Handelsblatt
RESEARCH INSTITUTE

DATENSCHUTZ UND BIG DATA: EIN LEITFADEN FÜR UNTERNEHMEN

Vorsprung durch Wissen.

Inhaltsverzeichnis

Vorwort

Selbstfahrende Autos, massenhafte Maßfertigung, präzise Wettervorhersagen, individuelle Medikamente – viele Innovationen, die den Menschen das Leben in naher Zukunft erleichtern werden, beruhen auf Big-Data-Analysen. Die technische Möglichkeit, unstrukturierte Daten in exponentiell steigender Menge aus unterschiedlichen Quellen sehr schnell zu sammeln und auszuwerten, wird das Alltagsleben revolutionieren. Unter dem Stichwort „Industrie 4.0“ wird diskutiert, wie sich durch diese Technologien die Produktion von Gütern aller Art verändern wird.

Die Daten für die Big-Data-Analysen stammen aus den unterschiedlichsten Quellen: Logistik- und Verkehrsmessdaten, Verbrauchsdaten von Strom- und Wasserversorgern, Statistiken der Gesundheitsbranche, Kreditkartenabrechnungen, Verbindungs- und Positionsdaten der Telekommunikationsunternehmen, wissenschaftliche Daten, Wetterinformationen, volkswirtschaftliche und soziale Statistiken, Messdaten aus der Produktion, Marktforschung, Kundeninformationen, Online-Transaktionen und Zugriffsstatistiken, Daten aus sozialen Netzwerken und vielen weiteren Ressourcen.

Viele dieser Daten berühren den persönlichen Bereich und ermöglichen vielfältige Rückschlüsse über Lebensumstände und Verhalten der von den Datenanalysen Betroffenen. Big-Data-Analysen werfen daher neue und vielschichtige Datenschutzfragen auf. Den verlockenden Erkenntnismöglichkeiten der Big-Data-Welt stehen berechtigte Anliegen des Datenschutzes gegenüber. Es gilt, einen ausgewogenen Ausgleich zwischen den Interessen der Menschen am Schutz persönlicher Daten und dem Interesse der Unternehmen und Behörden an der Nutzung der neuen Analysemöglichkeiten zu finden. Einerseits haben viele Menschen Angst davor, zu gläsernen Kunden zu werden, andererseits befürchten Unternehmen, den Anschluss an die internationale Konkurrenz zu verlieren, wenn der Datenschutz zu restriktiv gehandhabt wird.

Ein vertrauensvolles Verhältnis zwischen Unternehmen und ihren Kunden in Sachen Datenschutz ist eine wichtige Voraussetzung für eine stärkere Nutzung von Kundendaten für Big-Data-Analysen, die dazu beitragen, die Qualität von Produkten und Dienstleistungen zu verbessern und sogar gänzlich neue Geschäftsmodelle entstehen zu lassen. Nicht nur aus einzelbetrieblicher, sondern auch aus volkswirtschaftlicher Sicht ist es notwendig, hier einen angemessenen Ausgleich zu finden. Der setzt voraus, dass Unternehmen transparent und datenschutzkonform agieren und die Kunden fair an den Erträgen der Big-Data-Analysen beteiligen. Dieser Leitfaden informiert über die rechtlichen Voraussetzungen der Beziehung zwischen Unternehmen und Kunden im Big-Data-Zeitalter. Er basiert auf der Auswertung zahlreicher Studien und Informationsmaterialien durch das Handelsblatt Research Institute sowie in ganz wesentlichem Maße auf der Expertise der auf Datenschutzfragen spezialisierten Kanzlei Kinast & Partner Rechtsanwälte aus Köln.

1. Allgemeine Empfehlungen zum Datenschutz für Unternehmen

In den riesigen Datenbergen, die täglich in Unternehmen, Fabriken oder Haushalten anfallen, schlummert ein enormes Potenzial, das Unternehmen zur Optimierung ihrer Prozesse und Produkte verwenden können. Dabei müssen Sie aber einige wichtige Punkte beachten, wenn Sie personenbezogene Daten sammeln, speichern und verarbeiten. Der folgende Abschnitt gibt eine kurze Übersicht über die allgemeinen Grundsätze im Datenschutz, die wichtig für Unternehmen sind: wann dürfen Unternehmen Daten erheben, welche Regeln müssen sie dabei beachten und nach welchen Grundsätzen sollten Sie handeln?

1.1. Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung

Grundsätzlich dürfen personenbezogene Daten nur dann erhoben, verarbeitet oder genutzt werden, wenn dies durch das Bundesdatenschutzgesetz (BDSG) oder eine vorrangige Rechtsvorschrift erlaubt oder angeordnet wird oder der Betroffene gemäß § 4a BDSG eingewilligt hat. Es gilt somit das Verbot mit Erlaubnisvorbehalt. Daten erheben, verarbeiten und nutzen dürfen Sie demnach beispielsweise bei

- einer gesetzlichen Verpflichtung (z.B. bei der Strafverfolgung, der Steuerfahndung und zu Forschungszwecken)
- zur Erfüllung von bestimmten Pflichten aus einem Vertragsverhältnis
- zur Wahrung von berechtigten Geschäftsinteressen oder
- sofern es sich um öffentlich zugängliche Daten oder Listendaten handelt.

In allen weiteren Fällen braucht ein Unternehmen die Einwilligung des Betroffenen.

1.2. Einwilligungserklärung des Betroffenen

Sofern die oben genannten Erlaubnistatbestände die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten nicht ermöglichen, benötigt ein Unternehmen immer eine Einwilligung des Betroffenen (§ 4 BDSG), die grundsätzlich schriftlich erfolgen muss. Diese Einwilligung muss sich dabei gemäß § 4a BDSG ausdrücklich auf die erhobenen Daten und den Zweck der Erhebung beziehen. Für den Betroffenen müssen Art, Umfang und Inhalt der Datenerhebung erkennbar sein. Sie sollten in diesem Punkt transparent gegenüber Ihren Kunden sein und nicht versuchen, sich Einwilligungen zu „erschleichen“. Das ist weder rechtlich erlaubt noch stärkt es die Vertrauensbasis zwischen einem Unternehmen und seinen Kunden.

Es muss bei einer Einwilligungserklärung deutlich werden, wer für die Erhebung der Daten verantwortlich ist. Der komplette Name des Unternehmens als „verantwortliche Stelle“ im Sinne des BDSG und dessen Adresse muss dabei angegeben werden. Grundsätzlich muss eine Einwilligungserklärung in Schriftform erfolgen und mit eigenhändiger Unterschrift versehen sein, siehe § 4a Abs. 1 S. 3 BDSG. Daher sind Erklärungen per E-Mail, Kopie oder Scan nicht ausreichend.

