artegic Bird&Bird

CHECKLISTE: 23 FRAGEN ZU BIG DATA UND RECHT

artegic Bird & Bird

INHALT

VORWORT

Big Data ist das Thema der Stunde. In der digitalen Wirtschaft hat sich Big Data zu einem wichtigen Wertschöpfungsfaktor entwickelt, den kaum ein Unternehmen noch ausser Acht lassen kann. Doch die Erfassung und Verarbeitung von großen Datenmengen unterliegt, insbesondere im kommerziellen Umfeld, einer Reihe gesetzlicher Vorschriften. Die nachfolgende Checkliste hilft dabei, rechtliche Fallstricke im Umgang mit Big Data zu vermeiden.

„Big Data ist ein Thema an dem Unternehmen, insbesondere in der digitalen Wirtschaft, kaum noch vorbei kommen. Zeitgleich steigt die Sensibilität für das Thema Datenschutz in den Medien, in der Öffentlichkeit, beim Gesetzgeber und auch bei Entscheidern in Unternehmen. Unsere Erfahrungen aus der Beratungspraxis zeigen, dass der Datenschutz mittlerweile als zentrales Thema auf Ebene von Geschäftsführung und Vorstand verankert ist. Grund hierfür ist, dass zum einen die richtige Nutzung von Big Data heutzutage ein wesentlicher Wettbewerbsvorteil geworden ist, zum Anderen Rechtssicherheit und Datenschutz im Big Data Umfeld jedoch unerlässlich sind. Die meisten Unternehmen im Markt verfügen prinzipiell über ein sehr gutes Verständnis vom Thema Datenschutz. Neue Entwicklungen wie Big Data führen jedoch auch immer wieder zu Unsicherheit. Welche Datenerhebungen bzw. –auswertungen bedürfen der Zustimmung? Gibt es eine Bindung erhobener Daten für einen bestimmten Zweck? Wie ist mit automatisierten Entscheidungen aus der Daten-Analyse umzugehen? Diese und weitere Fragen soll die vorliegende Checkliste beantworten."

DR. FABIAN NIEMANN (BIRD & BIRD)
E-Mail: Fabian.Niemann@twobirds.com

artegic Bird & Bird

01

WAS IST BIG DATA?

Die Zahl Daten-produzierender Anwendungen und Endgeräte nimmt kontinuierlich zu, während gleichzeitig die Kosten für die Speicherung und Verarbeitung großer Datenmengen sinken. Dies führt dazu, dass die Menge erfasster Daten, insbesondere in Unternehmen aber auch in Behörden, in der Forschung und sonstigen Stellen stetig zunimmt. Dieses Phänomen wird aktuell diskutiert unter dem Schlagwort Big Data. Laut einer Umfrage von IBM werden unter Big Data von Managern solche Begriffe wie „Große Bandbreite an Informationen", „Neue Arten von Daten Analyse", „Echtzeitinformationen", „Moderne Medienarten", „Datenzustrom", „Große Datenmengen" oder auch „Daten aus sozialen Medien" subsummiert. Die Definition der wissenschaftlichen Dienste des deutschen Bundestags lautet: „Big Data bezeichnet große Datenmengen aus vielfältigen Quellen, die mit Hilfe neu entwickelter Methoden und Technologien erfasst, verteilt, gespeichert, durchsucht, analysiert und visualisiert werden können".

Big Data ist jedoch kein alleiniges Thema der Informationstechnologie mehr. Datensammlung und -verarbeitung ist kein Selbstzweck. Sie ist mehr und mehr die Basis, um Informationen zu generieren, aus denen Wissen abgeleitet werden kann, das zur Erfüllung von Unternehmenszielen im betrieblichen Alltag beiträgt aber auch in anderen Lebensbereichen wie z.B. der Medizin oder im Auto Einzug hält und unsere Lebenswelten weiter verändern wird. Bezogen auf die Erreichung wirtschaftlicher Ziele muss Big Data also in erster Linie zielgerichtet sein. Insbesondere für das Marketing steht Big Data für Erkenntnisgewinn und eröffnet somit neue Potentiale, welche direkt auf den Umsatz einzahlen.

artegic Bird & Bird

02

WELCHE UNTERSCHIEDLICHEN TYPEN VON DATEN GIBT ES BEISPIELSWEISE IM MARKETING?

