility-Management festgehalten. Räume innerhalb des Betriebsgeländes werden vermietet, Pauschalen für die Infrastruktur wie Strom, Wasser bis hin zur IT-Netzstruktur vereinbart.

Der Pförtner ist in Personalunion für beide Unternehmen tätig und wird durch Videokameras unterstützt. Die Putzfrauen kommen wie gewohnt, die Kollegen sind dieselben. Die zu erledigenden Aufgaben bleiben erstmal gleich – nur die Firmenbezeichnung auf der monatlichen Gehaltsabrechnung hat sich geändert.

Egal, ob Instandhaltung, Putzkolonne oder Help Desk – werden Unternehmensteile ausgegliedert, darf der Datenschutz nicht an letzter Stelle stehen.

Outsourcing erfolgreich – Datenschutz bleibt links liegen

Leider wird der Datenschutz in die Prozesskette kaum involviert. Der DSB aus dem Kernunternehmen, das den Teilbereich ausgliedert, mischt sich in der Regel nicht in das Procedere ein.

Das neu gegründete Unternehmen kennt und hat noch keinen Datenschutzbeauftragten. In der Folge bleibt der Datenschutz links liegen.

Herausforderung Umdenken

Ein DSB, der nun nachträglich seine Arbeit aufnimmt, hat es nicht einfach. Eine Fülle von Aufgaben erwartet ihn, wobei das Umdenken der Mitarbeiter die größte Herausforderung ist.

Denn sie sind nicht mehr bei Firma ABC beschäftigt, sondern bei dem neu gegründeten Unternehmen XY-GmbH. Der freundliche Mitarbeiter der IT-Betreuung ist nicht mehr Kollege, sondern nach dem BDSG der Dienstleister eines Fremdunternehmens.

Zerlegen Sie das Facility Management in seine Einzelteile

Die Aufgaben des Datenschutzbeauftragten bestehen zudem darin, das Facility Management „aufzudröseln“. Wer hat z.B. Zutritt auf das Gelände der Firma ABC und Zugang zu den Betriebsräumen der XY-GmbH (Zugangskontrollen nach § 9 BDSG)?

Gibt es ein Drehkreuz mit Ausweisleser, werden die Bewegungsdaten von Mitarbeitern gespeichert, wer hat Zugriff auf die Ein- und Ausgangsdaten? Welche Aufgaben hat der gemeinsame Pförtner für Ihr Unternehmen, wie wird mit Besuchern umgegangen, wie die erhobenen Besucherdaten elektronisch gespeichert und ausgewertet?

Weiterhin stehen Kernelemente wie Stromversorgung, Klimatisierung, Brandschutz, Nachtwache oder Videokontrolle zur Überprüfung an.

Ist die IT-Netzwerkstruktur eindeutig getrennt, oder gibt es noch Verbindungen zum alten Unternehmen? Wie steht es um die TK-Dienste – wer hat bei einer gemeinsamen TK-Anlage Zugriff auf die Verbindungsdaten? Wird das TK-Gesetz eingehalten?

Muster erleichtern die Arbeit!

Als Abonnent von Datenschutz PRAXIS können Sie unter *www.datenschuetzer.de* das Muster einer Verpflichtungserklärung nach § 5 BDSG kostenlos herunterladen.

Überprüfen Sie die Personalakten

Im Personalbereich sind auf jeden Fall die Personalakten zu überprüfen. Dürfen Informationen über die Mitarbeiter aus der alten Firma ABC übernommen werden? Gelten bestehende Betriebsvereinbarungen, müssen neue TK- und IT-Richtlinien erstellt werden?

Vergessen Sie auf keinen Fall, die Mitarbeiter nach dem § 5 BDSG neu zu verpflichten.

Prüfen Sie Dienstleister und Auftragsdatenverarbeiter

Wenn Leistungen über die alte Firma bezogen werden, sind diese nach § 11 BDSG zu überprüfen. Auch müssen Sie die Mitarbeiter ggf. auf die Datenschutzverpflichtungen nach dem BDSG hinweisen, als wären sie Angehörige eines völlig fremden Unternehmens.

Hermann Keck

Meldesysteme datenschutzkonform aufbauen, Teil 2

Whistleblowing – Anzeigepflichten im Unternehmen

Der US-amerikanische Sarbanes Oxley Act verpflichtet US-börsennotierte Unternehmen oder ihre deutschen Töchter dazu, Fehlverhalten im Finanzbereich zu melden. Doch mehr und mehr deutsche Unternehmen führen freiwillig solche Meldesysteme ein. Nachdem der erste Teil in der Mai-Ausgabe die rechtlichen Grundlagen vorgestellt hat, geht es jetzt um die optimale organisatorische Umsetzung.

Am 1. Februar 2006 verabschiedete die Art.-29-Arbeitsgruppe (Gruppe der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten) ein Arbeitspapier, das sich erstmals umfassend mit Whistleblowing auseinander setzt.

Tipps für die Einführung

Das Positionspapier erkennt die Notwendigkeit von Whistleblowing-Systemen ausdrücklich an, will es Unternehmen aber erleichtern, diese Systeme datenschutzrechtlich korrekt zu gestalten und damit insbesondere den Vorgaben der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) zu genügen.

Das Papier finden Sie in englischer Sprache auf der Website der Art.-29-Gruppe über *www.eu.int*.

1. Halten Sie den Kreis der potenziell Beteiligten möglichst klein

Laut Arbeitspapier sollte der Kreis potenzieller „Whistleblower“ möglichst klein sein. Dies soll den Missbrauch durch Falschmeldungen minimieren.

2. Sorgen Sie für Vertraulichkeit

Sichern Sie dem Anzeigenden Vertraulichkeit zu. Akzeptieren Sie anonyme Anzeigen nur in Ausnahmefällen, da sie das Vertrauen in solche Systeme stark erschüttern können.

3. Achten Sie auf Zweckbindung und Datensparsamkeit

Es dürfen nur die Informationen verarbeitet werden, die für die Bearbeitung der Anzeige notwendig sind. Dies folgt zwingend aus den Prinzipien der Zweckbindung und der Datensparsamkeit. Meldungen dürfen nicht mit anderen personenbezogenen Daten des Meldenden verbunden werden.

Die Identität der „Whistleblower“ muss vertraulich behandelt werden.

4. Organisieren Sie die Datenlöschung

Innerhalb von zwei Monaten nach Abschluss der Untersuchung sollten die gespeicherten Daten gelöscht werden. Lediglich in Fällen, in denen weitere rechtliche Schritte erforderlich sind, dürfen die Daten auch für einen längeren Zeitraum gespeichert bleiben. Daten, die sich im Rahmen der Untersuchung als überflüssig erweisen, sollen unverzüglich gelöscht werden.