Es gibt jedoch Ausnahmen: Die Einwilligung per E-Mail ist rechtssicher, wenn das sogenannte Double-Opt-In-Verfahren genutzt wird. Die ursprünglich formlose Einwilligung und ihr Inhalt müssen in diesem Fall anschließend noch einmal bestätigt werden, zum Beispiel durch eine Bestätigungs-E-Mail, in der der Benutzer über einen Link

zur erneuten Bestätigung der Einwilligung aufgefordert wird. Sie müssen den Betroffenen darauf hinweisen, dass seine Angaben freiwillig erfolgen. Nicht freiwillig sind beispielsweise Einwilligungen, bei denen der Betroffene schwere Nachteile zu befürchten hat, wenn er ihre Abgabe verweigert. Im Rahmen der Einwilligung muss der betroffene Kunde zudem über sein Widerrufsrecht informiert werden (vgl. §28 Abs. 4 S. 2 BDSG). Wird ein Widerspruch, der jederzeit möglich ist, abgegeben, ist die Datenverarbeitung unzulässig und die Daten des Betroffenen müssen von Ihrem Unternehmen umgehend aus dem Datensatz entfernt oder zumindest gesperrt werden. Sie sollten daher jede Einwilligung von Kunden präzise dokumentieren, damit Sie später jederzeit nachweisen können, dass eine legitime Einwilligung vorliegt.

1.3. Grundsatz der Direkterhebung

Gemäß § 4 Abs. 2 Satz 1 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Der Betroffene soll seine Daten bewusst preisgeben, Kenntnis über deren Nutzung und Verarbeitung haben und wissen, wer seine Daten erhebt und verarbeitet, um sein Recht der informationellen Selbstbestimmung wirkungsvoll ausüben zu können. Nur in Ausnahmefällen dürfen personenbezogene Daten erhoben werden, ohne dass es der Mitwirkung des Betroffenen bedarf. Die dafür geltenden Voraussetzungen sind in § 4 Abs. 2 BDSG genannt.

1.4. Zweckbindung

Das Prinzip der Zweckbindung im Datenschutzrecht besagt, dass die verantwortliche Stelle auf den ursprünglich genannten Verwendungszweck festgelegt ist. Der Zweck muss dabei für den Betroffenen präzise und erkennbar bestimmt sein. Dies gewährleistet, dass die Verarbeitung und Nutzung der Daten im Umfang nie über die erteilte Einwilligung des Kunden hinausgeht. Wenn ein Kunde etwa seine Daten zu vertraglichen Zwecken zur Speicherung freigegeben hat, dürfen Sie diese Daten nicht zu anderen Zwecken verwenden. Das sollten Sie stets beachten. Wenn sich der Zweck ändert oder eine Verwendung für weitere Zwecke beabsichtigt ist, sollten Sie sich eine neue Einwilligung beim Nutzer einholen. Sie sollten Ihren Datenbestand und die dazugehörigen Einwilligungserklärungen inklusive dem jeweiligen Zweck sorgfältig mithilfe geeigneter CRM-Systeme verwalten. Im Zweifelsfall müssen Sie jederzeit beweisen können, dass Ihnen eine Einwilligungserklärung des Betroffenen für diesen bestimmten Zweck vorliegt.

1.5. Anonymisierung und Pseudonymisierung

„Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“ (§3, Absatz 6 BDSG). Pseudonymisierung wird dagegen in § 3 Absatz 6a BDSG definiert als „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." Bei der Pseudonymisierung werden Merkmale zur Identifikation, also etwa der Name, durch ein Pseudonym ersetzt.

Der Gesetzgeber verlangt durch den Grundsatz der Datensparsamkeit, § 3a BDSG, dass Unternehmen so wenige personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen. Soweit es möglich ist, sollten Sie daher anonymisierte oder pseudonymisierte Daten verwenden, zum Beispiel bei der Auswertung des Nutzerverhaltens auf einer Homepage. Die Einhaltung dieses Grundsatzes muss jedoch für die verarbeitende Stelle verhältnismäßig sein. Wenn Sie die gesammelten Daten anonymisieren, so dass sie keinen Personenbezug mehr haben, sind die teilweise strengen Vorgaben aus dem Datenschutzgesetz nicht anwendbar. Um eine Datenbank von personenbezogenen Daten zu „befreien“, gibt es je nach Situation und Zweck spezielle Software-Werkzeuge.

1.6. Datensparsamkeit und Datenvermeidung

Unternehmen sind zur Datensparsamkeit und Datenvermeidung verpflichtet. So dürfen sie nach § 3a BDSG nicht mehr personenbezogene Daten von Benutzern erheben, als sie für den bestimmten Zweck zwingend benötigen. Möchte der Nutzer nur einen Newsletter abonnieren, dürfen Sie zum Beispiel keine Daten zu Konsumgewohnheiten erheben.

1.7. Die Pflicht zur Berichtigung, Löschung oder Sperrung von Kundendaten

Der Nutzer muss jederzeit die Möglichkeit haben, eine erklärte Einwilligung zu widerrufen. In diesem Fall müssen Sie die erhobenen personenbezogenen Daten unverzüglich löschen oder sperren. Sofern sich gespeicherte personenbezogene Daten als unrichtig oder unvollständig erweisen, müssen Sie diese gemäß § 35 Abs. 1 BDSG umgehend berichtigen. Personenbezogene Daten müssen Sie zudem sofort löschen, wenn die Erhebung oder Verarbeitung nicht zulässig war, die Verarbeitung oder Nutzung sich auf Grund nachträglich eingetretener Umstände als unzulässig erweist oder die Kenntnis der Daten für die verantwortliche Stelle nicht mehr erforderlich ist. Unternehmen müssen ihre Datenbestände regelmäßig überprüfen, um zu entscheiden, welche Daten nicht mehr notwendig sind. An Stelle einer Löschung kann laut Bundesdatenschutzgesetz in Ausnahmefällen auch eine Sperrung durchgeführt werden. Wann dies der Fall ist, regelt § 35 Abs. 3 BDSG. Um Daten ordnungsgemäß löschen oder sperren zu können, benötigen Sie einen guten Überblick über die im Unternehmen gespeicherten Daten und deren Verknüpfungen, über die relevanten Prozesse, Speicherorte und IT-Systeme.

1.8. Auskunftspflicht

Betroffene haben das Recht, jederzeit Auskunft über die Daten zu verlangen, die Unternehmen über sie gesammelt haben, siehe § 34 BDSG. Das Unternehmen muss mitteilen, welche Daten zur Person gespeichert sind, wo diese Daten erhoben wurden, an wen diese Daten weitergegeben werden und zu welchem Zweck sie gespeichert wurden. Die Auskunft darf lediglich verweigert werden, wenn das Interesse zur Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt. Sie müssen die Auskunft auf Anfrage des Betroffenen grundsätzlich kostenlos erteilen. Über Daten, die geschäftsmäßig zum Zweck der Übermittlung gespeichert werden, kann der Kunde einmal jährlich kostenfreie Auskünfte erbitten. Für weitere Auskünfte dürfen Sie Geld verlangen, müssen sie aber erteilen. Damit ein Unternehmen jederzeit in der

Lage ist, rechtskonform Auskunft über die gespeicherten Daten zu geben, sollte es ein effizientes und sorgfältiges Datenmanagement aufbauen und pflegen.

