HELBING
Kanzlei für IT- und Datenschutzrecht

BIG DATA UND BUSINESS INTELLIGENCE

Anforderungen des Datenschutzrechts kennen und beachten

Rechtsanwaltskanzlei
Dr. Thomas Helbing

www.thomashelbing.com

Königinstraße 11a
80539 München

T +49 (0) 89 - 28 72 465-28
E helbing@thomashelbing.com

USt.-IdNr. DE815182912

EINLEITUNG

Für 89 Prozent der Unternehmen sind juristische Fragen zum Datenschutz ein wesentliches Problem bei der Planung von Big Data und Business Analytics [7]. Im folgenden Beitrag erhalten Sie einen fundierten, praxisnahen Einblick in das hierfür relevante Datenschutzrecht.

Sie erfahren welche datenschutzrechtlichen Anforderungen für Big Data und Business Analytics gelten und wie Sie Daten in Ihrem Projekt rechtskonform verwenden.

Der Beitrag entspricht dem von mir verfassten Kapitel in dem bald erscheinenden "Handbuch Business Intelligence - Potenziale, Strategien und Best Practices", Hrsg.: Michael Lang, ISBN 978-3-86329-660-5.

München, im November 2015

Dr. Thomas Helbing
Rechtsanwalt

DEN KOPF NICHT IN DEN SAND STECKEN

Verstöße gegen den Datenschutz können mit Bußgeldern bis 300.000 Euro geahndet werden, in bestimmten Fällen drohen sogar Haftstrafen. Der Sanktionsrahmen dürfte zudem bald ausgeweitet werden. Noch schwerer wiegt häufig der öffentliche Imageschaden bei Datenschutzverletzungen. Das Thema Datenschutz außen vor zu lassen ist also keine Lösung.

WOZU DIENT DAS DATENSCHUTZRECHT?

Das Datenschutzrecht legt fest, unter welchen Voraussetzungen personenbezogene Daten verwendet werden dürfen.

Wer »Datenschutz« hört, denkt oft an Verschlüsselung, Firewalls und andere technische Aspekte. Tatsächlich regelt das Bundesdatenschutzgesetz aber nur in einem einzigen Paragrafen und einem kurzen Anhang die Datensicherheit, und das sehr rudimentär. Die Datensicherheit ist nur ein kleiner Teilaspekt des Datenschutzes. Die gesetzlichen Bestimmungen sollen nicht die Daten, sondern die Menschen schützen, nämlich vor einer »Verdatung«.

Das Bundesverfassungsgericht hat dazu entschieden, dass das Persönlichkeitsrecht auch ein »Recht auf informationelle Selbstbestimmung« beinhaltet. Dieses gibt dem Einzelnen die Befugnis, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Das mag sich alles etwas hochtrabend anhören. Verdeutlichen kann man sich das Ganze an einem anderen Teil des Persönlichkeitsrechts: am Recht am eigenen Bild. So wie es unzulässig ist, Menschen zu filmen und dieses Filmmaterial öffentlich beliebig verfügbar zu machen, so sind auch dem Sammeln und Verwenden anderer Informationen über Menschen rechtliche Grenzen gesetzt.

Personenbezogen, nicht persönlich

In Deutschland finden sich die wichtigsten Bestimmungen zu personenbezogenen Daten im Bundesdatenschutzgesetz (BDSG). Dieses Gesetz ist immer dann zu beachten, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Wie wir gleich sehen werden, ist der Anwendungsbereich sehr weit. Personenbezogene Daten sind »alle Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person« (§ 3 BDSG). Auf die Sensibilität der Daten kommt es nicht an. Die Information, dass Hubert Müller dieses Buch gekauft hat oder bei der ABC GmbH arbeitet, ist also bereits ein personenbezogenes Datum. Es geht eben nicht nur um »persönliche« Daten, sondern um alle personenbezogenen oder -beziehbaren Informationen. Gerade im Bereich Business Intelligence und Big Data werden Datenschutzanforderungen häufig zu schnell beiseitegeschoben, weil fälschlicherweise davon ausgegangen wird, es seien keine personenbezogenen Daten im Spiel. Dazu später mehr.

Haben wir es mit personenbezogenen Daten zu tun, so unterliegt faktisch jeder Umgang damit den Datenschutzgesetzen. Insbesondere zählen dazu das Speichern, Erfassen, Aufnehmen oder Aufbewahren, das Verändern, das Übermitteln oder Zugriffgewähren, das Sperren und das Löschen sowie das Auswerten oder sonstige Nutzen der Daten. Ausnahmen bestehen im familiären und privaten Bereich sowie dann, wenn die Daten nicht elektronisch verarbeitet werden. Bei Business Intelligence sind diese Ausnahmen aber bedeutungslos.

Grundsätzlich ist erst einmal alles verboten

Der Umgang mit personenbezogenen Daten ist aus Business-Intelligence- und Big-Data-Sicht streng geregelt: Alles ist verboten, außer es ist erlaubt. In Juristendeutsch gesprochen: Es gilt ein »Verbot mit Erlaubnisvorbehalt«.

Bei einem Business-Intelligence-Projekt stellt sich also nicht die Frage: »Verbietet uns das Datenschutzrecht das?«, sondern man muss sich überlegen: »Ist das überhaupt erlaubt?« Unternehmen, die personenbezogene Daten sammeln und auswerten wollen, stehen damit

stets unter einem juristischen Rechtfertigungsdruck.

Das Mantra des Datenschutzes lautet: »Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn eine Erlaubnisnorm dies gestattet oder die Einwilligung der Betroffenen vorliegt« (§ 4 Abs. 1 BDSG). Da es an der Einwilligung der Betroffenen zur Datenauswertung quasi immer fehlt und die gesetzlichen Anforderungen an wirksame Einwilligungen hoch sind, helfen Einwilligungen bei Business-Intelligence-Analysen meist nicht weiter. Damit bleibt nur die Suche nach einer gesetzlichen Erlaubnisnorm. Glücklicherweise gibt es davon eine ganze Reihe. Unglücklicherweise sind sie gut versteckt und äußert vage.

Um herauszufinden, ob die Verwendung personenbezogener Daten zulässig ist, hilft die Lektüre des Gesetzes wenig. Erst durch Kenntnis der Fachliteratur und Stellungnahmen von Datenschutzbehörden erschließt sich, was die Bestimmungen erlauben und was nicht. Leider ist dies immer wieder Grund und Anlass, Datenschutzgesetze nach Gutdünken und oft auch falsch zu interpretieren, sowohl im positiven wie im negativen Sinn. Datenschutzrechtliche Fragen sind nichts, was ein IT-Verantwortlicher oder Projektmanager nebenbei beantworten kann. Dafür bedarf es spezialisierter Experten.