5. Informieren Sie den Angezeigten

Die beschuldigte Person muss über die Anzeige informiert werden, sobald kein Risiko besteht, dass sie Beweise vernichtet. Der Angezeigte sollte den Namen des Anzeigenden im Regelfall aber nur dann erfahren, wenn die Anzeige vorsätzlich falsch war. Die Information soll enthalten:

- die verantwortliche Stelle,
- den Tatbestand der Anschuldigung,
- mögliche Adressaten des internen Berichts und
- eine Belehrung über das Auskunfts- und Berichtigungsrecht.

6. Daten müssen sicher sein

Legen Sie bei der Speicherung der Daten besonderes Augenmerk auf die Einhaltung organisatorisch-technischer Maßnahmen, um zu verhindern, dass diese Daten in falsche Hände gelangen.

7. Setzen Sie nur ausgewählte Mitarbeiter ein

Whistleblowing-Verfahren sollten ausschließlich durch speziell ausgewählte und geschulte Mitarbeiter betreut werden. Es kann sich anbieten, eine spezielle Abteilung zu bilden. Zudem ist strikt darauf zu achten, dass solche Abteilungen streng von anderen getrennt werden (etwa von Personal/HR).

8. Achten Sie auf korrekte Übermittlung

Im Fall der Auslagerung von Whistleblowing-Verfahren ist zu bedenken, dass das beauftragende Unternehmen stets verantwortliche Stelle bleibt.

Bei multinationalen Konzernen sollten die Daten nicht an „exterritoriale“ Gruppenunternehmen übermittelt werden. Ausnahmen sind nur möglich, wenn andere Gruppenunternehmen unmittelbar oder mittelbar von den Vorwürfen betroffen sind.

Werden dennoch Daten übermittelt, greifen Sie auf die Standardvertragsklauseln zurück bzw. bei der Übermittlung in die USA auf Safe Harbor.

Dr. Philipp Kramer/Hans Gliss/ Michael Herrmann

Fortsetzung von Seite 1

Dieser Aspekt ist nicht hoch genug zu bewerten, da die Angst vor Datenmissbrauch das größte Hemmnis des E-Commerce darstellt.

Das Gütesiegel ist das Tor auch zur öffentlichen Verwaltung

Das Datenschutz-Gütesiegel des ULD erleichtert auch den Einsatz von IT-Verfahren in der öffentlichen Verwaltung. So sieht insbesondere das schleswig-holsteinische Landesdatenschutzgesetz ausdrücklich vor, dass die Behörden vorrangig zertifizierte Software-Produkte einsetzen sollen.

Das Gütesiegel kann deshalb für ein Unternehmen auch bei öffentlichen Ausschreibungen von Vorteil sein. In Schleswig-Holstein wird das Gütesiegel zwingend berücksichtigt.

… allerdings nicht uneingeschränkt in allen Bundesländern

Mit Ausnahme von Brandenburg sind die Verwaltungen der anderen Bundesländer nicht gehalten, ein Gütesiegel des ULD in ihre Entscheidung einzubeziehen. Es gibt zwar teilweise auch dort Bestrebungen, zertifizierte Produkte bevorzugt zu behandeln. Das ULD-Gütesiegel wird jedoch nicht vorbehaltlos anerkannt.

Ob das Siegel anerkannt wird, hängt vom einzelnen LDSG ab

Die Anerkennung des Gütesiegels in anderen Bundesländern hängt davon ab, ob das jeweilige Landesdatenschutzgesetz abweichende Regelungen enthält und ob diese durch das IT-Verfahren eingehalten werden.

In der Regel unterscheiden sich die einzelnen Landesdatenschutzgesetze kaum. Eventuelle Abweichungen können anhand des veröffentlichten Kurzgutachtens kostensparend und einfach aufgedeckt und Ergänzungen bzw. Änderungen vorgenommen werden, um das Produkt in der jeweiligen Behörde einsetzen zu können.

Im Übrigen können landesspezifische Datenschutzvorschriften im Gutachten berücksichtigt werden, wenn der Hersteller zum Zertifizierungszeitpunkt bereits weiß, in welchem Bundesland er das Produkt einsetzen möchte.

Das ULD zertifiziert auch Produkte für den privatwirtschaftlichen Bereich

Das Datenschutz-Gütesiegel des ULD wird auch Produkten verliehen, die ausschließlich im nichtöffentlichen Bereich eingesetzt werden. Aus dem Register der zertifizierten Produkte beim ULD ergibt sich, dass vielen Verfahren, die für den Einsatz im privaten Bereich konzipiert sind, bereits ein Gütesiegel verliehen wurde.

Beispiele sind eine Software-Applikation für digitale ärztliche Diktate sowie eine webbasierte Anwendung für berufsvorbereitende Bildungsmaßnahmen.

Prüfung in vier Schritten

Das ULD hat einen Anforderungskatalog erstellt, der aus vier Bausteinen besteht. Einzelheiten finden Sie im Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD.

Baustein 1 untersucht die Mechanismen der Datenvermeidung, Datensparsamkeit und Transparenz

Anhand des ersten Bausteins wird geprüft, ob die technische Gestaltung die Grundsätze der Datenvermeidung und der Datensparsamkeit berücksichtigt hat. Wenn schon aufgrund des Einsatzzwecks die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten notwendig ist, stellt sich die Frage, ob die Daten früh gelöscht, anonymisiert oder pseudonymisiert werden können.

Ferner wird hier geprüft, ob die Verarbeitung der personenbezogenen Daten transparent erfolgt. Transparenz erfordert, dass insbesondere die Produktbeschreibung leicht zu finden ist, der Datenfluss deutlich gemacht wird und die Daten auf dem aktuellen Stand sind.

Baustein 2 kontrolliert die Rechtmäßigkeit der Datenverarbeitung

Baustein zwei prüft, ob die Verarbeitung der Daten rechtmäßig erfolgt. Im Vorfeld muss der Gutachter anhand der zu speichernden Datenarten bereits die einzelnen datenschutzrelevanten Verfahren definiert haben.

Angelehnt an den datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt wird zunächst geprüft, ob eine gesetzliche Ermächtigungsgrundlage vorliegt, dann, ob die Möglichkeit besteht, eine Einwilligung

So läuft ein Zertifizierungsverfahren beim ULD ab

Jedes Unternehmen unabhängig vom Firmensitz kann einen Zertifizierungsantrag stellen. Gegenstand der Zertifizierung ist die Vereinbarkeit des Produkts mit den Anforderungen an den Datenschutz und an die Datensicherheit.