Daten sind nicht gleich Daten. Insbesondere im Marketing gilt es, nicht einfach nur Daten zu erfassen, sondern die richtigen Daten, die auch zweckmäßig eingesetzt werden können. Marketing-relevante Typen von Daten sind etwa folgende:

- Nutzungs-/Reaktionsdaten in digitalen Kanälen (z.B. E-Mail, Social Media, Website): Öffnungen, Klicks, Conversions, Nutzungsdauer, Social Shares, besuchte Websites usw.
- Technische Daten: IP-Adresse, Browser, Endgeräte, E-Mail-Client, installierte Plug-Ins usw.
- Transaktionsdaten aus Online Shops: gekaufte Produkte, generierter Umsatz, letzter Kauf, Retouren-Quote, Kauffrequenz, Preissensibilität usw.
- Ortsbezogene Daten: Standort stationär (ermittelt durch IP-Adresse), Standort mobil (ermittelt z.B. durch GPS oder Bluetooth) usw.
- Soziodemografische Daten: Alter, Geschlecht, Wohnort, Familienstand, Beruf usw.

artegic Bird&Bird

03

WELCHE RECHTLICHEN REGELUNGEN SIND EINSCHLÄGIG?

Für „Big Data" gelten die allgemeinen Gesetze, es gibt keine spezialgesetzlichen Regelungen hierfür im deutschen Recht. Für die Speicherung und kommerzielle Verwertung von „Big Data" sind insbesondere das Urheber- und Datenschutzgesetz relevant, daneben spielen das Telemediengesetz und das allgemeine Zivilrecht (namentlich das Bürgerliche Gesetzbuch – BGB) eine Rolle. Diese Gesetze regeln insbesondere, wem die Daten gehören und inwieweit sie von Unternehmen genutzt werden dürfen.

Das Urhebergesetz (UrhG) ist anwendbar, wenn und soweit Audio-, Video- und Bilddateien oder auch größere Texte verarbeitet oder übermittelt werden sollen, also Werke, die Urheberschutz genießen. In diesen Fällen ist eine Nutzung von entsprechenden „Big Data" ggf. nur mit Zustimmung der Rechteinhaber möglich (siehe dazu Frage 4.). Einzelne Informationen/Daten (und damit ein großer Teil von Big Data) sind jedoch vom Urheberrecht nicht erfasst und unterliegen folglich auch den urheberrechtlichen Beschränkungen nicht. Jedoch können Sammlungen von Daten urheberrechtlich oder als Datenbank geschützt sein. Wenn daher ganze Sammlungen oder Datenbanken (oder wesentliche Teile davon) übernommen werden, gelten wieder die obigen urheberrechtlichen Einschränkungen.

Beim Erheben, Speichern, Verarbeiten, Nutzen und Übermitteln von Daten sind des Weiteren immer die Vorgaben des Bundesdatenschutzgesetzes (BDSG) zu beachten. Seiner Konzeption nach, so viele Daten wie möglich zu sammeln und zu verwerten, steht „Big Data" in einem natürlichen Spannungsfeld zu den bisherigen Grundsätzen des deutschen Datenschutzrechts. Dieses geht vom Prinzip der Datensparsamkeit bzw. Datenminimierung aus. Danach dürfen grundsätzlich nicht mehr als die für den jeweiligen Vorgang erforderlichen personenbezogenen Daten erhoben und verarbeitet werden und grundsätzlich sollen personenbezogene Daten so wenig wie möglich gespeichert und genutzt werden. Wenn möglich, sollten Daten deshalb immer anonymisiert werden. Allgemein gilt, dass das Datenschutzrecht überaltert ist und nicht wirklich für die aktuellen technischen und technologischen Entwicklungen wie Big Data oder Cloud Computing passt (und es steht zu befürchten, dass etwaige Anpassungen – etwa im Rahmen der geplanten EU-Datenschutzgrundverordnung – die Nutzung durch die Wirtschaft nicht vereinfachen). Das aktuelle, geltende Recht ist daher im Licht der technologischen und gesellschaftlichen Entwicklungen auszulegen und einen Kompromiss zwischen (strengem) Datenschutz und der Realität von Big Data Anwendungen zu finden.