Im Unterschied zu anderen Rechtsbereichen kennt das Datenschutzrecht nur wenige Urteile und kaum höchstrichterliche Rechtsprechung. Selbst fundamentale Fragen sind nach Jahrzehnten noch nicht von den obersten Gerichten entschieden. Das liegt daran, dass Betroffene wenig Motivation haben, ihre Rechte kostspielig vor Gerichten durchzusetzen. Zudem werden viele Beschwerden und Streitigkeiten mit den Aufsichtsbehörden außergerichtlich und für die Öffentlichkeit intransparent aus der Welt geschafft.

Weitere Anforderungen des Datenschutzrechts

Neben dem »Verbot mit Erlaubnisvorbehalt« enthält das Datenschutzrecht noch weitere Vorgaben. So muss dem Betroffenen klar sein, wer welche Daten zu welchem Zweck verarbeitet (Transparenz). Auch dürfen nicht mehr Daten erhoben werden, als für den konkreten Zweck benötigt werden, und nicht mehr benötigte Daten sind zu löschen (Datensparsamkeit). Personenbezogene Daten sind zudem grundsätzlich bei den Betroffenen selbst, also beim Mitarbeiter oder beim Kunden, zu erheben und nicht über Drittquellen (Direkterhebungsgrundsatz). Personenbezogene Daten dürfen nur für spezifische, im Voraus festgelegte Zwecke verwendet werden. Eine spätere Verwendung für einen anderen Zweck ist nur zulässig, wenn dieser mit dem ursprünglichen vereinbar ist (Zweckbindungsgrundsatz). Gerade diese Zweckbindung kann eine Hürde bei Business-Intelligence-Projekten darstellen, weil die Daten ursprünglich nicht zu Auswertungszwecken erhoben wurden. Dazu später mehr.

Sonderregelungen gelten zudem, wenn personenbezogene Daten in Länder außerhalb der Europäischen Union und des Europäischen Wirtschaftraums übertragen werden oder wenn IT-Dienstleister Daten im Auftrag eines Unternehmens speichern, auswerten oder verwenden. In letzterem Fall müssen besondere Vereinbarungen mit dem beauftragten Unternehmen geschlossen werden, sogenannte Auftragsdatenverarbeitungsverträge (§ 11 BDSG). Dies gilt zum Beispiel für Big-Data- oder Business-Intelligence-Anwendungen aus der Cloud (»as a service«). Bereits die bloße Nutzung von Speicherplatz oder Rechenleistung aus der Cloud machen nach deutschem Recht Spezialverträge erforderlich, auf die manche ausländischen Anbieter nicht eingestellt sind.

Daneben gibt es Spezialregelungen, etwa für Gesundheitsdaten, im Onlinebereich, bei Verbindungsdaten in der Telekommunikation oder bei Standortdaten. Auf einige für Business Intelligence und Big Data besonders relevante Bereiche gehe ich später noch ein.

Unternehmen in Deutschland, in denen regelmäßig zehn oder mehr Mitarbeiter mit personenbezogenen Daten umgehen, benötigen einen Datenschutzbeauftragten. Dieser ist bei Business-Intelligence-Auswertungen frühzeitig einzubinden. Das ist keine Höflichkeit,

sondern gesetzlich vorgeschrieben (§ 4g Abs. 2 BDSG). Die Einbindung ist wichtig, damit Datenschutzbelange rechtzeitig berücksichtigt werden können. Sonst könnte die mühsam aufgesetzte Business Intelligence am Ende an Datenschutzproblemen scheitern oder aufwendig und kostspielig geändert werden müssen.

DATENSCHUTZ GOES GLOBAL – DEUTSCHLAND, EUROPA UND DIE WELT

Es gibt zurzeit kein einheitliches europäisches Datenschutzrecht. Auf europäischer Ebene existieren jedoch zahlreiche Richtlinien, die datenschutzrechtliche Vorgaben enthalten. Diese Richtlinien sind nur für die Mitgliedstaaten und nicht für Unternehmen und Bürger in der EU verbindlich. Sie geben den Ländern in der EU vor, wie deren Bestimmungen zum Schutz personenbezogener Daten auszusehen haben. Die Länder setzen die Vorgaben durch nationale Gesetze um. Wer also wissen will, was in Spanien oder Frankreich gilt, muss in die dortigen Datenschutzgesetze sehen, nicht in die EU-Richtlinien.

Durch die EU-Richtlinien wurde das Datenschutzrecht aber harmonisiert: Die Datenschutzgesetze innerhalb der EU sind einander sehr ähnlich. Ähnlich – aber eben nicht gleich. Bei der Umsetzung haben die einzelnen Länder nämlich gewisse Spielräume genutzt. Außerdem legen die Mitgliedstaaten und deren Datenschutzbehörden die Vorgaben unterschiedlich aus. In Deutschland kommt hinzu, dass es zwar nur ein Datenschutzgesetz gibt, jedes Bundesland aber seine eigene Aufsichtsbehörde hat. Insofern gibt es auch innerhalb Deutschlands Unterschiede bei der Auslegung der nationalen Vorschriften, was die Situation gerade für Konzerne mit mehreren Gesellschaften in unterschiedlichen Bundesländern erschwert. Immerhin haben die Behörden Gremien gebildet, um sich abzustimmen. Auf EU-Ebene ist das die Artikel-29-Arbeitsgruppe. In Deutschland setzen sich die Aufsichtsbehörden regelmäßig im sogenannten Düsseldorfer Kreis zusammen.

Um das vermeintlich in die Jahre gekommene Datenschutzrecht zu modernisieren und weiter zu vereinheitlichen, will man das Recht reformieren und eine EU-Datenschutz-Grundverordnung erlassen. Eine EU-Verordnung ist im Gegensatz zu einer Richtlinie unmittelbar in den Mitgliedstaaten gültig; sie bedarf keiner Umsetzung durch nationale Gesetze. Europa hätte dann einen einheitlichen Gesetzestext für den Datenschutz. Als dieser Beitrag verfasst wurde (September 2015), lagen ein Entwurf für eine Datenschutz-Grundverordnung der EU-Kommission vom 25. Januar 2012, ein Entwurf des EU-Parlaments vom 12. März 2014 und ein Beschluss des Rates der Europäischen Union vom 15. Juni 2015 vor (Links zu den Texten finden Sie unter [1]). Unmittelbar im Anschluss hat der Einigungsprozess zwischen Rat, Parlament und Kommission begonnen, der sogenannte Trilog. Dieser dauert noch an und könnte im besten Fall Ende 2015 ein erfolgreiches Ende finden. Da der Entwurf eine zweijährige Übergangsfrist vorsieht, würde das neue Recht jedenfalls frühestens ab Anfang 2018 gelten. Für die schnelllebige IT-Branche ist das eine Ewigkeit.

Die Datenschutz-Grundverordnung hat sich als schwieriges Projekt erwiesen. Kaum eine andere EU-Norm stand unter ähnlichem Beschuss von Lobbyisten wie das neue Datenschutzregelwerk. Und auch zwischen den EU-Mitgliedstaaten besteht Uneinigkeit. Hauptstreitpunkte unter den Politikern im Rat sind derzeit die Regeln für den Datenexport aus der EU in Drittländer und die Zuständigkeit der nationalen Aufsichtsbehörden in Fällen, die mehrere Mitgliedstaaten betreffen.