Sachverständige machen die Vorbereitung und erstellen ein Gutachten

Die Zertifizierungsvorbereitung erfolgt durch einen oder mehrere Gutachter, die am ULD als Sachverständige akkreditiert sind. Diese erstellen ein Gutachten, das aus einem rechtlichen und einem technischen Teil besteht.

Das Siegel ist zwei Jahre gültig

Nach bestandener Überprüfung des Gutachtens durch das ULD erfolgt die Zertifizierung durch den Erlass eines Zertifizierungsbescheids. Das Gütesiegel wird i.d.R. zeitlich befristet auf zwei Jahre verliehen. Nach Ablauf dieses Zeitraums ist eine Rezertifizierung notwendig.

wirksam abzufragen. Die Wirksamkeitsvoraussetzungen einer Einwilligung werden hier eingehend geprüft. Ferner werden Besonderheiten berücksichtigt, wie die Verarbeitung besonderer personenbezogener Daten, die Übermittlung von Daten und die Frage, ob und wie die Löschung der Daten nach dem Wegfall des Erhebungszwecks bewerkstelligt wird.

Die allgemeinen Datenschutzgrundsätze – Zweckbindungs- und Trennungsgrundsatz – sind auch Bestandteile des zweiten Prüfungsbausteins.

Sollte eine Auftragsdatenverarbeitung vorgesehen sein, wird untersucht, ob der Einsatz externer Dritter zulässig ist. Schließlich widmet sich der Gutachter auch der Prüfung besonderer technischer Datenverarbeitungsmaßnahmen, wie z.B. dem Einsatz von Systemen zur automatisierten Einzelentscheidung oder Videoüberwachungsmaßnahmen.

Baustein 3 beschäftigt sich mit den technischen und organisatorischen Maßnahmen

Der dritte Prüfungsschritt widmet sich den technischen und organisatorischen Maßnahmen, die zum Schutz der Betroffenen eingesetzt werden. Das sind folgende Maßnahmen entsprechend der Anlage zu § 9 BDSG:

- **Zutrittskontrolle:** Sicherstellung, dass Unbefugten der Zutritt zu den Systemen verwehrt wird, mit denen personenbezogene Daten verarbeitet oder genutzt werden
- **Zugangskontrolle:** Verhinderung, dass die Systeme von Unbefugten genutzt werden können (werden z.B. Authentifizierungs-, Zugriffskontroll- und Verschlüsselungsmechanismen eingesetzt?)
- **Zugriffskontrolle:** Vorliegen eines Berechtigungskonzepts, wonach gewährleistet werden soll, dass nur die Personen mit der entsprechenden Berechtigung Zugriff haben auf die Systembestandteile, die für sie bestimmt sind (werden Protokollierungen vorgenommen, wie wird mit den Protokolldaten verfahren?)
- **Weitergabekontrolle:** Gewährleistung, dass im Rahmen eines Datentransfers die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass festgestellt werden kann, an welchen Empfänger die Daten übermittelt werden
- **Eingabekontrolle:** Sicherstellung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten eingegeben, verändert oder entfernt worden sind
- **Auftragskontrolle:** Sicherstellung, dass im Rahmen einer Auftragsdatenverarbeitung personenbezogene Daten entsprechend den Weisungen des Auftraggebers verarbeitet werden können
- **Verfügbarkeitskontrolle:** Schutz der personenbezogenen Daten gegen zufällige Zerstörung oder Verlust
- **Trennungsgebot:** Sicherstellung, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden können

Ferner wird untersucht, ob die Vorabkontrolle, die Erstellung von Verfahrensverzeichnissen sowie die Tätigkeit des Datenschutzbeauftragten unterstützt werden.

Schließlich sind die technischen und organisatorischen Maßnahmen beim Einsatz besonderer Verfahren wie Chipkarten oder Videoüberwachung Gegenstand dieses Prüfungsschritts.

Bevor das ULD sein Datenschutz-Gütesiegel vergibt, nehmen seine Sachverständigen die Softwarekandidaten genau unter die Lupe.

Baustein 4 fragt nach den Rechten der Betroffenen

Die Einhaltung der Rechte der Betroffenen wird im vierten Baustein geprüft. Dabei fokussiert die Untersuchung darauf, ob das Softwareprodukt aufgrund seiner Gestaltung die Einhaltung der Rechte der Betroffenen ermöglicht bzw. unterstützt.

Weiterführende Informationen über das Zertifizierungsverfahren finden Sie unter *www.datenschutzzentrum.de,* dem Internetauftritt des ULD.

Sigrid Wild LL.M.

Frau Sigrid Wild berät als Rechtsanwältin Unternehmen in den Bereichen Datenschutz und EDV-Recht und ist anerkannte Sachverständige für IT-Produkte (rechtlich) beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.

Datenschutzgerecht kaum realisierbar

Warndateien und schwarze Listen – zu aufwändige „Mini-Schufas“

Die Idee scheint bestechend und in Zeiten schlechter Zahlungsmoral fast zwingend: Unternehmen mit gleichen Interessen – beispielsweise alle Unternehmen eines Konzerns – schließen sich zusammen und tauschen über eine geschlossene Benutzergruppe Daten über „schlechte Zahler“, „insolvenzanfällige Schuldner“ und ähnliche unangenehme Personengruppen aus.

Solche Übersichten sind Auskunfteien

Durch einen solchen Schritt schaffen die Beteiligten eine Auskunftei und müssen deshalb alle Rechtsvorschriften beachten, die für Auskunfteien einschlägig sind.

Die hessische Datenschutzaufsicht hat darauf hingewiesen, „dass sich solche Beauskunftungen an den Voraussetzungen für den Auskunfteibetrieb nach § 29 BDSG messen lassen müssen, was eine Reihe von technischen und organisatorischen Maßnahmen nach sich zieht. Insbesondere der Aufwand für die Einrichtung automatisierter Abrufverfahren nach § 10 BDSG sowie für die erforderlichen Schulungen und Kontrollen durch die Auskunftei wurden meist verkannt“ (18. Bericht vom 5.12.2005, Seite 19, *www.rpda.de/dezernate/datenschutz/download/datenschutzbericht2004.pdf*).

Projekte bleiben oft reine Planung

Es wundert kaum, dass solche Projekte deshalb oft im Planungsstadium stecken bleiben. Der Aufwand, eine Art interne „Mini-Schufa“ aufzubauen, ist zu groß. Denkbar wäre ein Warndienst, in dessen Dateien ausschließlich größere juristische Personen aufgenommen werden. Denn die Daten solcher Unternehmen fallen mangels Personenbezug nicht unter den Datenschutz.