Darüber hinaus können auch die datenschutzrechtlichen Vorschriften des Telemediengesetzes (TMG) relevant werden, die für Anbieter von Waren oder Dienstleistungen mittels einer Webseite gelten.

Schließlich kann auch das BGB relevant werden, insbesondere die Regeln zum Sacheigentum. Denn Eigentum kann auch an Daten und Datenträgern bestehen. Wenn beispielsweise von der Automobil- oder Versicherungsindustrie im Bereich der Telematik auf Daten in Autos (Black Box) zugegriffen wird, fragt sich, ob dies ein Eingriff in das Eigentum des Fahrzeugeigentümers ist und seine Zustimmung erfordert.

artegic Bird & Bird

04

WELCHE DATENERHEBUNGEN BZW.– AUSWERTUNGEN BEDÜRFEN DER ZUSTIMMUNG?

Maßgeblich sind hier Urheberrecht (soweit einschlägig), Datenschutzrecht und BGB.

Nach dem UrhG ist eine urheberrechtlich relevante Nutzung (also insbesondere eine Speicherung der Daten und ihre öffentliche Zurverfügungstellung) von urheberrechtlich geschützten Werken (siehe Frage 3.) grundsätzlich nur mit Zustimmung der Inhaber der Verwertungsrechte an den Werken zulässig; ohne eine solche Zustimmung ist eine relevante Nutzung nur in sehr eingeschränktem Umfang im Rahmen urheberrechtlicher Schrankenbestimmungen erlaubt, insbesondere – unter bestimmten Umständen – zum wissenschaftlichen oder privaten Gebrauch. Die gewerbliche Nutzung urheberrechtlich geschützter Big Data wird dagegen regelmäßig die Zustimmung der Rechteinhaber erfordern. Wichtig ist, dass Informationen/Daten an sich vom Urheberrecht nicht erfasst sind (soweit nicht wesentliche Teile von Datenbanken oder Sammlungen übernommen werden) und damit auch die urheberrechtlichen Beschränkungen für diese nicht gelten.

Soweit keine rein anonymen Daten genutzt werden, sondern Daten die (teilweise) auch natürlichen Personen zugeordnet werden können (wie meist bei Big Data), ist aber in jedem Fall das Datenschutzrecht zu beachten. Das deutsche Datenschutzrecht geht von dem Grundkonzept aus, dass die Erhebung und Verwertung von Daten verboten ist. Ausnahmen von diesem Verbot stellen bestimmte gesetzliche Erlaubnisvorschriften oder die Zustimmung des Betroffenen dar (datenschutzrechtliche Rechtfertigung). Dabei unterscheiden sich die Anforderungen danach, ob es sich um allgemeine personenbezogene Daten oder sogenannte Standortdaten oder Verkehrsdaten handelt.

Die Erhebung und Auswertung allgemeiner personenbezogener Daten, d.h. Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Name, Adresse, E-Mailadresse, Familienstand, Beruf, Ausweisnummer, Versicherungsnummer, Telefonnummer) bedürfen der vorherigen Einwilligung des Betroffenen, soweit nicht eine gesetzliche Erlaubnis nach dem BDSG vorliegt.

- Allgemeine personenbezogene Daten sind zunächst insbesondere Bestandsdaten, d.h. solche, die zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertrags-verhältnisses zwischen dem Dienstanbieter und dem Betroffenen über die Nutzung von Telekommunikationsdiensten erforderlich sind (z.B. Name, Alter und Adresse des Betroffenen).

- Allgemeine personenbezogene Daten sind ebenfalls Nutzungsdaten, die eine Inanspruchnahme von Telemedien erst ermöglichen und für deren Abrechnung erforderlich sind (Merkmale zur Identifikation des Betroffenen, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Betroffenen in Anspruch genommenen Telemedien).