Kommt die Datenschutz-Grundverordnung, dürfte sich einiges ändern. Die Grundsäulen bleiben jedoch bestehen. Ich gehe an geeigneter Stelle auf das geplante Regelwerk ein.

Außerhalb Europas haben sich einzelne Länder an der EU-Richtlinie orientiert, andere haben gar kein Datenschutzecht oder nur für bestimmte Sektoren Vorschriften erlassen.

PERSONENBEZOGEN ODER NICHT?

Die Vorgaben der Datenschutzgesetze gelten nur bei personenbezogenen Daten. Können Daten keiner Person zugeordnet werden, unterliegen sie nicht den Beschränkungen des Datenschutzrechts. Wichtig: Bereits die Personenbeziehbarkeit genügt, um die datenschutzrechtlichen Vorschriften zur Anwendung kommen zu lassen. Ein Datensatz, der keinen Namen enthält, ist ein personenbezogenes Datum, wenn man die Informationen einer einzelnen Person zuordnen kann. Ein Logfile mit Nutzerkennungen und Log-in-Zeiten ist zum Beispiel personenbezogen, wenn man die Nutzerkennungen einem Namen zuordnen kann.

Doch wann können Daten einer individuellen Person zugeordnet werden? Hierüber ist eine ebenso lebhafte wie verwirrende Diskussion entstanden. Im Wesentlichen geht es um zwei Fragen:

Zum einen ist unklar, was alles bei der Frage zu berücksichtigen ist, ob die Daten einer bestimmten Person zugeordnet werden können. Zum anderen ist umstritten, ob der Begriff der personenbezogenen Daten relativ ist, ob also Informationen für das eine Unternehmen personenbeziehbar sein können, weil es über bestimmte Zusatzinformationen verfügt, während sie für ein anderes Unternehmen nicht personenbezogen sind, weil ihm die nötigen Zusatzinformationen fehlen.

Nach geltendem Recht gelten Daten, die nicht oder nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, nicht als personenbezogen, sondern als anonym. Dabei sind alle Mittel zu berücksichtigen, die erwartungsgemäß entweder vom datensammelnden Unternehmen selbst oder von einem Dritten eingesetzt werden können. Ausreichend ist dabei, wenn der Personenbezug mit Zusatzwissen Dritter hergestellt werden kann, soweit das Zusatzwissen absehbar genutzt wird.

An der »Bestimmbarkeit« fehlt es andererseits nicht erst bei absoluter Unmöglichkeit, sondern bereits dann, wenn das Reidentifizierungsrisiko so gering ist, dass es praktisch irrelevant erscheint, dass ein Personenbezug hergestellt wird.

Ohne hier in Details einzusteigen, kann man sich merken: Ob Informationen personenbezogene Daten sind oder nicht, muss jedes Unternehmen aus seiner Sicht bestimmen (Relativität des Personenbezugs). Bei der Frage, ob ein Personenbezug herstellbar ist, dürfen aber nicht nur die eigenen Informationen berücksichtigt, sondern es muss auch das Wissen Dritter einbezogen werden. Entscheidend ist die Frage: Wie hoch ist die Wahrscheinlichkeit, dass die Informationen doch irgendwie oder irgendwann einer Einzelperson zugeordnet werden können?

Personenbezug von IP-Adressen

Der Streit zeigt sich schon bei IP-Adressen: Eine IP-Adresse ist eine Nummernfolge, die der Internetzugangsanbieter (Access Provider) einem Rechner, der an das Internet angeschlossen ist, dauerhaft oder zeitweise zuweist. Wählt sich etwa ein Nutzer ins Internet ein, vergibt ihm der Internetzugangsanbieter, zum Beispiel die Deutsche Telekom, vorübergehend eine bestimmte IP-Adresse. Wählt sich derselbe Nutzer am nächsten Tag wieder ein, kann er eine andere IP-Adresse bekommen. Solche IP-Adressen nennt man daher auch »dynamisch«. Surft nun ein Nutzer auf einer Website, so überträgt sein Browser die IP-Adresse an den Server des Websitebetreibers, der sie standardmäßig zusammen mit Datum und Adresse der aufgerufenen Seite in einer Protokolldatei speichert.

Sind diese Protokolldateien personenbezogene Daten? Es stehen keine Namen in der Datei und der Websitebetreiber weiß nicht, welchem Telekom-Nutzer die IP-

Adresse zum fraglichen Zeitpunkt zugeteilt wurde. Die Telekom jedoch hat diese Information. Sie könnte die Protokolldateien problemlos ihrem Kunden Hans Müller aus der Dorfstraße zuordnen. Der Websiteanbieter kommt an diese Daten nicht so leicht. Eine Strafverfolgungsbehörde dagegen könnte die Auskunft bei Verdacht einer Straftat von der Telekom in Erfahrung bringen. Zusammen mit den Protokolldateien der Websitebetreiber könnte nachverfolgt werden, welche Internetseiten Hans Müller wann aufgerufen hat. Doch genügt diese theoretische Verkettungsmöglichkeit, um die dynamischen IP-Adressen für den Websitebetreiber als personenbezogene Daten einzustufen? Die Frage liegt derzeit nach einer Vorlage durch den deutschen Bundesgerichtshof beim Europäischen Gerichtshof [2].

Personenbezug bei Big-Data- und Business-Intelligence-Projekten

Business Intelligence nutzt Daten aus den unterschiedlichsten Bereichen, zum Beispiel:

- Mitarbeiterdaten aus der HR-Software (HR = Human Resources)
- Finanz- und Buchungsdaten aus dem ERP-System (ERP = Enterprise Resource Planning)
- Kundendaten und Vertragsdaten aus dem CRM-Tool (CRM =
- Customer Relationship Management)
- Protokoll- und Nutzungsdaten der Website, des Onlineshops und der vom Unternehmen bereitgestellten Apps
- Protokoll- und Kommunikationsdaten aus der Internet-, E-Mail- und sonstigen Softwarenutzung durch Mitarbeiter
- Standortdaten von Dienstfahrzeugen
- Produktions- und Logistikdaten aus der Fertigung und dem Warenversand

Häufig sind diese Daten personenbezogen, selbst wenn dies auf den ersten Blick nicht so scheint: Die Buchungsdaten des ERP-Systems zum Beispiel betreffen vordergründig nur das Unternehmen und keine Einzelpersonen. Buchungen werden aber oft von Menschen ausgeführt oder freigegeben, und auch diese Daten stecken im ERP-System und weisen damit Personenbezug auf. Bei der Aufdeckung potenzieller Missbrauchsfälle geht es dann letztlich auch um das Fehlverhalten von Personen. Auch die Standortdaten der Autoflotte sind personenbezogen, da das Unternehmen dokumentiert haben dürfte, welcher Mitarbeiter welches Fahrzeug nutzt. Selbst Produktionsdaten von Maschinen können Aussagen über die Maschinenführer oder Schichtverantwortlichen beinhalten.