1.9. Bestellung eines Datenschutzbeauftragten

Wenn ein Unternehmen personenbezogene Daten automatisiert verarbeitet und in der Regel mehr als neun Personen ständig damit beschäftigt sind oder wenn mindestens zwanzig Personen mit manueller Datenverarbeitung beschäftigt sind, muss es gemäß § 4f Abs.1 Satz 4 BDSG einen Datenschutzbeauftragten bestellen. Behörden und sonstige öffentliche Stellen im Anwendungsbereich des BDSG müssen dagegen immer einen Datenschutzbeauftragten bestellen. Letzteres gilt ebenso für Unternehmen, die automatisierte Verarbeitungen vornehmen, die unter den Tatbestand des § 4d Abs. 5 BDSG fallen. Dazu zählen Datenverarbeitungsvorgänge, die der Vorabkontrolle unterliegen, wie es vor allem bei der Datenverarbeitung mit Bezug zu personenbezogenen Daten besonderer Art der Fall ist. Zudem müssen auch nicht-öffentliche Stellen, die „personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten“ (§ 4f Abs. 1 S. 6 BDGS) unabhängig von der Anzahl der Personen einen Datenschutzbeauftragten bestellen.

Zum Datenschutzbeauftragten dürfen nur Personen bestellt werden, die bestimmte fachliche Anforderungen erfüllen und zuverlässig sind, organisatorische Fähigkeiten besitzen und frei von Interessenskonflikten sind. Die genauen Anforderungen variieren je nach Umfang der Datenverarbeitung im einzelnen Unternehmen und dem Schutzbedarf der personenbezogenen Daten. Der Datenschutzbeauftragte kann ein Mitarbeiter des Unternehmens sein oder als externer Datenschutzbeauftragter bestellt werden.

1.10. Informationspflicht bei Datenpannen

Sollten bestimmte personenbezogene Daten unrechtmäßig an Dritte gelangen und dies die Betroffenen schwerwiegend beeinträchtigen, dann müssen Unternehmen die Datenpanne bei der zuständigen Aufsichtsbehörde und bei den Betroffenen selber angeben (§ 42a BDSG). Sie müssen die Aufsichtsbehörde grundsätzlich unverzüglich informieren. Was genau „unverzüglich“ heißt, hängt von den Umständen des Einzelfalles ab. Sie müssen auch die Betroffenen unverzüglich informieren, sobald eine mögliche Strafverfolgung nicht mehr gefährdet wird und angemessene Maßnahmen zur Sicherung der Daten ergriffen worden sind.

1.11. Datensicherheit

Die Datensicherheit stellt ein enorm wichtiges Thema für jedes Unternehmen dar, denn Unternehmen müssen sowohl ihre eigenen Daten als auch die für Big-Data-Analysen gesammelten Daten der Kunden sorgfältig vor dem Zugriff Unbefugter schützen. Dabei sind menschliche Fehler einer Studie zufolge ein großes Risiko: Mehr als ein Drittel der Büroangestellten hat schon einmal sensible Geschäftsunterlagen auf Kopierern oder Druckern gefunden und die Mehrheit der Berufspendler hat bereits dem Sitznachbarn über die Schulter geschaut und dabei einen Einblick in vertrauliche Daten erhalten.

Sie sollten daher solchen Datenschutzverstößen mit Aufklärungsmaßnahmen und regelmäßigen Schulungen entgegenwirken und das Bewusstsein Ihrer Mitarbeiter schärfen. Mit einem Leitfaden können Mitarbeiter für den datenschutzkonformen Umgang mit vertraulichen Daten sensibilisiert werden.

Ein weiteres wichtiges Element eines umfassenden Datenschutzkonzepts ist die Sicherheit der IT-Systeme. Sie sollten die Rechtevergabe für den Zugriff auf Ihre IT-Systeme restriktiv handhaben und jedem Benutzer nur so viele Administrationsrechte geben, wie er für seine Arbeit benötigt. Eine der größten Gefahren sind unsichere Vernetzungen von Systemen und Internet-Anbindungen. Kein Computer, der geschäftlich benutzt wird, darf ohne Schutz durch eine geeignete Firewall mit dem Internet verbunden werden. IT-Systeme sollten regelmäßig gewartet werden. Empfehlenswert sind zudem ein Aktionsplan für Sicherheits-Updates sowie regelmäßige und umfangreiche Sicherheits-Backups.

Vorsicht ist auch bei Reparaturen und der Entsorgung von Computern erforderlich. Es muss sichergestellt werden, dass die kompletten Festplatten gelöscht werden, sonst können Unbefugte sensible und vertrauliche Daten selbst auf defekten Datenträgern noch rekonstruieren. Servicetechniker sollten nie alleine ohne Aufsicht an IT-Systemen arbeiten. Sensible Daten in den Papierkorb zu verschieben, genügt nicht. Um Dateien sicher und unwiderruflich zu löschen, ist Spezial-Software erforderlich.

2. Empfehlungen zum Datenschutz beim Umgang mit Big Data

Auf diese allgemeinen datenschutzrechtlichen Ratschläge folgen nun Empfehlungen, die sich speziell auf den Umgang mit Big Data richten. Sie zeigen aus Sicht der Unternehmen, welche Möglichkeiten es im Rahmen des bestehenden Datenschutzrechts gibt, Big-Data-Analysen durchzuführen. Dabei differenzieren wir nach Empfehlungen für das Management und die Fachabteilungen.

2.1. Empfehlungen für das Management

2.1.1. Öffentlich-rechtliche, strafrechtliche und zivilrechtliche Haftung und Sanktionen

Datenschutzverstöße können ernsthafte Sanktionen nach sich ziehen. Es existieren nicht nur die besonderen Ordnungswidrigkeits- und Straftatbestände laut §§ 43, 44 BDSG, darüber hinaus können auch Tatbestände aus dem Strafgesetzbuch (StGB) und zivilrechtliche Schadensersatz- und Unterlassungsansprüche in Betracht kommen.