- Soweit solche Daten außerhalb des eigentlichen Vertragszweckes im Rahmen von Big Data Analysen und Anwendungen gespeichert und genutzt werden, ist dafür eine

Einwilligung aller natürlichen Personen erforderlich, deren Daten betroffen sind. Das gilt nur dann nicht, wenn ihre Nutzung von einer gesetzlichen Erlaubnis erfasst ist. Hier kommt im Normalfall einzig die sogenannte Interessensabwägung nach § 28 Abs. 1 Nr. 2 BDSG in Betracht. Danach ist eine Nutzung zulässig, wenn berechtigte Interessen des Nutzenden an der Nutzung die des Betroffenen überwiegen. Hier gilt ein strenger Maßstab, der im Rahmen der Nutzung für Forschung, medizinische Zwecke oder ähnliches oftmals erfüllt sein kann, bei rein kommerzieller Nutzung regelmäßig aber nicht. Wer hier auf Nummer sicher gehen will, der benötigt entweder eine Einwilligung oder muss die Daten anonymisieren. In jedem Fall ist stets eine Überprüfung des Einzelfalls erforderlich; pauschale Antworten verbieten sich wie meistens im Datenschutzrecht.

- Verkehrsdaten, d.h. solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (der in Anspruch genommene Telekommunikationsdienst, die Nummer oder die Kennung der beteiligten Anschlüsse (Anrufer und Angerufener), personenbezogene Berechtigungskennungen, die Kartennummer (bei Verwendung von Kundenkarten), eventuelle Standortdaten (bei Mobiltelefonen) sowie der Beginn und das Ende der jeweiligen Verbindung (Datum und Uhrzeit) dürfen nur mit Zustimmung des Betroffenen erhoben werden. Die Verarbeitung dieser Daten zu Marketingzwecken bedarf ebenfalls der Einwilligung des betroffenen Teilnehmers. Zusätzlich müssen die Daten des Angerufenen (der anderen Seite, die in der Praxis nicht einwilligen kann) unverzüglich anonymisiert werden.

- Standortdaten, d.h. Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben, dürfen ebenfalls nur mit Zustimmung des Betroffenen und nur in dem für die Funktion des Dienstes notwendigen Umfang erhoben und verarbeitet werden. Wie auch sonst ist eine Verarbeitung dieser Daten ohne Zustimmung möglich, wenn die Daten anonymisiert wurden.

artegic Bird & Bird

05

HANDELT ES SICH UM PERSONENBEZOGENE DATEN, WENN EINE VERKETTUNG VON DATEN RÜCKSCHLÜSSE AUF EINE PERSON GEBEN KANN?

Die von einer Person erhaltenen Daten führen nicht zwangsläufig direkt dazu, dass Rückschlüsse auf ihre Identität gezogen werden können. Es kommt auf den Einzelfall an. Dabei ist der anzuwendende Maßstab umstritten. Insbesondere ist es umstritten, ob ein an sich anonymes Datum, wie z.B. die IP-Adresse für den Inhaber einer Webseite, ein personenbezogenes Datum sein kann, wenn ein Dritter (bei IP-Adressen: der Internet Service Provider), eine Zuordnung vornehmen kann.

Die deutschen und europäischen Regelungen sind insoweit nicht eindeutig. Im Wesentlichen werden in der juristischen Literatur, von den Datenschutzbehörden und den Gerichten drei verschiedene Ansätze vertreten.

Die von den meisten Datenschutzbehörden gewählte Herangehensweise ist sehr vereinfachend und (zu) restriktiv. Sie gehen davon aus, dass es ausreicht, wenn aus objektiver Sicht (sogenannter „objektiver Datenbegriff") theoretisch die Möglichkeit besteht, dass mithilfe eines Datums eine konkrete Person bestimmbar ist, auch wenn dazu die nutzende Person bzw. das nutzende Unternehmen Informationen von Dritten benötigt. Das gilt unabhängig davon, ob es wahrscheinlich ist, dass eine solche Mitwirkung jemals erfolgt. Relevant ist dies beispielsweise für Big Data Anwendungen, die IP Adressen Profilen zuordnen oder diese anderweitig nutzen. Nach dieser Ansicht ist eine Person neben IP-Adressen auch insbesondere aufgrund folgender Daten bestimmbar: Browser-Fingerprints, Daten eines mobilen Funkgeräts, Kfz-Daten (Fahrzeugnummer, Kennzeichen etc.), mit RFID-Chips ausgestattete Gegenstände, Pseudonyme.