Bei der Auswertung der Daten im Rahmen der Business Intelligence und bei Big Data will das Unternehmen aber häufig keine Informationen über Einzelpersonen gewinnen, sondern nur allgemeine Zusammenhänge, Strukturen und Beziehungen erkennen oder Vorhersagen treffen. Dennoch sind Ausgangsbasis der Analysen zunächst personenbezogene Daten. Sollen diese aus den operativen Systemen exportiert, strukturiert und dann ausgewertet werden, so handelt es sich deshalb im ersten Schritt um Datenverarbeitungen, für die es einer datenschutzrechtlichen Erlaubnis bedarf. Ziel muss dabei sein, die Personenbeziehbarkeit möglichst frühzeitig und umfassend auszuschließen. So können beim Datenexport aus den operativen Systemen Merkmale ignoriert, gelöscht oder überschrieben werden, die – zusammen mit weiteren Informationen – einen Personenbezug erlauben könnten. Dies können etwa der Name, die Nutzerkennung, die Anschrift oder die E-Mail-Adresse sein.

Dem Unternehmen dürfte es aber häufig dennoch weiterhin recht einfach möglich sein, diesen eingeschränkten Datenbestand wieder einzelnen Mitarbeitern oder Kunden zuzuordnen: Anhand von Informationen in den operativen Systemen, deren Back-ups oder archivierten Daten, die das Unternehmen aus steuerlichen Gründen oder zum Zweck der Wirtschaftsprüfung vorhalten muss, ließe sich leicht wieder ein Personenbezug herstellen. Es gilt also, zusätzliche Maßnahmen zu treffen, um dieses Reidentifizierungsrisiko weiter zu reduzieren.

Anonymisieren – aber richtig

Um Informationen zu anonymisieren, können z. B. die aus den operativen Systemen kopierten Daten verunschärft werden. Statt des Geburtsdatums eines Kunden kann nur die Altersklasse (30–35 Jahre), statt des genauen Standorts eines Fahrzeugs nur die grobe Position übernommen werden. Denkbar ist auch, die Daten nur in aggregierter Form zu übernehmen, z. B.: »12 Mitarbeiter haben eine Berufszugehörigkeit von fünf Jahren.«

Neben diesen technischen Mitteln können auch organisatorische Maßnahmen helfen, die Personenbeziehbarkeit des auszuwertenden Datenbestandes zu erschweren. So können die operative Nutzung der Daten in den Live-Systemen und die Auswertung im Rahmen der Business Intelligence funktional getrennt werden. Hierzu sollte die Auswertung in einem technisch getrennten und sicheren System erfolgen, zum Beispiel mit eigener Datenbank und eigener Hardware. Daneben ist auch organisatorisch eine Abtrennung vorzunehmen, etwa indem Echtdatenerfassung und Auswertung durch unterschiedliche Teams erfolgen. Zur organisatorischen Trennung können Auswertungen auch von einem externen Dienstleister oder einer eigens gegründeten IT-Servicegesellschaft durchgeführt werden. Zwischen dem Unternehmen und der auswertenden Gesellschaft sollte dann ein Vertrag mit strenger Zweckbindung, Wiederverknüpfungsverbot, Vertragsstrafen und ggf. Publizitätspflichten bei Verstößen geschlossen werden. Die Einhaltung der Anforderungen kann ergänzend durch einen unabhängigen Dritten, zum Beispiel einen Wirtschaftsprüfer, regelmäßig auditiert werden.

Diese Vorkehrungen können helfen, die Personenbeziehbarkeit der ins Data Warehouse einfließenden Daten auszuschließen oder zu erschweren. Ist nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft und unter Verstoß gegen vertragliche Vereinbarungen eine Reidentifkation von Einzelpersonen möglich, sind die Daten im Data Warehouse anonym. Auf die anschließenden Auswertungen ist dann das Datenschutzrecht nicht anwendbar.

Zu der Frage, welche Maßnahmen konkret nötig sind, um die Personenbeziehbarkeit zu verneinen, gibt es kaum verlässliche Antworten. Dennoch lohnt sich der Aufwand. Denn selbst wenn personenbezogene Daten im Warehouse stecken, helfen die oben genannten Maßnahmen, die Auswertungen auf eine datenschutzrechtliche Erlaubnisnorm zu stützen. Die Schutzmaßnahmen und eine funktionale Trennung werden nämlich im Rahmen der datenschutzrechtlichen Vorschriften zugunsten des Unternehmens berücksichtigt.

Sollen die aus den Auswertungen gezogenen Schlüsse auf Einzelpersonen angewendet werden, ist das Datenschutzrecht wieder anwendbar. Werden etwa aus anonymisierten Verkaufsdaten Kundensegmente und -typen gebildet und anschließend einzelne Kunden den Kundensegmenten zugeordnet und so Aussagen über potenzielle Vorlieben oder Verhaltensweisen ermittelt, sind die datenschutzrechtlichen Anforderungen wieder zu beachten.

Zudem gibt es auch bei der Business Intelligence Anwendungen, bei denen eine Anonymisierung ausscheidet, weil gerade eine Auswertung bezogen auf einzelne Kunden oder Mitarbeiter stattfinden soll. Beispiele sind Personalsysteme, die anhand interner und externer Mitarbeiterdaten erkennen, welche Beschäftigten möglicherweise kündigen, oder das Potenzial von Bewerbern anhand der Bewerbungsdaten und öffentlich zugänglicher Quellen zu ermitteln versuchen.

DATEN IM KONZERN

Bei der Datenanalyse sollen nicht nur die Daten eines Unternehmens, sondern auch diejenigen eventuell bestehender Tochtergesellschaften oder anderer verbundener Unternehmen in die Auswertung einfließen. Datenschutzrechtlich wird jedes Konzernunternehmen als eigenständige Einheit betrachtet. Sollen zum Beispiel Daten von der Vertriebstochtergesellschaft an die Konzernmutter übermittelt werden oder soll ihr Zugriff auf solche Daten gewährt werden, so liegt bereits eine Datenübermittlung vor. Das Gleiche gilt,

wenn Mitarbeiterdaten aller Verbundunternehmen in einem Datenpool gesammelt werden. Für die Übermittlungen innerhalb des Konzerns bedarf es einer Erlaubnisnorm. Diese ist nicht leicht zu finden, denn das Datenschutzrecht kennt kein Konzernprivileg: Die Datenübermittlung innerhalb des Konzerns wird grundsätzlich genauso behandelt wie die Datenweitergabe an externe Dritte.

Gerade beim Transfer von Personaldaten im Konzern vertreten die deutschen Aufsichtsbehörden eine strenge Linie. Daher ist es vorzuziehen, die Daten noch vor der Übermittlung unmittelbar bei der Tochtergesellschaft zu anonymisieren, bevor sie im zentralen Data Warehouse landen.