„Bußgeld in angemessener Höhe“

Einmal zu oft gefragt

Das war dem Bremischen Datenschutzbeauftragten denn doch zuviel. Die Creditreform Bremen hatte einen Vermieter angeschrieben mit der Bitte, die neue Anschrift eines früheren Mieters mitzuteilen. Das Schreiben enthielt eine ausführliche Aufstellung der gegenüber dem Betroffenen geltend gemachten finanziellen Forderungen mit dem Namen des Gläubigers.

Auch wenn jemand eine Menge Schulden hinterlassen hat und nicht auffindbar ist, darf ein Geldeintreiber nicht den ehemaligen Vermieter angehen und ihn ausführlich informieren.

Die genannte Person war dem Vermieter aber vollkommen unbekannt. Einziger Verbindungspunkt zwischen den beiden war, dass die Person, nach der gefragt wurde, vor ihrem Umzug zwar in derselben Straße, allerdings in einem ganz anderen Haus gewohnt hatte.

Unzulässige Datenübermittlung

Der Datenschutzbeauftragte beanstandete als Datenschutzaufsichtsbehörde für Privatunternehmen die unzulässige Datenübermittlung an den (scheinbaren) Vermieter und wies darauf hin, dass in solchen Fällen das Einwohnermeldeamt die richtige Anlaufstelle sei.

Mit der Beteuerung, solche Fälle würden nicht wieder vorkommen, gab er sich nicht zufrieden. Vielmehr verhängte er ein Bußgeld, dessen Höhe freilich nicht mitgeteilt ist (28. Tätigkeitsbericht, Ziff. 18.6., siehe *http://www.datenschutz-bremen.de/pdf/jahresbericht_28.pdf*).

Eine allgemeine Anfrage beim letzten Vermieter ist nur letzte Möglichkeit

Was aber ist, wenn die Nachfrage beim Einwohnermeldeamt erfolglos bleibt, weil der Betroffene seinen Umzug dort nicht gemeldet hat? In solchen Fällen darf man durchaus allgemein – also ohne Nennung von Forderungen usw. – beim bisherigen Vermieter nachfragen, ob der Betroffene und seine neue Anschrift dort bekannt sind.

Es muss aber sicher sein, wo der Betroffene bisher gewohnt hat. Anfragen auf der Basis von Gerüchten und Hörensagen sind nicht statthaft!

Art.-29-Datenschutzgruppe

Volles Programm für 2006

Medizinische Daten, RFID, Daten von Kindern. So lauten einige der neuen Schwerpunkte, die im Arbeitsprogramm der Datenschutzgruppe nach Art. 29 besonders auffallen (siehe *http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp120_en.pdf*). Das Programm wurde erst Anfang April veröffentlicht, sodass seine Realisierung in das Jahr 2007 hinüberreichen dürfte.

Für die meisten kleineren und mittleren Unternehmen kaum relevant dürften dagegen die umfangreichen Arbeiten sein, die zum Thema „Grenzüberschreitender Datenverkehr“ (Transborder Data Flow) angekündigt sind. Solche Unternehmen werden meistens weiterhin auf der Basis der von der EU-Kommission veröffentlichten Formularverträge arbeiten.

Dr. Eugen Ehmann

IDACON 2006 – der INTEREST Kongress für Datenschutzbeauftragte

Wissen aus erster Hand

Auf der IDACON beschäftigen sich bekannte Experten wie Prof. Dr. Rainer W. Gerling, Dr. Eugen Ehmann oder Rolf Breidenbach mit den zentralen Datenschutz-Themen des Jahres. Neben rechtlichen Neuerungen wie Details zum Informationsfreiheitsgesetz erfahren die Teilnehmer unter anderem, welche Konsequenzen neue technische Entwicklungen für den Datenschutz haben werden.

Bereits zum sechsten Mal treffen sich im kommenden Herbst Datenschutzbeauftragte aus ganz Deutschland in Augsburg zur IDACON – dem Fachkongress zum Thema Datenschutz.

Kongress und Plenum – Teilnehmerwünsche werden erfüllt

Die Veranstaltung bietet nach einem „Baukastensystem" zusammenstellbare optionale Intensivseminare sowie einen zweitägigen Kongress, auf dem hochkarätige Dozenten referieren.

Teilnehmer zur IDACON 2005:

„Der Kongress hat aktuelle und brisante Themen umfasst. Diese wurden sehr prägnant, praxisbezogen erläutert und anschließend zur kurzen, aber gewinnbringenden Diskussion gestellt. Der praktische Nutzen der IDACON 2005 war für meine weitere Tätigkeit immens."

Florian Stein, PC-Ware AG, Leipzig

„Eine ideale Gelegenheit zum Austausch mit Fachleuten und Kollegen aus der Praxis, kombiniert mit aktuellen Themen aus dem vielseitigen Bereich des Datenschutzes wie Recht, Technik und täglicher Umsetzung. Sehr gute Veranstaltung!"

Tina Szories, Bertrandt AG, Ehningen

Das Programm richtet sich ganz nach den Wünschen der Teilnehmer, die im Vorfeld abgefragt wurden. Dies garantiert eine hohe Praxisrelevanz. Das komplette Programm finden Sie auf dem beiliegenden Fax.

Datenschutz im öffentlichen Bereich

Im ersten optionalen Intensivseminar beleuchtet Rolf Breidenbach die Aspekte des Datenschutzes im öffentlichen Bereich. Der Ministerialrat und Referatsleiter „Datenschutz und Akteneinsicht" beim Innenministerium des Landes Brandenburg spricht über das Informationsfreiheitsgesetz (IFG).

Er berichtet aus der Praxis des behördlichen Datenschutzbeauftragten und erläutert die praktische Relevanz des Informationsfreiheitsgesetzes, das Anfang des Jahres in Kraft getreten ist.

Ordnungswidrigkeiten im Datenschutz

Dr. Eugen Ehmann informiert in einem weiteren Intensivseminar, das die Teilnehmer zusätzlich buchen können, umfassend über Ordnungswidrigkeiten im Datenschutz. Besonders spannend wird sicherlich die Auswertung der Berichte der Aufsichtsbehörden. Datenschützer können hier exemplarisch sehen, worauf die Behörden besonders achten – und im eigenen Unternehmen vorbeugende Maßnahmen treffen.

Datensicherheit

Praxislösungen vermittelt auch Prof. Dr. Rainer W. Gerling. In seinem Seminar „Datensicherheit: aktuelle Entwicklungen in Technologie & Software" nimmt er Trends wie Biometrie, VoIP (Voice over IP = Internettelefonie) oder Firewall Piercing unter die Lupe. Dabei zeigt er den Teilnehmern die

Auf der IDACON erwarten Sie hochkarätige Experten und der informative Austausch mit Kollegen.