Öffentlich-rechtliche Sanktionen

Grundsätzlich werden Datenschutzverstöße mit den Bußgeldvorschriften des § 43 BDSG sanktioniert. Laut § 43 Abs. 1 BDSG kann bei der vorsätzlichen oder fahrlässigen Verletzung einer Vorschrift des BDSG ein Bußgeld bis zu 50.000 Euro verhängt werden. Zu den in der Praxis häufigsten Verstößen gehören die Verletzung der Pflicht zur Bestellung eines Datenschutzbeauftragten nach § 4f Abs.1 S. 1,2,3,6 BDSG, Pflichtverletzungen im Zusammenhang mit Maßnahmen der Auftragsdatenverarbeitung nach § 11 Abs. 1, S. 2,4 BDSG, das Unterlassen

der Unterrichtung der Betroffenen bei der Nutzung der Daten zu Werbezwecken und für den Adresshandel oder Verstöße bei der Erteilung einer Auskunft im Falle des Auskunftsbegehrens eines Betroffenen. Ein Bußgeld von bis zu 300.000 Euro zieht hingegen ein Verstoß gegen die in § 43 Abs. 2 BDSG genannten Ordnungswidrigkeiten nach sich. Hier geht es vor allem um den Umgang mit personenbezogenen Daten. Sanktioniert werden insbesondere ein unbefugtes Erheben, Verarbeiten, Abrufen und Verschaffen von personenbezogenen Daten, die nicht allgemein zugänglich sind. Auch die Verletzung von Informationspflichten bei Datenpannen nach § 42a BDSG wird mit einem Bußgeld in dieser Höhe geahndet.

Strafrechtliche Sanktionen

Bei einer schwerwiegenden Verletzung von Datenschutzvorschriften sieht das BDSG in § 44 in bestimmten Fällen Freiheitsstrafen bis zu zwei Jahren oder Geldstrafen vor. Strafbar macht sich danach, wer eine in § 43 Abs. 2 BDSG normierte vorsätzliche Handlung gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Zwingende Voraussetzung für die Strafbarkeit ist damit der Vorsatz.

Zivilrechtliche Sanktionen

Sofern dem Betroffenen durch einen Datenschutzverstoß ein materieller oder immaterieller Schaden entstanden ist, kann er aus verschiedenen gesetzlichen Ansprüchen Schadensersatz gegenüber der verantwortlichen Stelle geltend machen. Zum einen sieht § 7 BDSG einen Schadensersatzanspruch vor, zum anderen können jedoch auch die allgemeinen Schadensersatzansprüche aus dem Bürgerlichen Gesetzbuch (BGB) wie §§ 823, 831, 824, 826 BGB in Betracht kommen.

Nach § 7 BDSG macht sich die verantwortliche Stelle gemäß § 3 Abs. 7 BDSG bei einer datenschutzwidrigen Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten des Betroffenen schadensersatzpflichtig, wenn dem Betroffenen dadurch ein Schaden entstanden ist und sofern sie dabei nicht die gebotene Sorgfalt beachtet hat. Einer der schwierigsten Punkte bei einem Schadensersatz aus einem Datenschutzverstoß ist die Nachweisbarkeit eines konkreten Schadens. Der Betroffene muss den Schaden beweisen.

Zu beachten sind auch die Ansprüche aus dem BGB. Datenschutzgerechtes Verhalten von Angestellten kann sich aus einer Hauptpflicht des Arbeitsvertragsverhältnisses ergeben, in der Regel aber aus vertraglichen Nebenpflichten, welche unter Umständen zu einem vertraglichen Schadensersatzanspruch führen können. Aus § 823 BGB in Verbindung mit dem informationellen Selbstbestimmungsrecht oder dem allgemeinen Persönlichkeitsrecht kann sich im Falle eines verschuldeten Verstoßes gegen datenschutzrechtliche Regelungen ein Schadensersatzanspruch gegen Mitarbeiter eines Unternehmens ergeben.

Verantwortlichkeit der Geschäftsleitung

Für die beschriebenen Aspekte gilt, dass die Geschäftsleitung grundsätzlich gesamtschuldnerisch sowohl gegenüber der Gesellschaft als auch gegenüber Dritten haftet. Sie haftet für jedes Handeln und Unterlassen, das der Sorgfalt eines „ordentlichen und gewissenhaften Geschäftsleiters" widerspricht. Die Pflicht „geeignete Maßnahmen zu treffen" bezieht sich aus datenschutzrechtlicher Sicht vor allem auf fachlich einwandfreie,

technische und organisatorische Maßnahmen. Dies bedeutet, dass Sie das BDSG, die Anlage zu § 9 BDSG, TKG, TMG, UWG und spezialgesetzliche Vorschriften (z.B. SGB V) zwingend beachten müssen.

2.1.2. Risiken in Bezug auf Big Data

Die beschriebenen Haftungsrisiken häufen sich beim Umgang mit Big Data. Das gilt vor allem für die Verletzung der im BDSG normierten Betroffenenrechte. Denn die Daten der Betroffenen können nicht an allen Speicherstellen in der jeweiligen Anwendung berichtigt, gesperrt oder gelöscht werden, wenn die Erforderlichkeit nicht mehr gegeben ist. Auch sind aktuelle Auskünfte aus Big-Data-Sammlungen in vielen Fällen schon technisch bedingt nicht möglich, was die Auskunftsrechte der Betroffenen verletzt. Das kann verschiedene Tatbestände nach § 43 BDSG erfüllen.

2.1.3. Notwendige Voraussetzungen für eine umfassende Compliance

Zwingend nötig für die zulässige Speicherung und Analyse von Big Data ist, dass Sie für jede Maßnahme überprüfen, ob sie mit den geltenden gesetzlichen Voraussetzungen des Bundesdatenschutzgesetztes (BDSG) und weiterer, spezialgesetzlicher Normen, die notwendige Erfordernisse für eine rechtskonforme Datenerhebung, -verarbeitung und -nutzung vorgeben, zu vereinbaren ist.

Sie müssen nach dem Grundsatz des Verbots mit Erlaubnisvorbehalt sicherstellen, dass Sie eine gültige Einwilligung der Betroffenen (§§ 4a BDSG, 13 Abs. 2 TMG) oder eine gesetzliche Regelung als Legitimation (vgl. §§ 4 Abs. 1 BDSG, 12 Abs. 1 TMG) haben. Die Spezifikationen von Big-Data-Analysen müssen an den Anforderungen des Gesetzes gemessen werden. Dabei muss der Schutz des informationellen Selbstbestimmungsrechts der Betroffenen mit den Interessen der verantwortlichen Stelle an den neuen Analysemöglichkeiten durch Big Data in einen angemessenen Ausgleich gebracht werden.

Datenschutz-Folgenabschätzung (PIA)

Die EU arbeitet derzeit an einer neuen Datenschutz-Grundverordnung. Diese sieht als wichtige Neuerung in Compliance-Fragen die Einführung der Risikoanalyse in das Datenschutzrecht vor. Diese Privacy Impact Assessments (PIA) dienen dem präventiven Schutz personenbezogener Daten. Unternehmen sollen immer dann zu dieser Folgenabschätzung verpflichtet sein, wenn die Verarbeitung der Daten auf Grund ihres Wesens, ihres Umfangs und ihrer Zwecke konkrete Risiken für Rechte und Freiheiten betroffener Personen birgt (vgl. Art. 33. Abs. 1 des derzeitigen Entwurfs der EU-GVO).