Im internationalen Konzernverbund kommt eine weitere Herausforderung hinzu: Auf Kunden- und Mitarbeiterdaten ausländischer Konzernunternehmen findet das lokale Datenschutzrecht Anwendung. Wie oben beschrieben ist dieses in der EU zwar vereinheitlicht, aber nicht identisch. Es kann daher nötig sein, mehrere Datenschutzgesetze zu berücksichtigen, wenn Daten aus verschiedenen Ländern zusammengeführt werden.

DER ZWECKBINDUNGS-GRUNDSATZ

Bei Business-Intelligence- oder Big-Data-Projekten werden Daten verschiedenen Quellen entnommenen, in einem Data Warehouse zusammengeführt, neu strukturiert und ausgewertet. Die aus Vertragsverhältnissen oder als Metadaten angefallenen Informationen werden dabei aus ihrem Zusammenhang gerissen und mit geänderter Zielrichtung ausgewertet. Dem kann der datenschutzrechtliche Grundsatz der Zweckbindung entgegenstehen.

Der Zweckbindungsgrundsatz steht in der EU-Datenschutzrichtlinie und hat zwei Aspekte: Erstens dürfen personenbezogene Daten nur »für festgelegte eindeutige und rechtmäßige Zwecke erhoben« werden (Zweckfestlegung). Zweitens dürfen sie nicht in einer mit der ursprünglichen Zweckbestimmung unvereinbaren Weise weiterverarbeitet werden (kompatible Nutzung).

Die EU-Datenschutzbehörden haben im Rahmen der Artikel-29-Arbeitsgruppe eine gemeinsame Stellungnahme zu ihrem Verständnis des Zweckbindungsgrundsatzes verfasst [3].

Der Stellungnahme nach ist der Zweck eindeutig, wenn er unmissverständlich und deutlich festgelegt ist und nach außen hin zum Ausdruck gebracht wurde. Innere Absichten, Vorstellungen und Wünsche des Unternehmens sind keine »eindeutig« festgelegten Zwecke. Wurden die Zwecke nicht kommuniziert oder sind sie missverständlich oder undeutlich, so sollen alle tatsächlichen Begebenheiten, das allgemeine Verständnis sowie die generellen Erwartungen der Betroffenen zur Zweckbestimmung herangezogen werden. Zweckfestlegungen wie »Verbesserung des Nutzungserlebnisses«, »Marketing« oder »IT-Sicherheit« sind nach Ansicht der Aufsichtsbehörden zu vage.

Der Wert von Daten eines Unternehmens hängt also maßgeblich davon ab, welcher Verwendungszweck bei der Erhebung festgelegt und auch nach außen hin kommuniziert wurde. Sollen Daten aus der Abwicklung von Kaufverträgen später zur Vorhersage des Kundenverhaltens genutzt werden, sollte dies bereits bei der Erhebung deutlich gemacht werden. Sonst schränkt der Zweckbindungsgrundsatz spätere Analysemöglichkeiten ein. Auch an anderer Stelle, etwa bei online erfassten Daten, Daten aus der Logistik oder bei zur Betrugsbekämpfung relevanten Daten ist bereits bei der Entstehung an spätere Nutzungsmöglichkeiten zu denken und dies nach außen hin deutlich zu machen. Rechtlich betrachtet hängt an Daten ein Schild mit der Beschriftung »Nutzungszweck«. Was darauf steht, bestimmt die Verwertbarkeit und den Wert der Daten entscheidend mit.

Der Grundsatz der kompatiblen Nutzung besagt: Daten dürfen nach ihrer Erhebung nicht in einer mit der ursprünglichen Zweckbestimmung unvereinbaren Weise weiterverarbeitet werden. Damit kommt zum Ausdruck,

dass eine Zweckänderung durchaus zulässig ist. Das Unternehmen ist nicht auf den ursprünglichen Zweck beschränkt. Die späteren Nutzungszwecke müssen aber mit der ursprünglichen Zweckfestlegung kompatibel sein. Als die Daten erhoben wurden, hat das Unternehmen unter Umständen nicht daran gedacht, diese später für Massendatenanalysen zu verwenden, und dies auch nicht nach außen kommuniziert. Der Frage, ob der neue Nutzungszweck (z. B. Vorhersage des Kündigungsverhaltens) mit dem ursprünglichen Erhebungszweck (z. B. Abwicklung des Kaufvertrags) kompatibel ist, kommt daher bei der datenschutzrechtlichen Zulässigkeit eine entscheidende Bedeutung zu.

Nach Auffassung von Aufsichtsbehörden wäre zum Beispiel folgendes Szenario ein Verstoß gegen das Gebot kompatibler Nutzung: Ein Supermarkt wertet die Einkäufe von Kunden dahin gehend aus, ob diese sich gesund ernähren. Die Kunden mit schlechter Ernährung werden angeschrieben und erhalten im Rahmen einer Partnerschaft mit der öffentlichen Hand Informationen zur Verbesserung ihrer Essgewohnheiten. Auch die Ermittlung einer potenziellen Schwangerschaft von Kundinnen einer Drogerie anhand ihres Einkaufsverhaltens und die Nutzung für passgenaue Werbung wären entsprechend unzulässig. Schließlich soll auch die Auswertung des Stromverbrauchs aus elektronischen Stromzählern (Smart Meters) zur Identifikation potenzieller Inhouse-Cannabis-Plantagen unzulässig sein.

Der Kompatibilitätstest ist im deutschen Recht nicht ausdrücklich geregelt, sondern in verschiedene Vorschriften hineinzulesen. Die von den EU-Behörden entwickelten Kriterien und Beispielsfälle bieten eine gute Grundlage, um Potenziale und Risiken abzuschätzen. Auch lassen sich daraus Vorkehrungen zur Sicherstellung der Datenschutzkonformität ableiten: Datenschutzbeauftragte können darauf achten, dass Transparenz hergestellt wird, dass den Betroffenen Widerspruchsmöglichkeiten eingeräumt werden oder dass eine funktionale Trennung vorgenommen wird.

Zum Entstehungszeitpunkt dieses Beitrags (September 2015) wird der Entwurf der EU-Datenschutzgrundverordnung gerade im Rahmen des Trilogs zwischen Rat, Kommission und Parlament diskutiert. Danach könnte es zu Änderungen beim Zweckänderungsgrundsatz kommen, die teilweise auf heftige Kritik stoßen, weil eine Aufweichung des Datenschutzes befürchtet wird [4]. Eine Zweckänderung soll nach den Vorstellungen des Rates dann zulässig sein, wenn eine Interessenabwägung zwischen den Betroffenen- und Unternehmensinteressen zugunsten des Unternehmens ausfällt. Ob eine solche Regelung in Kraft tritt, ist unklar. Und selbst wenn der Vorschlag Gesetz wird, dürfte entscheidend sein, wie diese Interessenabwägung in der behördlichen und gerichtlichen Praxis ausgelegt wird. Letztlich kann nämlich auch im Rahmen des aktuellen Kompatibilitätstests und des geltenden Rechts in Deutschland eine Nutzung für einen neuen Zweck zulässig sein, wenn eine Berücksichtigung verschiedener Kriterien und Belange positiv ausfällt. Das ist nichts anderes als eine Interessenabwägung. Die Aufregungen um die »Abschaffung des Zweckbindungsgrundsatzes« erscheinen daher ungerechtfertigt.