Gefahren und Einsatzmöglichkeiten in der Praxis auf.

Prof. Dr. Gerling ist selbst Datenschutzbeauftragter der Max-Planck-Gesellschaft in München. Daneben hat er eine Honorarprofessur für IT-Sicherheit an der FH München inne.

Datenschutz im medizinischen Bereich

Richtig brisant ist das Thema Datenschutz im medizinischen Bereich. TÜV-Akademie-Dozent Dirk-Michael Mülot richtet sein Seminar sehr stark an der täglichen Praxis in Kliniken aus.

So erfahren die Teilnehmer, wie sich Datenschutz trotz aller Widrigkeiten in das Tagesgeschäft eines Krankenhauses integrieren lässt. Dabei zeigt der Sachverständige für Datenschutz und Datensicherheit Wege zwischen Pflichtprogramm und „nice to have".

Experten unter Kollegen

Das einzigartige an diesem Kongress ist der intensive Austausch mit den Experten sowie mit Datenschutzkollegen.

Andrea Stickel

Datensicherheit mit TrueCrypt

Mit verschlüsselten Laufwerken sicher unterwegs

Die verschlüsselte Speicherung aller Worddokumente, Exceltabellen oder sonstigen Datendateien funktioniert erfahrungsgemäß nur, wenn sie automatisch ohne Zutun des Anwenders geschieht. Mit der kostenlosen Software TrueCrypt steht eine komfortable Open-Source-Anwendung zur Verfügung, die es erlaubt, unter Windows und Linux mit verschlüsselten Laufwerken zu arbeiten.

Gerade auf mobilen Datenträgern, die das Unternehmen verlassen, sollten personenbezogene und andere vertrauliche Daten so gespeichert werden, dass ein Verlust des Datenträgers keinen Schaden durch Kompromittierung der Daten verursacht.

Solche Datenträger sind Festplatten in Notebooks, aber auch Disketten, USB-Sticks, USB-Festplatten, CDs oder DVDs. Hier hilft nur eine konsequente Verschlüsselung.

Mit TrueCrypt bequem verschlüsselte Laufwerke erstellen

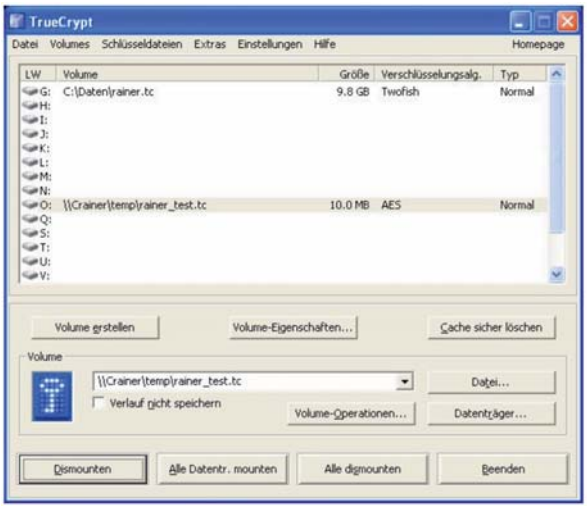
Mit TrueCrypt lässt sich ein Laufwerk über eine Container-Datei oder eine eigene Partition erstellen. Die Partition z.B. eines USB-Sticks kann so komplett verschlüsselt werden. Container-Dateien lassen sich beliebig kopieren und transportieren. Sie dürfen auf Netzwerklaufwerken liegen und können auf CD/DVD gebrannt werden.

Ohne Passwort kein Zugang

Zugang zum Laufwerk verschafft ein Passwort, eine Schlüsseldatei oder eine Kombination aus beiden. Als Schlüsseldatei kann jede Datei fungieren. Sie wird nicht verändert, sondern ihr Bitmuster wird lediglich mit dem Passwort vermischt. Ist die Schlüsseldatei defekt, ist das verschlüsselte Laufwerk nicht mehr zugänglich.

Für Reisende ist die Verschlüsselung ohne Installation sehr praktisch

TrueCrypt unterstützt einen Traveller-Mode, um verschlüsselte Datenträger zu benutzen, ohne die Software zu installieren. Prinzipbedingt benötigt der User hierfür Administratorprivilegien, da er vorübergehend einen Treiber ins System bringen muss.



Das Hauptfenster von TrueCrypt 4.2. Hier werden Laufwerke erstellt, angemeldet und wieder abgemeldet.

Über einen Menüpunkt lässt sich eine Traveller-Disk erstellen. Sie enthält alles, was zum Umgang mit verschlüsselten Laufwerken nötig ist (ca. 1,6 MB). Soweit vom Betriebssystem unterstützt, lässt sich über den Autostart-Mechanismus das Laufwerk sogar automatisch beim Einlegen des Datenträgers starten.

Verbesserungspotenzial bei der Nutzung unter Linux und bei Chipkarten

Das aktuelle TrueCrypt unterstützt Windows 2000, Windows XP, Windows 2003 Server und Linux ab Kernel 2.6.5. Ab Version 4.2 können nun auch endlich unter Linux verschlüsselte Laufwerke erstellt werden. Lediglich ein GUI fehlt noch für Linux.

Während beim Wechsel in den Ruhezustand alle angemeldeten Laufwerke automatisch abgemeldet werden können, müssen bei der Wiederanmeldung aus dem Ruhezustand die Laufwerke explizit wieder angemeldet werden.

Auch gibt es bislang keinen Support für Chipkarten.

Bewertung des Tools

Truecrypt ist ein erstklassiges und kostenloses Werkzeug, um auf Notebooks Daten verschlüsselt zu speichern. Dabei sind eine Programmpartition und eine verschlüsselte Datenpartition sicherlich die beste Lösung. Eine sorgfältige Planung des Einsatzes schützt vor Datenverlust durch vergessene Passwörter.

Sie können dieses Tool unter *www.datenschuetzer.de* herunterladen oder unter *www.truecrypt.org*.

Das Tool ist nicht für den Unternehmenseinsatz geeignet, aber z.B. für den Außendienstler mit Notebook

Die Zielgruppe ist eindeutig der Endanwender. Deshalb fehlen viele der ausgefeilten Unternehmens-Funktionalitäten anderer Produkte, wie z.B. Daten-Recovery-Unterstützung, falls der Mitarbeiter sein Passwort vergisst. Hier hilft nur ein rechtzeitiges Backup.