Die EU-GVO selbst macht zum Vorgehen bei einer Folgenabschätzung nur recht allgemeine Vorgaben. Die folgenden Phasen sollten dem Grundsatz nach aber jedenfalls bei der Durchführung von PIAs absolviert werden:

- In einem ersten Schritt sollte ein Unternehmen feststellen, ob die Durchführung eines PIA grundsätzlich angezeigt ist. Kriterium hierfür ist die Frage, ob das Projekt personenbezogene Daten berührt oder auch nur berühren könnte. Die Größe des Projekts, die Sensibilität der Daten, das verwendete Datenvolumen

und die potentielle Zahl der Betroffenen geben vor, mit welchem Aufwand das PIA betrieben werden muss und wieviel Zeit und Ressourcen dafür einzuplanen sind.

- Nach Prüfung des Bedarfs für ein PIA sollte das Team zur Durchführung zusammengestellt, Verantwortlichkeiten zugewiesen und ein Plan aufgestellt werden, der aber für notwendige Änderungen und Ergänzungen offen bleiben sollte.
- Anschließend wird das zu prüfende Projekt erfasst und verstanden, also eine Abgrenzung des Prüfungsgegenstandes vorgenommen, der Kontext des Projektes erfasst und typische Abläufe und Fälle entwickelt, um diese überprüfbar zu machen.
- In einer folgenden Audit-Phase wird das Projekt im Detail geprüft, also die Datenflüsse analysiert, die zugrundliegenden IT-Systeme und Schnittstellen erfasst und die Verarbeitungsprozesse und Rollen sowie insbesondere auch die Motive der Beteiligten analysiert. Die Projektmitglieder werden befragt und ihr Bewusstsein für den Datenschutz gefördert.
- Anschließend gilt es, die datenschutzrechtlichen Risiken zu erfassen, ihre Auswirkungen zu analysieren und den Handlungsbedarf abzuschätzen. Auf dieser Grundlage werden Maßnahmen zur Sicherung des Datenschutzes empfohlen.
- Das Ergebnis wird in Berichten niedergelegt und im Unternehmen kommuniziert. Im Verlauf des Projekts wird überprüft, ob die empfohlenen Maßnahmen auch umgesetzt werden, und das Ganze dokumentiert.

Auswahl und Schulung von Mitarbeitern

Auf die haftungsrechtlichen Risiken, die datenschutzrechtliche Verstöße nach sich ziehen können, wurde bereits in Abschnitt 2.1.1 eingegangen. Insbesondere einer Verletzung der Organisationspflicht können das Unternehmen und die Geschäftsleitung nur entgehen, wenn sie ihre Mitarbeiter hinreichend sensibilisieren und schulen. Die Bedeutung des Datenschutzes muss mehr denn je von der Geschäftsleitung betont und vorgelebt werden. Im ganzen Unternehmen sollte ein grundlegendes Verständnis der neuen Analysemöglichkeiten, die Big Data bietet, ebenso wie eine Sensibilität für die rechtlichen Grenzen dieser Anwendungen verbreitet werden.

Die wesentlichen Unterschiede von Big Data im Vergleich zu bisher bekannter Datenverarbeitung erfordern neue Kompetenzen im Unternehmen. Sie erfordern neue Kenntnisse und Fähigkeiten bei allen involvierten Mitarbeitern aus allen betroffenen Fachbereichen, also insbesondere in den Bereichen Unternehmensentwicklung und IT. Um diese Kompetenzen aufzubauen, kommen verschiedene Möglichkeiten in Betracht. Vor allem ist natürlich an ein Training der betroffenen Mitarbeiter zu denken. Insbesondere für die Berufsgruppen Anwendungsentwickler, Datenarchitekt, Business Intelligence Analyst, Datenbankadministrator und Systemadministrator ist eine solche Weiterbildung empfehlenswert. Sie werden sich insbesondere Kenntnisse über neue Big-Data-Technologien und -Systeme aneignen müssen. Aber auch neue Expertenprofile mit neuen Berufsbildern können in Zukunft entwickelt werden. Auch wenn es dafür bislang in Deutschland keine entsprechenden Ausbildungsgänge gibt, ist der Bedarf an diesen Spezialisten hoch.

2.2. Hinweise für Fachabteilungen

2.2.1. Informiertheit der Betroffenen

Rechtliche Anforderungen

Damit personenbezogene Daten in rechtlich zulässiger Weise erhoben, verarbeitet oder genutzt werden dürfen, sind, wie bereits ausführlich erläutert, konkrete Vorgaben einzuhalten, die der Gesetzgeber im Bundesdatenschutzgesetz (§§ 4 f., 33 BDSG) aufzählt. Grundsätzlich dürfen personenbezogene Daten demnach nur dann erhoben, verarbeitet oder genutzt werden, wenn entweder eine Rechtsvorschrift dies erlaubt oder eine Einwilligung des Betroffenen vorliegt.

Liegt eine dieser Voraussetzungen vor, muss eine weitere Hürde genommen werden. Der Betroffene muss darüber informiert werden, wer die Daten erhebt, verarbeitet und nutzt, zu welchem konkreten Zweck die Daten genutzt werden und wer alles auf die Daten zugreifen kann, vgl. § 4 Abs. 3 BDSG. Die Informationspflicht trifft die verantwortliche Stelle bereits bei der erstmaligen Erhebung, Verarbeitung oder Nutzung der Daten und gilt selbst dann, wenn personenbezogene Daten nur zur Übermittlung im geschäftsmäßigen Verkehr gespeichert werden. Der Betroffene hat ein Recht darauf, zu erfahren, wer weshalb welche Daten von ihm kennt und nutzt.

Allerdings gibt es von dem Grundsatz der Informiertheit zahlreiche Ausnahmen. Handelt es sich bei der datenverarbeitenden Stelle um ein privates Unternehmen, beschreibt § 33 BDSG, in welchen Fällen der Betroffene nicht informiert werden muss. Die Pflicht zur Benachrichtigung entfällt für die verantwortliche Stelle in besonderen Fällen. Die Art der Benachrichtigung des Betroffenen ist formfrei; die verantwortliche Stelle kann also frei wählen. Es empfiehlt sich jedoch die Schriftform, um einen Beweis vorliegen zu haben. Ein Verstoß gegen die Informationspflicht kann ein Bußgeld nach sich ziehen.

Problembereiche und Grenzen von Big Data

Die beschriebene Informationspflicht besteht aber nicht nur, wenn personenbezogene Daten erstmals in einem Computer erfasst werden. Sie gilt auch, wenn Personendaten aus einer herkömmlichen Anwendung in eine Big-Data-Anwendung übernommen oder herkömmliche Datenbestände in Big-Data-Anwendungen eines anderen Unternehmens zusammengeführt werden. Solche Übermittlungen stellen eine Datenerhebung durch das Empfängerunternehmen dar, über die die Betroffenen informiert werden müssen.