Der Kompatibilitätstest

Die EU-Datenschutzbehörden haben für die Überprüfung der Nutzungskompatibilität einen Katalog mit folgenden Kriterien entwickelt:

1. Zusammenhang zwischen dem ursprünglichen und dem späteren Verwendungszweck:

War der spätere Verwendungszweck zum Zeitpunkt der Erhebung mehr oder weniger schon impliziert, stellt die Verwendung für den späteren Zweck also einen absehbaren nächsten Schritt dar? Abzustellen ist nicht formal auf den Wortlaut der Zweckfestlegung z. B. in Datenschutzhinweisen (Privacy Policy), sondern auf die tatsächlichen Begebenheiten und das allgemeine Verständnis der Beteiligten zum Erhebungszeitpunkt.

2. Kontext, in dem die personenbezogenen Daten ursprünglich erhoben wurden, und die vernünftigen Erwartungen der Betroffenen:

Hier ist entscheidend, ob ein durchschnittlicher Betroffener zum Zeitpunkt der Erhebung mit der Verwendung für den späteren Zweck gerechnet hat. Ist der spätere Verwendungszweck üblich und allgemein akzeptiert, so spricht dies für eine Kompatibilität. Eine wichtige Rolle spielt dabei die Transparenz, nämlich ob und wie der Betroffene bei der Erhebung oder auch später über die Nutzungszwecke informiert wurde.

3. Die Art der Daten und die Auswirkungen der neuen Verwendung auf die Betroffenen:

Je sensibler die Daten sind, desto eher ist eine spätere Verwendung für einen anderen Zweck mit dem ursprünglichen Zweck inkompatibel. Dies gilt vor allem bei Gesundheitsdaten, biometrischen oder genetischen Daten, Kommunikationsdaten und Standortdaten.

Daneben sind die Auswirkungen der neuen Zweckverwendung für die Betroffenen zu berücksichtigen, und zwar positive wie negative. Negative Auswirkungen können etwa ein Ausschluss von Leistungen, Diskriminierung oder auch eine emotionale Beeinträchtigung durch den Verlust der Kontrolle über personenbezogene Daten sein.

Relevant ist vor allem die Art der späteren Datenverwendung. Erfolgt diese durch ein anderes Unternehmen, werden Daten veröffentlicht oder mit unvorhersehbaren Folgen weiterverarbeitet oder werden große Datenmengen miteinander kombiniert, so spricht dies tendenziell gegen eine kompatible Nutzung.

4. Vom Unternehmen getroffene Schutzmaßnahmen zur Verhinderung unangemessener Datenverwendungen und nachteiliger Auswirkungen auf die Betroffenen:

Schließlich sind bei der Kompatibilitätsprüfung Maßnahmen zu berücksichtigen, die die verantwortliche Stelle zum Schutz der Betroffenen ergriffen hat. Solche Maßnahmen sind gemäß der Artikel-29-Arbeitsgruppe typischerweise eine Anonymisierung oder Pseudonymisierung oder das Aggregieren von Daten. Auch eine erhöhte oder nachgeholte Transparenz der Datenverarbeitung kann berücksichtigt werden, ebenso das Einräumen eines Widerspruchsrechts für den Betroffenen oder das Einholen seiner Zustimmung zur Nutzung für den neuen Zweck. Als Schutzmaßnahme kommt auch eine funktionale Trennung in Betracht, wie sie oben beschrieben wurde.

Beim Kompatibilitätstest werden alle oben genannten Faktoren berücksichtigt und gewertet. Im Ergebnis können also geeignete Schutzmaßnahmen durchaus auch umfangreichere Zweckänderungen legitimieren.

AM FALSCHEN ENDE SPAREN – PROBLEME MIT DER DATENSPARSAMKEIT

Neben dem Zweckbindungsgrundsatz kann der Einsatz von Big-Data- und Business-Intelligence-Analysen auch zu Konflikten mit dem Grundsatz der Datensparsamkeit führen. Personenbezogene Daten dürfen nur gespeichert werden, solange hierfür eine Rechtsgrundlage besteht. Daten aus Vertragsverhältnissen dürfen zum Beispiel zur Durchführung und Beendigung des Vertragsverhältnisses gespeichert werden. Ist der Vertrag abgewickelt, etwa nachdem die verkaufte Ware an den Kunden ausgeliefert wurde, sind die Daten grundsätzlich zu löschen. Eine Speicherung kann sich dann allenfalls aus einer anderen Rechtsgrundlage ergeben, zum Beispiel weil die Daten aus steuerlichen Gründen archiviert werden müssen. Die so archivierten Daten dürfen dann aber nach dem Zweckbindungsgrundsatz nur für steuerliche Prüfungen genutzt werden.

Für die Auswertung historischer Daten bei Big Data oder Business Intelligence müssen Daten aber meist längerfristig gespeichert werden. Zudem werden die Daten oft aus den operativen Systemen in ein Data Warehouse übertragen. Die in den operativen Systemen vorgesehenen Löschmechanismen greifen dann nicht mehr.

Um Verstöße gegen das Datenschutzrecht zu vermeiden, sollten die Daten im Data Warehouse anonymisiert sein. Ist dies nicht möglich, muss eine Rechtsgrundlage für eine verlängerte Speicherung gefunden werden. Da Einwilligungen in der Regel ausscheiden, kommen die oben bei der Zweckbindung geschilderten Schutzmaßnahmen in Betracht. Zudem kann versucht werden, den Zweck der Auswertung schon bei der Datenerhebung transparent zu machen, sodass dieser legitimierte Auswertungszweck eine längerfristige Speicherung ermöglicht.

DIE BETROFFENENRECHTE

Werden die genutzten Daten in einem Data Warehouse vorgehalten, ist neben dem Löschungsgebot auch besonderes Augenmerk auf das Recht der Betroffenen auf Auskunft zu legen. Betroffene haben das Recht, vom Unternehmen Auskunft zu allen über sie gespeicherten Daten zu erhalten. Das schließt ein Data Warehouse ein, selbst wenn die Daten dort nicht mit Klarnamen, sondern unter einem auflösbaren Pseudonym gespeichert sind. Das Data Warehouse muss technisch in der Lage sein, solche Auskunftsansprüche durch Bereitstellung von Datenextrakten zu erfüllen.

In bestimmten Fällen kann den Betroffenen zudem das Recht zustehen, der Auswertung ihrer Daten zu widersprechen. Die genutzte Software muss entsprechend die Möglichkeit bieten, die betroffenen Datensätze bei der Analyse auszublenden oder im Data Warehouse zu löschen.