Prof. Dr. Rainer W. Gerling

Datenklau durch Pharming

Vom Fischer zum Farmer

Mit immer neuen Tricks versuchen Betrüger, über das Internet Passwörter, PINs, TANs und ähnlich sensible Daten auszuspionieren. Dabei werden in der Regel Angriffsarten wie Phishing eingesetzt. In letzter Zeit mehren sich so genannte Pharming-Attacken. Doch auch davor können Sie sich schützen.

Pharming – häufig auch als DNS-Spoofing bezeichnet – ist eine Weiterentwicklung des Phishing.

Ziel beider Angriffsarten ist es, die Nutzeranfragen auf fremde Webserver umzuleiten, die die Angreifer kontrollieren. Beim Phishing versuchen Betrüger, die Gutgläubigkeit von Usern auszunutzen, indem diese mittels Mail aufgefordert werden, eine bestimmte Internetseite aufzusuchen und dort sensible Informationen einzugeben.

Beim Pharming manipulieren die Betrüger dagegen eine IP-Adresse, mit deren Hilfe eine dazugehörige Internetadresse aufgerufen wird.

Betrüger arbeiten mit „Serverfarmen“

Der Begriff Pharming rührt daher, dass die Täter große Serverfarmen unterhalten, auf denen gefälschte Kopien bestehender Webseiten abgelegt sind.

So funktioniert der Betrug mit gefälschten Internetadressen

Beim Pharming werden Internetadressen gefälscht. Der Internetbetrüger ändert dazu auf einem DNS-Server oder in der lokalen Datei „hosts“ eine vorhandene IP-Adresse, die einem realen Namen (Domäne) zugeordnet ist. Die neue IP-Adresse ist dann diejenige einer gefälschten Seite, während der Name dieser Adresse unverändert bleibt.

Tippt nun das Opfer in seinem Browser den (richtigen) Namen der gefälschten Adresse ein, wird die Anfrage statt auf den Original-Server auf einen vom Betrüger betriebenen Rechner umgeleitet, ohne dass dies der Nutzer bemerkt.

Vorsicht bei der Eingabe von PIN, TAN und anderen sensiblen Daten

Gibt der Benutzer auf dieser falschen Seite nun z.B. Kreditkartennummern oder Kontodaten ein, um etwa einen fiktiven Kauf abzuschließen oder Online-Banking zu betreiben, so fallen diese sensiblen Daten in die Hände des Betrügers – und der kann sie für seine Zwecke benutzen.

Eine Firewall und aktuelle Antivirenprogramme sind absolutes Muss

Auch wenn Pharming-Angriffe nur schwer erkennbar sind, gibt es doch eine Reihe von Vorsichtsmaßnahmen, um einen Angriff zu verhindern.

So kann eine Firewall das Eindringen eines Täters und damit eine Änderung der IP-Adressen zumindest erschweren. Gegen entsprechende Manipulationsversuche eines Trojanischen Pferds hilft ein Antivirenprogramm, das regelmäßig aktualisiert wird.

Nutzen Sie nur sichere Verbindungen

Werden über das Web Einkäufe oder Bankgeschäfte getätigt, dann sollte dies über eine sichere (SSL-)Verbindung erfolgen. Ob dies der Fall ist, können Sie z.B. daran erkennen, dass die Adresse des Zielservers mit dem Präfix https:// statt http:// beginnt.

Achten Sie auf die Vertrauenswürdigkeit des Zertifikats

Sollen Daten mittels https übertragen werden, muss sich dazu der aufgerufene Server mit einem Zertifikat authentifizieren. Wer das Zertifikat herausgegeben hat bzw. ob der Herausgeber vertrauenswürdig ist, lässt sich bei einer Überprüfung des Zertifikats feststellen. Diese Überprüfung kann jeder User selbst durchführen, indem er auf das am unteren Rand eines Browserfensters erkennbare Symbol eines Vorhängeschlosses klickt.

Sensibilisieren Sie die Benutzer

Häufig werden aber die vom eigenen Browser ausgegebenen Warnungen bezüglich eines – unbekannten oder abgelaufenen – Zertifikats vom Nutzer ignoriert. Hier hilft nur, die User zu informieren, in welche Fallen sie damit unter Umständen tappen.

Udo Höhn

Udo Höhn ist Referent im Sachgebiet „Technik und Organisation“ beim Bayerischen Landesbeauftragten für den Datenschutz.

Von IP-Adressen und DNS-Servern

Jeder Rechner im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse (z.B. 123.123.123.123). Damit ein Anwender sich nicht diese Zahlenfolge zum Aufruf einer Webseite merken muss, kann er stattdessen auch den Namen dieser Adresse eingeben (z.B. *www.interest.de).*

Um diesen Namen wiederum in die entsprechende IP-Adresse umzuwandeln, kann ein Rechner automatisch so genannte DNS-Server (Domain Name System) aufsuchen, die die Domainnamen in IP-Adressen auflösen.

Außerdem besitzt jeder Rechner eine eigene Datei namens „hosts“, die tabellenartig die am häufigsten genutzten IP-Adressen aufführt. Diese Datei wird bei einem Seitenaufruf zunächst dahingehend durchsucht, ob in ihr der Name und die zugehörige Internetadresse schon aufgeführt sind. Falls ja, erübrigt sich die Kontaktierung eines DNS-Servers.

Die Gestaltung von Einverständniserklärungen

Der Kunde – extrem schutzbedürftig oder souverän?

Vor Gericht und auf See bist du in Gottes Hand. Dass dieser volkstümliche Spruch manchmal mehr als nur ein Körnchen Wahrheit enthält, mussten vor kurzem der Payback-Rabattverein und die im Düsseldorfer Kreis zusammengeschlossenen Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft erfahren. Das Landgericht München I kassierte nämlich eine Einwilligungsklausel, auf die sich der Verein und der Düsseldorfer Kreis in einem langwierigen Abstimmungsverfahren geeinigt hatten.

Die Payback-Karte gibt es seit dem Jahr 2000. Wie sie datenschutzrechtlich zu beurteilen ist, war dabei schon vom ersten Tag an umstritten.

Vor allem die Einverständniserklärung war Stein des Anstoßes

Schon am 1. Februar 2001 erklärte das Landgericht München I die damals verwendete Einverständniserklärung für rechtswidrig (Urteil unter *www.jurpc.de/rechtspr/20010117.htm)*.

Payback suchte zusammen mit den Aufsichtsbehörden eine Lösung

In der Folgezeit trat der Payback-Verein, der von interessierten Unternehmen getragen wird, in Gespräche mit den deutschen Datenschutzaufsichtsbehörden ein. Rechtlich maßgebend war dabei nur die Haltung der bayerischen Datenschutzaufsicht, da der Verein seinen Sitz in München hat.