Das Problem dabei ist, dass bei Big-Data-Anwendungen erst auf der großen Datenbasis überhaupt festgestellt wird, welche Verwendungen möglich und sinnvoll sind. Unternehmen müssen sich deshalb jeweils fragen, ob sie überhaupt im Vorfeld einen Verarbeitungsvorgang so genau umschreiben können, dass sie vorab informieren können. Sofern eine Big-Data-Anwendung für eine Vielzahl von Unternehmen mit nicht eindeutig bestimmten Daten für noch nicht feststehende Zwecke arbeitet, stößt die Möglichkeit der Vorabinformation an praktische Grenzen und birgt damit für die beteiligten Unternehmen rechtliche Risiken.

2.2.2. Die Einholung datenschutzrechtlicher Einwilligungen

Wenn es keine gesetzliche Erlaubnis gibt, die eine vorgesehene Big-Data-Anwendung gestattet, ist das verantwortliche Unternehmen darauf angewiesen, Einwilligungen der betroffenen Personen einzuholen. Die Betroffenen müssen vor dem jeweiligen Vorhaben ausdrücklich erklären, dass sie mit der geplanten Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten einverstanden sind.

Diese auf den ersten Blick einfach erscheinende Lösung ist in der Unternehmenspraxis jedoch mit vielfältigen Problemen verbunden. Denn das Datenschutzrecht (vgl. § 4a Abs.1 BDSG) stellt eine Reihe strenger Anforderungen, die zwingend eingehalten werden müssen, damit eine eingeholte Einwilligung als rechtswirksam anzusehen ist. Insbesondere im Kontext von Big-Data-Anwendungen ist die Gefahr groß, dass Einwilligungserklärungen hinter diesen Vorgaben zurückbleiben. Gelingt es einem Unternehmen nicht, eine rechtlich fehlerfreie Einwilligung zu erhalten, dann kann nicht nur die jeweilige Datenverwendung, sondern die ganze Big-Data-Anwendung unzulässig sein.

2.2.2.1. Rechtliche Anforderungen und mögliche Konflikte und praktische Grenzen der Einwilligung im Rahmen von Big Data

Wie also können Sie eine Einwilligung wirksam und damit rechtssicher einholen? In jedem Fall muss die Einwilligung zeitlich stets vor der ersten Datenerhebung vorliegen. Des Weiteren definiert das Bundesdatenschutzgesetz (BDSG) für eine Einwilligungserklärung bestimmte inhaltliche und formale Anforderungen.

Außerdem müssen sich Einwilligungen an den gesetzlichen Vorschriften des Bürgerlichen Gesetzbuches (BGB) für Allgemeine Geschäftsbedingungen (AGB) messen lassen, wenn das Unternehmen – etwa in einem Vertrag mit dem Kunden – die Einverständniserklärung vorformuliert. Im sehr praxisrelevanten Bereich der Werbung sind zusätzlich die Regelungen des Gesetzes über den unlauteren Wettbewerb (UWG) zu beachten.

Inhaltliche Vorgaben

Freiwilligkeit

Als inhaltliche Grundvoraussetzung einer wirksamen Einwilligung fordert das Gesetz zunächst eine freie Entscheidung der einwilligenden Person. Es kann problematisch sein, wenn Unternehmen bestimmte Leistungen von der Einwilligung in Big-Data-Anwendungen abhängig machen, obwohl diese nicht mit der eigentlichen Leistung zusammenhängen. Solche Klauseln, die der Betroffene vorformuliert akzeptieren muss, um die Leistung in Anspruch nehmen zu können, müssen verhältnismäßig sein. Allgemein verboten sind sie nicht. Dies gilt mit Besonderheiten selbst im Bereich der Werbung. Die geforderte Freiwilligkeit steht Big-Data-Anwendungen also prinzipiell nicht entgegen. Die Einwilligung kann aber unwirksam sein, wenn die Grenze der Verhältnismäßigkeit überschritten wird, etwa durch übermäßige Belohnungen für den Einwilligenden.

Informierte Einwilligung

Eine bewusste Einwilligung setzt voraus, dass der Betroffene ausreichend über die Sachlage informiert ist. In vielen Fällen von Big Data stehen eingesetzte Verfahren der Datenanalyse, erzielte Ergebnisse und deren

anschließende Verwendung vorab noch nicht abschließend fest. Vielmehr ergeben sich mögliche zukünftige Anwendungen erst durch die Big-Data-Analyse selbst. Dies kollidiert mit dem Erfordernis einer informierten Einwilligung. Denn da bei dynamischen Prozessen auch die verantwortlichen Unternehmen nicht abschließend wissen, wohin die Analyse führt, können sie auch die Betroffenen nicht hinreichend informieren, in welche Verarbeitungsvorgänge und -zwecke sie einwilligen sollen.

Bestimmtheit

In engem Zusammenhang mit diesen Informationspflichten steht die datenschutzrechtlich geforderte Bestimmtheit der Einwilligungserklärung. Der Inhalt der Erklärung muss konkret abgefasst sein. Vielfach sind aber Komplexität, Dynamik und Charakteristika von Big-Data-Analysen mit dem Bestimmtheitserfordernis unvereinbar. Regelmäßig stehen weder die in Big-Data-Anwendungen genutzten Daten noch die einzelnen Schritte ihrer Verarbeitung oder späteren Verwendung fest. Vielmehr sollen Daten aus unterschiedlichsten Quellen extrahiert und für alle möglichen Zwecke genutzt werden. Zudem ergeben sich durch Zusammenführungen und Kontextänderungen stetig neue Arten und Verwendungen von Daten. Das Einholen einer einmalig vorab erteilten und hinreichend bestimmten Einwilligungserklärung ist damit praktisch nicht möglich.

Aber auch ein späteres Einholen einer neuen, angepassten Einwilligungserklärung ist kein tauglicher Lösungsansatz. Denn es scheint weder praktikabel noch wirtschaftlich, die vielen Betroffenen im riesigen Volumen eines Big-Data-Bestandes zu identifizieren und um ihr Einverständnis zu den entsprechenden Änderungen zu ersuchen. Auch aus diesen Gründen scheidet die Einwilligung als Ermächtigungsgrundlage für Big-Data-Anwendungen in aller Regel aus.

Unternehmen sollten also die Funktionsweise und Zielsetzung geplanter Big Data-Anwendungen genau hinterfragen, um von den Betroffenen eingeholte Einwilligungserklärungen so weit wie möglich an den gesetzlichen Vorgaben zu orientieren. Sobald aber mögliche zukünftige Anwendungen durch die Big-Data-Analyse selbst erst erschlossen werden sollen, kann wegen der dann nicht mehr zu gewährleistenden Information, Transparenz, Zweckbindung und Bestimmtheit die jeweilige Big-Data-Anwendung nicht mehr rechtssicher allein auf eine Einwilligung gestützt werden. Um datenschutzrechtliche Compliance herzustellen, sind dann weitere Maßnahmen, etwa die Anonymisierung der verwendeten Daten zu ergreifen.