AUTOMATISIERTE EINZELFALLENTSCHEIDUNG, SCORING UND PROFILING

Für bestimmte Datenauswertungen hat der Gesetzgeber neben den allgemeinen Vorschriften Sonderreglungen erlassen. So verbietet das Gesetz etwa »automatisierte Einzelfallentscheidungen« (§ 6a BDSG). Entscheidungen, die für den Betroffenen rechtliche Folgen nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nach diesem Verbot nicht ausschließlich auf die Entscheidung einer Maschine gestützt werden, wenn diese der Bewertung einzelner Persönlichkeitsmerkmale dient. Die Bewertung einzelner Persönlichkeitsmerkmale liegt zum Beispiel vor, wenn die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit oder das Verhalten von Menschen durch Computer errechnet oder vorhergesagt werden.

Entscheidet ein Computer anhand von Bewerbungsunterlagen, wer eingeladen bzw. eingestellt wird, so wäre dies eine verbotene automatisierte Einzelfallentscheidung. Das Gleiche dürfte gelten, wenn man die Effektivität von Mitarbeitern anhand ihrer elektronischen Post und anderer Metadaten automatisiert bewertet und dies unreflektiert in Beförderungsentscheidungen übernimmt. Aber auch das Verweigern von Vorzugskonditionen für Kunden auf der Basis maschinengestützter Entscheidungen soll nach ein Verboten sind indes nur Fälle, in denen allein der Computer entscheidet und kein Mensch zwischengeschaltet ist. Empfiehlt die Maschine nur oder schafft sie lediglich eine Entscheidungsgrundlage, so bereitet das Verbot automatisierter Einzelfallentscheidungen keine Probleme. Wenn man bei automatisierten ablehnenden Entscheidungen die Letztentscheidung einem Menschen überlässt, gerät man in keinen Konflikt mit dem Verbot der automatisierten Einzelfallentscheidung.

Zudem sieht das Gesetz bestimmte Ausnahmen vor: Das Verbot gilt nicht bei positiver Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrags, also etwa wenn ein Kredit oder ein Kauf auf Rechnung bewilligt wird. Nicht verboten sind automatisierte Entscheidungen auch dann, wenn das Unternehmen Schutzmaßnahmen zugunsten der Betroffenen trifft, die Betroffenen über die Computerentscheidung informiert und ihnen auf Verlangen die wesentlichen Gründe der automatisierten Entscheidung mitteilt und erläutert. Der Mechanismus muss also transparent gemacht werden, zum Beispiel in den AGB oder Datenschutzhinweisen. Außerdem

muss der Kunde eine Einspruchsmöglichkeit erhalten.

Neben dem Verbot automatisierter Einzelfallentscheidungen enthält das Gesetz auch Sonderanforderungen für das sogenannte Scoring (§ 28b BDSG). Beim Scoring wird ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten eines Menschen ermittelt, z. B. ob dieser seine Zahlungen fristgerecht begleichen wird. Zweck der Ermittlung dieses Wertes muss sein, über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses zu entscheiden. Liegt ein solches Scoring vor, so verlangt das Gesetz, dass ein wissenschaftlich anerkanntes mathematisch-statistisches Verfahren zum Einsatz kommt, das nachweisbar für die Berechnung der Wahrscheinlichkeit des Verhaltens erheblich ist. Zudem dürfen für ein solches Scoring nicht ausschließlich die Anschriften der Betroffenen verwendet werden. Werden die Anschriften neben anderen Daten genutzt, ist dies zulässig, es muss dann aber explizit über die Verwendung der Anschriftendaten informiert werden. Beim Scoring hatte der Gesetzgeber vor allem das Kredit-Scoring im Auge, bei dem die Zahlungswahrscheinlichkeit von Schuldnern berechnet wird. Die Bestimmung kann aber auch bei Big-Data- bzw. Business-Intelligence-Projekten relevant werden, wenn der Computer das Verhalten von Menschen prognostiziert und dies für Vertragsentscheidungen genutzt wird. Wird jedoch die Affinität von Kunden für einzelne Produkte ermittelt, um diesen passgenaue Werbung zuzusenden (Werbe-Scoring), so greift die Vorschrift nicht.

In den Entwürfen der EU-Datenschutzgrundverordnung finden sich die Bestimmungen zum Verbot automatisierter Einzelfallentscheidungen unter dem Stichwort »Profiling« in veränderter Form wieder. Wie die Regelung aussieht, ist zum derzeitigen Stand offen, eine gute Übersicht findet sich in [5]. Der Gesetzentwurf der EU-Kommission sieht eine dem jetzigen Verbot automatisierter Einzelfallentscheidungen ähnliche Regelung vor, wobei die Einwilligung des Betroffenen vom Verbot befreien können soll. Der Vorschlag des EU-Parlaments sieht dagegen eine Ausweitung des Verbots vor. Auch Auswertungen, die zu bestimmten Diskriminierungen führen können (z. B. aufgrund der sexuellen Neigung) sollen verboten werden. Die EU-Aufsichtsbehörden fordern die Einführung ergänzender Begleitpflichten [6]. So sollen Unternehmen die Verfahren für Betroffene offenlegen und ihnen Zugriff auf die über sie erstellen Profile gewähren.

STANDORT-, KOMMUNIKATIONS-, GESUNDHEITS- UND INTERNETDATEN

Neben Spezialregelungen zu einzelnen Anwendungsfeldern wie den automatisierten Einzelfallentscheidungen hat der Gesetzgeber auch für bestimmte Arten von Daten Sonderregelungen aufgestellt. Dies betrifft etwa Standortdaten mobiler Endgeräte, Gesundheitsdaten und Kommunikationsdaten aus E-Mails, Telefonaten oder Chats. Auch für Daten, die über Apps oder von Besuchern auf Websites erfasst werden, gelten Spezialregelungen.

Online gesammelte Daten dürfen grundsätzlich nur verwendet werden, soweit dies zur Erbringung des jeweiligen Onlinedienstes erforderlich ist. Der deutsche Gesetzgeber hat hier im Telemediengesetz Regelungen aufgestellt, die teilweise strenger als das Bundesdatenschutzgesetz und die europäischen Vorgaben sind.

Die Information, wann sich ein Nutzer in seinen Online-Account eingeloggt hat, muss zur technischen Abwicklung des Log-ins möglicherweise kurzfristig gespeichert werden. Für eine längerfristige Speicherung und Verwendung über den Nutzungsvorgang hinaus fehlt es allerdings bereits an einer rechtlichen Grundlage. Das Gleiche gilt für das Speichern der von einem Nutzer aufgerufenen Seiten eines Onlineangebots oder der eingegebenen Suchbegriffe. Die Spezialregeln schränken die Erfassung und Auswertung von Onlinedaten für Business-Intelligence-Zwecke stark ein, sofern keine Einwilligung vorliegt oder die Daten nicht anonymisiert wurden.