Das Abstimmungsgremium der Aufsichten ist der Düsseldorfer Kreis

Da Payback inzwischen über 30 Millionen Rabattkarten ausgegeben hat und bundesweite Bedeutung besitzt, kam es allerdings zu einem Gedankenaustausch zwischen allen deutschen Datenschutzaufsichtsbehörden, die für die Privatwirtschaft zuständig sind.

Das Forum hierfür ist seit nunmehr fast 30 Jahren der „Düsseldorfer Kreis“, ein gesetzlich nicht geregeltes Gremium, in dem sich die Aufsichtsbehörden bei grundlegenden Fragen abstimmen. Ziel der Gespräche in diesem Gremium ist es, unterschiedliche Handhabungen bei den einzelnen Aufsichtsbehörden zu vermeiden.

Beim Einkaufen Rabattpunkte zu sammeln, ist äußerst beliebt. Über 30 Millionen Payback-Karten sind mittlerweile bundesweit im Umlauf.

Payback sammelt Daten für personalisierte, gezielte Werbung beim Kunden

Ziel des Payback-Systems ist, Daten aus konkreten einzelnen Transaktionen wie etwa Käufen, bei denen der Kunde die Rabattkarte vorlegt, für persönlich adressierte Werbung sowie für Zwecke der Marktforschung zu verwenden.

Dazu bedarf es – darüber besteht vom Grundsatz her keinerlei Streit – einer Einwilligung des Betroffenen.

Was, wenn der Payback-Kunde seine Daten nicht weitergegeben sehen will?

Was ist nun, wenn der Kunde zwar eine Rabattkarte möchte, aber weder Werbung erhalten will noch damit einverstanden ist, dass seine Daten für Marktforschung verwendet werden?

Seit 2005 wählte Payback diesen Weg:

- Wenn der Kunde eine Rabattkarte will, muss er einen entsprechenden Antrag ausfüllen.
- In diesen Antrag „eingebaut“ ist eine Einverständniserklärung.
- In ihr ist im Einzelnen dargestellt, wer welche Daten über ihn für Werbung und Marktforschung erhalten darf.
- Der Antrag ist insgesamt am Ende zu unterschreiben. Eine gesonderte Unterschrift unter die Einwilligungsklausel ist nicht vorgesehen.
- Unterschreibt der Interessent den Antrag und tut ansonsten nichts, ist damit die Einwilligung erteilt.
- Will er dagegen vermeiden, dass seine Daten für Werbung oder Marktforschung verwendet werden, kann er ein Kästchen im Antragstext ankreuzen, neben dem folgender Text steht: „Hier ankreuzen, falls die Einwilligung nicht erteilt wird.“

Der Düsseldorfer Kreis stimmte dieser geänderten Einverständnisklausel zu

Mit dieser Ausgestaltung waren sowohl die bayerische Datenschutzaufsicht als auch die anderen im Düsseldorfer Kreis vertretenen Aufsichtsbehörden einverstanden. Damit konnte der Payback-Verein davon ausgehen, dass diese Lösung allgemein mitgetragen wird.

Opt-In contra Opt-Out

Worin besteht nun die rechtliche Besonderheit und damit allerdings auch zugleich die rechtliche Tücke dieser Ausgestaltung einer Einwilligung?

Dies lässt sich an dem Begriffspaar Opt-In und Opt-Out festmachen:

- Opt-In bedeutet, dass eine Einwilligung durch ausdrückliches aktives Handeln erteilt wird. Diese Variante läge vor, wenn die Einwilligung erst dadurch erteilt würde, dass der Interessent dafür ein Kästchen ankreuzen müsste. Tut er es dagegen nicht – gleich, ob bewusst oder nicht –, liegt keine Einwilligung vor.
- Bei einer Opt-Out-Lösung gilt dagegen eine Einwilligung als erteilt, es sei denn, der Kunde erklärt sich ausdrücklich dagegen.

Im vorliegenden Fall haben wir es mit einer Variante des Opt-Out zu tun. Sobald der Kunde den Antrag insgesamt unterschreibt, gilt die Einwilligung als erteilt. Entspricht das nicht seinem Willen, muss er aktiv werden und ankreuzen, dass er nicht einwilligen will.

Payback tendiert zu Opt-Out, um an so viele Daten wie möglich zu kommen

Der Grund dafür liegt auf der Hand. Payback möchte viele Einwilligungen erhalten, damit es möglichst viele Daten vermarkten kann. Daran ist an sich nichts Verwerfliches. Allerdings stellt sich die Frage, womit der Kunde rechnen muss und womit nicht.

Payback vermutet, dass der „typische Kunde" einwilligen möchte, und will ihm das möglichst einfach machen. Wahrscheinlich trifft die Sicht von Payback sogar zu.

Viele Kunden sehen den Deal „Daten gegen Rabatt" als unkritisch an

Es ist erstaunlich, wie unwichtig vielen Kunden die eigenen Daten sind. Und vielen wird tatsächlich klar sein, dass kaum jemand einfach etwas nur verschenkt. Diese Kunden empfinden – wenn es sie überhaupt interessiert – die Nutzung ihrer Daten für die Werbung als etwas, womit sie die Rabattkarte quasi bezahlen.

Das Landgericht München I will vom Opt-Out jedoch nichts wissen

Das Landgericht folgt diesen Überlegungen allerdings nicht (siehe *www.justiz.bayern.de/lgmuenchen1/presse/presse1.html)*. Auf die Klage eines Verbrauchervereins erklärte es das Kernstück der Einwilligungsklausel für unwirksam. Dabei störten das Gericht vor allem folgende Punkte:

- Die Einwilligung beruht nicht auf der freien Entscheidung des Kunden, wie es § 4a Abs. 1 Satz 1 BDSG fordert. Denn die Einwilligung gilt auch dann als erklärt, wenn der Kunde die Möglichkeit des „Auskreuzens" schlicht übersehen hat.
- Dass er das Kästchen hätte ankreuzen können, ändert daran nichts. Wenn der Kunde die Wahlmöglichkeit gar nicht erkennt, beruht seine Einwilligung nicht auf einer freien Entscheidung.
- Damit, dass er in eine Verwendung von Daten für Werbezwecke einwilligt, muss er nicht rechnen. Denn ihm geht es nur um eine Rabattkarte.
- Durch die Ausgestaltung der Klausel wird der Kunde unter Druck gesetzt. Für ihn wirkt es so, als sei die Einwilligung der Regelfall und das Versagen der Einwilligung die Ausnahme. Nach dem BDSG verhält es sich jedoch gerade umgekehrt.