Transparenz

Big-Data-Analysen basieren auf komplexen mathematischen Verfahren. Auswertungsalgorithmen oder andere wichtige Elemente werden von den jeweiligen Unternehmen in aller Regel als Betriebsgeheimnisse geheim gehalten. Infolgedessen kann der Einwilligende nicht in Erfahrung bringen, auf welche Weise welche seiner personenbezogenen Daten generiert und ausgewertet werden. Und selbst wenn das Unternehmen sein Vorgehen gar nicht geheim halten will, kann es die Verarbeitung aufgrund ihrer Komplexität nicht immer transparent machen. Die meisten Big-Data-Anwendungen sind deshalb intransparent. Daraus allein folgt noch nicht zwingend, dass die Verwendung der Daten unzulässig ist. Die Intransparenz führt aber dazu, dass die eingeholten Einwilligungen nicht immer eine rechtssichere Grundlage bilden.

2.2.3. Prüfung der gesetzlichen Erlaubnis

Wie bereits beschrieben, gilt im Datenschutzrecht der Grundsatz des Verbots mit Erlaubnisvorbehalt. Das heißt: Jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist verboten, wenn sie nicht ausnahmsweise per Gesetz erlaubt oder gar angeordnet sind oder eine wirksame Einwilligung des Betroffenen vorliegt.

Da die Probleme mit der Einwilligung bereits ausführlich diskutiert worden sind, wird an dieser Stelle nur noch die Prüfung einer gesetzlichen Erlaubnisnorm erörtert. Es ist zu berücksichtigen, dass sich grundsätzlich gesetzliche Erlaubnistatbestände auf vier verschieden Ebenen finden lassen:

- fach- und bereichsspezifische Rechtsnormen des Bundes
- andere nachrangige Rechtsvorschriften
- Zweckbestimmung eines Vertragsverhältnisses
- Bundesdatenschutzgesetz

2.2.4. Anonymisierung / Pseudonymisierung

Für eine erfolgreiche Anwendung und Analyse von Big Data müssen Fachabteilungen eine kennzahlenbasierte Anonymisierung realisieren. Ziel muss dabei sein, dass die resultierenden anonymen Datensätze auch weiterhin untereinander in Bezug gesetzt werden können.

Ein wesentliches Charakteristikum von Big Data sind die Bezugsmöglichkeiten zwischen den verschiedenen gespeicherten Datensätzen. So sollten Datensätze, die ursprünglich anhand einer bestimmten Kennzahl untereinander zuordenbar waren, auch im Zustand der Anonymität anhand einer Kennzahl zuordenbar bleiben. Es darf jedoch nicht oder nur unter unverhältnismäßig großen Umständen möglich sein, von der anonymisierten Kennzahl auf die ursprüngliche personenbezogene Kennzahl zu schließen. Um das zu gewährleisten, benötigen Sie eine Kombination technischer und organisatorischer Maßnahmen.

Beispielsweise wird aus einzelnen personenbezogenen Daten durch ein geeignetes Hash-Verfahren zunächst ein Pseudonym generiert. In diesem Stadium ist jedoch noch ein Rückschluss auf den Personenbezug denkbar, denn da der für das Hash-Verfahren eingesetzte Schlüssel für einen bestimmten Zeitraum konstant sein muss, könnte das Hash-Verfahren (ggf. wiederholt) durchlaufen und dabei jeweils der Input (personenbezogene Kennzahl) und der erzeugte Output (verschlüsselte Kennzahl) in einer sogenannten Referenzliste zusammen gespeichert werden. Auch wenn ein Unternehmen die Zugriffsrechte so auf verschiedene Mitarbeiter verteilt, dass jeder nur einen Teil dieses Verschlüsselungsprozesses beeinflussen kann, kann man für die Rückschlussmöglichkeit wohl noch nicht von einem „unverhältnismäßigen Aufwand“ sprechen, wie er für die Anonymität gefordert ist. Allerdings könnte bei einer Aufspaltung von personenbezogener Kennzahl und verschlüsselter Kennzahl auf zwei unterschiedliche Unternehmen von einem solchen Aufwand ausgegangen werden.

Am Beispiel der längerfristigen Speicherung von Standortdaten wird deutlich, wie schnell die Gefahr einer direkten De-Anonymisierung realisierbar ist. Wenn etwa eine einzelne Information relativ eindeutig einem einzelnen Individuum oder einer kleinen Gruppe von Individuen zugeordnet werden kann, muss technisch für jeden Standort sichergestellt werden, dass die anfallenden Standortdaten stets von einer gewissen Mindestzahl an Individuen stammen, bevor sie für weitere Verarbeitungsstufen freigegeben werden. Diese Mindestzahl muss auch in einem bestimmten Prüfungszeitraum vorliegen. Andernfalls könnten etwa in einer dünn besiedelten Region Standortdaten von GPS- oder Mobilfunkservices mit Daten etwa aus Melderegistern verknüpft werden und so eine Rückverfolgung bis hin zur tatsächlichen Identität der betroffenen Person stattfinden. Können die genannten Mindestvoraussetzungen, also Mindestzahl an Individuen und bestimmter Prüfungszeitraum, nicht gewährleistet werden, sind die gesammelten Daten zu verwerfen.

Durch die oben beschriebene Bezugsmöglichkeit zwischen den unterschiedlichen Datensätzen, die Big Data immanent ist, besteht bei der Verarbeitung und Speicherung entsprechend anonymisierter Datensätze jedoch gleichzeitig auch die Gefahr einer indirekten De-Anonymisierung. Das trifft zu, wenn durch die Kombination von Kennzahlen ein mehr oder minder eindeutiges Muster auslesbar ist, das wiederum auf eine bestimmte Person rückführbar ist.

Es ist also erkennbar, dass durch eine sinnvolle zeitliche Beschränkung der Bezugsmöglichkeit einzelner Datensätze ein wichtiges Grundprinzip für eine anonyme Verarbeitung gerade von Standortdaten berücksichtigt wird. Auf technischer Seite wird diese Anforderung durch einen regelmäßigen Wechsel des Schlüssels zur Erzeugung der anonymen Kennung unterstützt. Für eine unzulässige Profilbildung (und einen möglichen Missbrauch) ist diese Datenbasis dann unzureichend.