Glücklicherweise hat der deutsche Gesetzgeber aber eine Möglichkeit offengelassen: Das Telemediengesetz erlaubt nämlich die Bildung von Nutzerprofilen zu Werbezwecken anhand von Pseudonymen, wenn der Nutzer hierüber informiert wurde und die Möglichkeit hat zu widersprechen. Der Websiteanbieter darf also erfassen und auswerten, wann sich Nutzer angemeldet und welche Aktionen sie auf der Seite ausgeführt haben. Er darf diese Information allerdings nicht zusammen mit dem Nutzernamen, der E-Mail-Adresse oder der Nutzerkennung speichern. Vielmehr sind die Daten unter Pseudonymen, etwa einer für jeden Nutzer zufällig generierten Kennzahl, zu speichern und dürfen mit den Klarnamen der Nutzer nicht zusammengeführt werden. Außerdem sind die Nutzer über die Datenerfassung und Auswertung in den Datenschutzhinweisen der Website bzw. App klar und verständlich zu informieren. Über einen Link ist eine Widerspruchsmöglichkeit einzuräumen; nach Anklicken des Links darf keine Auswertung des Nutzerverhaltens (Tracking) mehr erfolgen. Die entsprechenden Anforderungen sind zum Beispiel bei Analysetools wie Google Analytics oder Kissmetrics zu beachten. Daten, die durch diese Vorkehrungen gesammelt werden, sind rechtlich nicht oder kaum nutzbar.

Besonderheiten sind auch bei der Erfassung und Auswertung von Kommunikationsdaten, etwa aus Telefonaten, Chats oder E-Mails, zu beachten. Hier enthält das Telekommunikationsgesetz Spezialvorschriften. Zudem kann das Fernmeldegeheimnis betroffen sein, sodass den IT-Verantwortlichen bei unbefugter Auswertung von E-Mails sogar eine Strafbarkeit droht. Dabei wird die Ansicht vertreten, dass ein Arbeitgeber, der seinen Mitarbeitern die eingeschränkte private Nutzung von E-Mail, Internet oder Telefon erlaubt, dies nicht verboten hat oder faktisch duldet, als Telekommunikationsanbieter anzusehen ist. Folge ist, dass der Arbeitgeber im Verhältnis zu seinen Mitarbeitern an das Fernmeldegeheimnis gebunden ist. Ohne Einwilligung der Mitarbeiter könnte sich der Arbeitgeber dann bei Einsichtnahme oder Auswertung von Kommunikationsdaten strafbar machen. Als Daumenregel gilt daher bei Kommunikationsdaten einschließlich Standortdaten von Handys: Eine Auswertung ist in der Regel nur anonymisiert oder mit Einwilligung der Betroffenen zulässig.

Ähnliche Vorsicht ist bei bestimmten sensiblen, »besonderen« Arten von Daten geboten. Dazu gehören Informationen über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Auch hier funktioniert ohne Einwilligung in der Regel gar nichts. Die Definition von »sensible Daten« ist dabei recht weit. Alles, was Rückschlüsse zum Beispiel auf die Gesundheit erlaubt, kann unter diese Kategorie fallen. So werden etwa die Krankheitsfehltage der Mitarbeiter von Aufsichtsbehörden zu den sensiblen Daten gezählt.

SO KLAPPT ES MIT DEM DATENSCHUTZ: ZUSAMMENFASSENDE EMPFEHLUNGEN

Nehmen Sie sich die folgenden Empfehlungen zu Herzen, dann klappt es auch mit dem Datenschutz:

Halten Sie Datenschutzanforderungen bei Big Data oder Business Intelligence nicht voreilig für irrelevant, weil vermeintlich nur anonyme Daten genutzt werden. Der Anwendungsbereich des Datenschutzrechts ist weit. Auch Informationen, die nur mit gewissem Aufwand und Zusatzwissen Dritter auf Einzelpersonen zurückgeführt werden können, unterliegen den Datenschutzbestimmungen.

Binden Sie bei Big-Data- oder Business-Intelligence-Projekten den Datenschutzbeauftragten oder die Rechtsabteilung so früh wie möglich und kontinuierlich ein. Für die Verwertbarkeit Ihrer Daten sollten Sie bereits bei der Erhebung die Weichen richtig stellen.

Prüfen Sie sorgfältig die datenschutzrechtlichen Risiken und treffen Sie geeignete Vorkehrungen. Nur weil Auswertungen möglich

sind, Dienstleister diese anpreisen und andere es machen, sind sie noch lange nicht zulässig. Im Datenschutzrecht gelten ein strenges Verbot mit Erlaubnisvorbehalt, ein Zweckbindungsgrundsatz und ein Löschgebot. Zudem stehen Betroffenen Auskunftsansprüche zu. Durch Analyse der Datenschutzanforderungen lassen sich Schutzmaßnahmen treffen, um das rechtliche Risiko zu minimieren. Dazu gehört etwa, Auswertungen transparent zu machen, Daten zu pseudonymisieren, Betroffenen Widerspruchsrechte einzuräumen, Verwendungszwecke einzuschränken oder bestimmte Datenarten außen vor zu lassen.

Lassen Sie sich beim Datenschutz nicht von allgemeinen Aussagen in die Irre führen. Jeder Sachverhalt hat seine Besonderheiten. Zudem gibt es eine Vielzahl von Sonderregelungen, etwa bei maschinengestützten Entscheidungen, beim Anlegen von Nutzerprofilen sowie bei der Verwendung von Online- oder Gesundheitsdaten oder Daten aus Kommunikationsvorgängen.

Nehmen sie die geplante Reform des Datenschutzrechts in Europa nicht zum Anlass, den Datenschutz auf die lange Bank zu schieben. Die neuen Regeln dürften allenfalls Anfang 2018 in Kraft treten. Derzeit ist der Gesetzgebungsprozess in vollem Gange. Auf welche Inhalte sich die Kommission, das Parlament und der Rat einigen werden, ist derzeit noch unklar. Behalten Sie deshalb die Reform im Auge.

INTERNETQUELLEN

[1] https://www.thomashelbing.com/de/links-quellen-datenschutzrecht (letzter Zugriff am 12. April 2015)

[2] http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Ger..., Pressemitteilung des Bundesgerichtshof Nr. 152/2014 (letzter Zugriff am 12. April 2015)

[3] http://ec.europa.eu/justice/data-protection/article-29/documentation/opi... (nur in Englisch verfügbar) (letzter Zugriff am 12. April 2015)

[4] https://www.datenschutz.hessen.de/k89.htm#entry4317, Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015 (letzter Zugriff am 12. April 2015)

[5] http://www.out-law.com/en/articles/2015/february/eu-data-protection-refo... (auf Englisch) (letzter Zugriff am 12. April 2015)

[6] http://ec.europa.eu/justice/data-protection/article-29/documentation/oth..., Artikel-29-Arbeitsgruppe: Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, 13. Mai 2013 (letzter Zugriff am 12. April 2015)

[7] BI BI TKOM : Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte, 2012, S. 16. Online verfügbar unter: https://www.bitkom.org/Publikationen/2012/Leitfaden/Leitfaden-Big-Data-i...

Rechtsanwaltskanzlei
Dr. Thomas Helbing

Königinstraße 11a
80539 München

T +49 (0) 89 - 28 72 465 - 28
E helbing@thomashelbing.com
www.thomashelbing.com