Nach der liberaleren Gegenansicht ist bei der Frage nach dem Personenbezug von Daten nur zu berücksichtigen, inwieweit die konkrete Stelle, welche Daten verarbeitet, die Möglichkeit hat, eine bestimmte Person zu ermitteln (sogenannter „subjektiver Datenbegriff"). Informationen von außerhalb sind hiernach nicht relevant. Nach dieser Ansicht ist insbesondere die IP-Adresse kein personenbezogenes Datum (außer für den Internet Service Provider bei Einzelanschlüssen), da es sich lediglich um eine Zahlenfolge handelt, welche auch im Zusammenhang mit der Angabe, dass zu einer bestimmten Zeit ein Zugriff auf eine bestimmte Webseite erfolgt ist, kein Rückschluss auf eine Person möglich ist.

Unserer Ansicht nach sind beide Seiten zu pauschal und einseitig. Vielmehr ist eine vermittelnde Lösung interessengerecht. Es muss zunächst aus Sicht des jeweiligen Datenverarbeiters bestimmt werden, ob es sich um personenbezogene Daten handelt oder nicht. Dabei können aber auch Daten von Dritten relevant sein, wenn es naheliegend ist, dass dieser Zugriff auf diese Daten hat und mit deren Hilfe die Identität einer konkreten Person bestimmen kann. (Nur) wenn das der Fall ist, liegt ein Personenbezug vor, mit der Folge, dass die datenschutzrechtlichen Anforderungen (insbesondere oftmals Zustimmung, siehe Frage 4.) einzuhalten sind. Für „Big Data" bedeutet dies dennoch, dass im Zweifelsfall personenbezogene Daten involviert sind, da zumeist eine Mischung aus mehreren Datentypen vorliegen wird. Ein Personenbezug ist aber dann auszuschließen, wenn die

Daten bereits vor deren Weiterverarbeitung anonymisiert wurden (vgl. dazu auch Frage 8), wobei für die Anonymisierung aus unserer Sicht nicht die strenge Auffassung der meisten Datenschutzbehörden, sondern die hier vertretene vermittelnde Ansicht maßgeblich ist. Wenn man kein Risiko eingehen möchte, muss man allerdings den strengen Maßstab zugrunde legen.

06

GIBT ES EINE BINDUNG ERHOBENER DATEN FÜR EINEN BESTIMMTEN ZWECK?

ODER KÖNNEN DIE ERHOBENEN DATEN GENERELL VORGEHALTEN UND AUSGEWERTET WERDEN?

Im Datenschutzrecht gilt der Grundsatz der Zweckbindung, d.h. Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Der Betroffene ist bei der Erhebung seiner Daten über die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung der Daten zu informieren.

Werden die Daten für die Erfüllung eigener Geschäftszwecke, d.h. im Zusammenhang mit der Abwicklung von Verträgen oder der Pflege von Kundenkontakten, verwendet, ist eine nachträgliche Änderung des Zwecks zulässig. Die Zweckänderung ist dabei beim Vorliegen berechtigter Interessen des Verarbeitenden, eines Dritten oder der Öffentlichkeit zulässig.

Ein generelles Vorhalten von Daten kommt jedoch auch nach den obigen Grundsätzen der Zweckveränderung nicht in Betracht. Die datenverarbeitende Stelle ist trotzdem verpflichtet, einen bestimmten Zweck für das Vorhalten von Daten festzulegen.

Dies gilt nur dann nicht, wenn es sich ausschließlich um anonyme Daten handelt.

Für „Big Data" bedeutet dies, dass im Zweifel eine neue datenschutzrechtliche Rechtfertigung vor der Verarbeitung der Daten gefunden werden muss (vgl. Fragen 4, 9, 17). Dies ergibt sich daraus, dass alle in dem Daten-Pool enthaltenen Daten möglicherweise zu einem anderen Zweck erhoben wurden, als der Zweck, mit welchem nun die Weiterverarbeitung erfolgen soll.

artegic Bird&Bird

07

DARF MAN ALLE DATEN ZUSAMMENFÜHREN?

DARF ICH INSBESONDERE EXTERNE DATEN HINZUZIEHEN/ABGLEICHEN UND DARF ICH DATENSÄTZE VERSCHMELZEN, WENN ICH GLAUBE, DASS SIE VON EIN UND DEMSELBEN KUNDEN STAMMEN?