Wie können dann aber Auswertungen über einen längeren Zeitraum vollzogen werden? Gerade Langzeitaussagen bieten oftmals weitaus wertvollere Erkenntnisse, denn nur bei einem längerfristigen Prüfungszeitraum können auch Unregelmäßigkeiten beachtet werden. Dazu ist es geboten, sogenannte „aggregationsbasierte Langzeitindizes“ zu erzeugen. Das bedeutet, dass die Berechnung auf Grundlage mehrerer bereits aggregierter Werte erfolgt, die jeweils anhand eines einzelnen kurzfristigen Bezugszeitraums ermittelt wurden. Es wird also nicht ein solcher Wert direkt aus einer Vielzahl der über einen langen Zeitraum gesammelten personenbezogenen Daten abgeleitet.

Technisch wird dafür zunächst ein aggregierter Wert für eine vorab festgelegte Fragestellung ermittelt, der eine statistische Häufigkeits- oder Wahrscheinlichkeitsaussage für den jeweiligen kurzfristigen Bezugszeitraum darstellt. Durch Verschlüsselungstechniken können diese Kurzzeitaussagen anschließend über einen längeren Zeitraum in Bezug gesetzt werden. Eine Relation von mehreren Kurzzeitaussagen führt schließlich zu den gewünschten Langzeitaussagen.

2.2.5. Nutzung allgemein zugänglicher Daten

Der in Kapitel 1 angesprochene Grundsatz der unbeschränkten Nutzungsmöglichkeit von allgemein zugänglichen Daten bedeutet im Umkehrschluss nicht, dass Big-Data-Analysen solcher Daten keinen Einschränkungen unterliegen. Sie müssen für jeden Auswertungsfall im Einzelnen überprüfen, ob ein Datum tatsächlich aus einer allgemein zugänglichen Quelle stammt und ob nicht das Interesse der verantwortlichen Stelle von einem schutzwürdigen Interesse des Betroffenen überwogen wird (§§ 28 Abs. 1 S. 1 Nr.3, 29 Abs. 1 S. 1 Nr. 2 BDSG). Voraussetzung ist mithin zunächst, dass die Daten, die für Big-Data-Anwendungen genutzt werden sollen, öffentlich zugänglich sind. Das gilt nur für Daten, die sowohl von der Intention als auch von der eingesetzten Technik her nicht auf den Zugriff durch einen eingeschränkten Nutzerkreis beschränkt sind. Hier sind Quellen wie Medien und das Telefonbuch gemeint. Internetdaten müssen zur Erfüllung dieser Voraussetzung also von jedermann einsehbar sein. Bedarf es einer zusätzlichen Authentisierung oder Autorisierung, wie etwa bei einem sozialen Netzwerk, so handelt es sich nicht um öffentlich zugängliche Daten.

Liegen nun Daten vor, die einer öffentlich zugänglichen Quelle entstammen, verlangen die gesetzlichen Vorgaben weiter, dass die Interessenabwägung nicht zu Lasten der schutzwürdigen Interessen des Betroffenen ausfällt. Ob die Erhebung mithin zulässig ist, ist wohl letztlich von der Sensibilität der Daten abhängig, die in Rede stehen.

Zulässig ist bei einer Weiterverarbeitung öffentlich zugänglicher Massendaten jedoch auch eine Pauschalierung möglicher schutzwürdiger Interessen, wenn und soweit eine Einzelfallprüfung nicht möglich ist.

Fazit

Die Grundlagen des Datenschutzrechts in Deutschland und Europa sind fast zwei Jahrzehnte alt und stammen damit aus einer Ära, in der das Internet tatsächlich noch Neuland war. Niemand konnte damals absehen, auf welch tiefgreifende Weise die Digitalisierung das Alltags- und Wirtschaftsleben verändern würde. Ebenso wenig war absehbar, dass Daten einmal zum vierten Produktionsfaktor neben Arbeit, Kapital und Rohstoffen werden würden. Darum ist es auch nicht verwunderlich, dass dieses Datenschutzrecht keine einfach zu handhabende Grundlage für die Anwendung der sich rasant entwickelnden Big-Data-Technologie bildet. Es gibt jedoch, wie beschrieben, einige gangbare Wege, die Unternehmen beschreiten können, um die Möglichkeiten von Big Data zu nutzen, ohne gegen das Datenschutzrecht zu verstoßen.

Weiterführende Links

Artegic AG (2014): „Checkliste: 23 Fragen zu Big Data und Recht“
https://www.artegic.de/files/0,0/2129/artegic_checkliste_23_Fragen_Version_artegic_03_12_14.pdf

Berliner Beauftragter für Datenschutz und Informationsfreiheit (2013). „Dokumente zu Datenschutz und Informationsfreiheit“
http://www.datenschutz-berlin.de/content/veroeffentlichungen/dokumente

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2013): „Management von Big-Data-Projekten“
http://www.bitkom.org/files/documents/LF_big_data2013_web.pdf

Bundesamt für Sicherheit in der Informationstechnik (2012): „Leitfaden Informationssicherheit – IT-Grundschutz kompakt“
http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

Bundesministerium der Justiz und für Verbraucherschutz: „Das Bundesdatenschutzgesetz“:
http://www.gesetze-im-internet.de/bdsg_1990/index.html

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit:
http://www.bfdi.bund.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: *Informationsseite Datenschutz*:
https://www.ldi.nrw.de/mainmenu_Datenschutz/index.php

Rechtlicher Hinweis

Die vorstehenden Angaben und Aussagen stellen keine Anlage-, Rechts- oder Steuerberatung dar. Die verwendeten Daten stammen aus unterschiedlichen Quellen und wurden als korrekt und verlässlich betrachtet, jedoch nicht unabhängig überprüft; ihre Vollständigkeit und Richtigkeit sind nicht garantiert, und es wird keine Haftung für direkte oder indirekte Schäden aus deren Verwendung übernommen, soweit nicht durch grobe Fahrlässigkeit oder vorsätzliches Fehlverhalten unsererseits verursacht.
Alle Meinungen können ohne vorherige Ankündigung und ohne Angabe von Gründen geändert werden.
Die vorstehenden Aussagen werden lediglich zu Informationszwecken des Auftraggebers gemacht und ohne darüber hinausgehende vertragliche oder sonstige Verpflichtung zur Verfügung gestellt.
Soweit in vorstehenden Angaben Prognosen oder Erwartungen geäußert oder sonstige zukunftsbezogene Aussagen gemacht werden, können diese Angaben mit bekannten und unbekannten Risiken und Ungewissheiten verbunden sein. Es kann daher zu erheblichen Abweichungen der tatsächlichen Ergebnisse oder Entwicklungen zu den geäußerten Erwartungen kommen. Neben weiteren hier nicht aufgeführten Gründen können sich insbesondere Abweichungen aus der Veränderung der allgemeinen wirtschaftlichen Lage, der Entwicklung der Finanzmärkte und Wechselkurse sowie durch Gesetzesänderungen ergeben.
Das Handelsblatt Research Institute verpflichtet sich nicht, Angaben, Aussagen und Meinungsäußerungen zu aktualisieren.

Es gelten die Allgemeinen Geschäftsbedingungen des Handelsblatt Research Institute.