Das Menschenbild wird entscheiden

Geht man davon aus, dass das Gesetz vor allem den unaufmerksamen, unbeholfenen Kunden schützen soll, wird man der Entscheidung zustimmen. Man kann es aber auch anders sehen. Wer unterschreibt, ist sich in der Regel darüber im Klaren, dass damit etwas rechtlich Relevantes erreicht werden soll. Dann aber liegt es an ihm, den unterschriebenen Text auch zu lesen.

Das Verfahren geht in die nächste Instanz. Dort wird entschieden, welcher Sichtweise der Vorrang gebührt.

Das Ergebnis ist für viele relevant

Das Ergebnis ist für alle Unternehmen wesentlich, die Einwilligungen von Kunden einholen. Deshalb reicht die Bedeutung des Verfahrens weit über Rabattkartensysteme hinaus.

Dr. Eugen Ehmann

IMPRESSUM Datenschutz PRAXIS

Verlag:
WEKA MEDIA GmbH & Co. KG
Geschäftsbereich INTEREST
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-94 92
Telefax: 0 82 33.23-74 00
www.interest.de

Herausgeber:
WEKA MEDIA GmbH & Co. KG
Gesellschafter der WEKA MEDIA GmbH & Co. KG
sind als Kommanditistin:
WEKA Business Information GmbH & Co. KG
und als Komplementärin:
WEKA MEDIA Beteiligungs-GmbH

Geschäftsführer:
Lutz Bandte, Niklas Friedrichsen, Werner Müller, Werner Pehland

Redaktionsleitung:
Lutz Wehner

Chefredakteur:
Raphael Stange (V.i.S.d.P.)

Redaktion:
Dr. Andrea Brill, Andrea Stickel, Ricarda Veidt, M.A.
E-Mail: datenschutzpraxis@interest.de

Vertrieb:
Andreas Thull
E-Mail: andreas.thull@interest.de

Erscheinungsweise:
Zwölfmal pro Jahr

Aboverwaltung:
Telefon: 0 82 33.23-94 92
Telefax: 0 82 33.23-74 20
E-Mail: service@interest.de

Abonnementpreis:
12 Ausgaben 98,00 € (zzgl. MwSt.)
Einzelheft 9,00 € (zzgl. MwSt.)

Druck:
Geiselmann Printkommunikation GmbHLeonhardstr. 23
88471 Laupheim

Layout & Satz:
Melanie Takke

Bestell-Nr.
909228

ISSN-Nr.
1614-6867

Bestellung unter:
Telefon: 0 82 33.23-94 92
Telefax: 0 82 33.23-74 20
www.datenschuetzer.de

Haftung:
Die WEKA MEDIA GmbH & Co. KG ist bemüht, ihre Produkte jeweils nach neuesten Erkenntnissen zu erstellen. Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Bei Nichtlieferung durch höhere Gewalt, Streik oder Aussperrung besteht kein Anspruch auf Ersatz. Erfüllungsort und Gerichtsstand ist Kissing.

Neu im Juli:

Das Anonymisierungs-Tool JAP

Gefahr im Verzug

Die Universität Dresden und das Unabhängige Landeszentrum für Datenschutz stellen mit dem Anonymisierungs-Tool JAP ein allgemein anerkanntes Datenschutz-Tool zur Verfügung. Es dient der Wahrung der Privatsphäre im Internet.

Beschäftigte können es aber auch dazu benutzen, Sicherheitseinstellungen auf der Firewall des Unternehmens zu unterlaufen. Sollten Sie das Tool deshalb im Unternehmen besser verbieten?

Automatische Sprachnachrichten

Vielen Dank – schon zuviel gehört!

Da viele Kunden Briefpost kaum noch lesen, greifen Unternehmen immer mehr zu automatisch generierten Sprachnachrichten, um ihre Kunden z.B. über Liefertermine zu informieren oder anzumahnen. Was aber, wenn ein Dritter die Nachricht in Empfang nimmt?

Dr. Ehmann beschäftigt sich mit dieser ganz neuen Problematik, zu der es weder Urteile noch Beschlüsse von Datenschutzgremien gibt.

Spielregeln für Auskunftsersuchen

Gute Aussichten für die Dateneinsicht

Das Auskunftsrecht ist ein Grundpfeiler des Datenschutzrechts und wesentliche Voraussetzung für den Löschungs- und Berichtigungsanspruch von Betroffenen.

Immer wieder werden Sie als Datenschutzbeauftragter mit Auskunftsersuchen von Betroffenen konfrontiert. Lesen Sie, wie Sie ohne großen Aufwand solche Auskunftsersuchen handhaben.

Datenschutz-Begriff des Monats

Sensitive Daten

Sensitive Daten sind besonders schutzbedürftige Daten, die Rückschlüsse auf die Privat- und Intimsphäre einer Person zulassen. Das BDSG sieht für diese Daten besondere Regelungen vor.

Freiwillige Einwilligung erforderlich

In der Regel setzt die Erhebung und Verwendung die freiwillige Einwilligung der betroffenen Person voraus.

Sensitive Daten sind Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit des Betroffenen hervorgeht, sowie Angaben zur Gesundheit oder zum Sexualleben.

Schlussfolgerung, Wahrscheinlichkeit oder willkürliche Zuordnung genügen für eine Einordnung als „sensitiv“

Es genügt,

- dass Daten den Schluss auf Informationen dieser Art zulassen. Wenn sich beispielsweise eine Person an einem Gewinnspiel eines Blutzuckermessgeräteherstellers beteiligt, so gibt sie damit die sensitive Information weiter, dass es sich bei ihr um eine Person mit einer Blutzuckererkrankung handelt.
- dass die Eigenschaft der betreffenden Person wahrscheinlich zuzuordnen ist. Wenn jemand etwa bestimmte politische Bücher bestellt, enthält die Bestellung die wahrscheinliche sensitive Information, dass der Betroffene eine bestimmte politische Meinung hat.
- dass die betreffende Person nach einer Einschätzung des Unternehmens einer Gruppe zugeordnet wird, die das betreffende sensitive Datum aufweist. Bildet ein Marktforschungsunternehmen aus den Bewohnern eines bestimmten Stadtbezirks eine Gruppe, stellt fest, dass diese Bewohner typischerweise Ausländer sind, und ordnet die betreffende Person dieser Gruppe zu, so schlägt die Bewertung der Gruppe auf die Person als deren Datum durch.

Der Datenschutz-Begriff des Monats ist entnommen aus dem Datenschutz-Glossar von INTEREST. Mehr Informationen dazu finden Sie unter *www.interest.de/produkte/1921.html.*

Dr. Philipp Kramer