Daten zu Kunden entstehen an unterschiedlichen Stellen und für verschiedene Einsatzzwecke. Im Zusammenhang mit „Big Data" ist es in der Tat ein Unterschied, ob bereits ein Daten-Pool vorhanden ist, dessen Daten ausgewertet werden sollen, oder ein solcher erst noch erstellt werden soll. Wenn der Daten-Pool nicht ausschließlich anonyme Daten enthält, so ist für jeden Einzelfall gesondert sowohl zu fragen, ob eine datenschutzrechtliche Rechtfertigung für die Nutzung als auch eine datenschutzrechtliche Rechtfertigung für eine etwaige vorgelagerte Zusammenführung von Daten vorliegt. Dabei sind insbesondere folgende Punkte zu beachten:

- Generell gelten die Grundsätze der Zweckbindung und Datentrennung, d.h. die Daten dürfen jeweils nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Verschiedene Datensätze müssen dementsprechend auch grundsätzlich unabhängig voneinander verwaltet werden. Eine Zusammenführung ist nur aufgrund einer separaten datenschutzrechtlichen Legitimation (entweder Einwilligung oder gesetzliche Rechtfertigung, siehe Frage 4.) zulässig. Die gewerbliche Nutzung – z.B. um die Daten des Kaufprofils im Shop im Newsletter zu verwenden – ist dabei meistens nur nach Einwilligung des Empfängers zulässig (siehe Frage 4.).

- Die Einwilligung muss nicht separat erfolgen, sondern kann Teil der Datennutzungserklärung im Rahmen der Newsletter-Anmeldung oder des Shop-Registrierungsprozesses sein, solange die Einwilligung diesbezüglich klar und verständlich ist. Wenn der Betroffene so z.B. bei der Anmeldung im Shop die Datennutzungserklärung akzeptiert, berechtigt er den Anbieter auch zum Zusammenführen von Daten.

- Gleiches gilt für die Anreicherung mit externen Daten – z.B. zur Aktualisierung von postalischen Anschriften oder Bonitätsdaten sowie zur Anreicherung von E-Mail-Adressen um die darüber genutzten Social Networks, sofern diese Informationen nicht allgemein verfügbar sind.

- Ohne Einwilligung zulässig ist aber die Zusammenführung von listenmäßig gespeicherten Daten mit im Internet frei verfügbaren Informationen für Zwecke der Werbung für eigene Angebote des Online Shop Anbieters als datenschutzrechtlich verantwortlicher Stelle.

artegic Bird & Bird

08

DARF ICH ERKENNTNISSE AUS DER ANALYSE ZUR PROFILIERUNG EINES KUNDENPROFILS NUTZEN?

Beim Erstellen von Nutzerprofilen ist grundsätzlich danach zu unterscheiden, ob es sich um personenbezogene Daten handelt oder nicht (vgl. Frage 5) und ob der Betroffene zugestimmt hat oder nicht: Die deutschen und europäischen Regelungen sind insoweit nicht eindeutig. Im Wesentlichen werden in der juristischen Literatur, von den Datenschutzbehörden und den Gerichten drei verschiedene Ansätze vertreten.

Zulässig ist die Verwendung nicht-personenbezogener Daten ohne Einwilligung des Betroffenen dann, wenn die Daten anonymisiert sind.

Nach den Anforderungen des Bundesdatenschutzgesetzes liegen anonymisierte Daten vor, wenn man die entsprechenden Einzelangaben nicht mehr bzw. nur noch mit einem unverhältnismäßig hohen Aufwand einem bestimmten Betroffenen zuordnen kann. Soweit Einzelangaben einem Betroffenen nicht mehr zugeordnet werden können (sog. „echte" Anonymisierung), können diese Daten ohne Einschränkung für die Verwendung von Webanalysen genutzt werden und insbesondere auch an Dritte übermittelt werden (im Einzelnen zu den Anforderungen an Anonymisierung, siehe Frage 5.). Da ein Wiedererkennen des Betroffenen hier ausgeschlossen ist, bedarf es bei der Erstellung von Nutzerprofilen mittels anonymisierter Daten auch keiner Einwilligung des Betroffenen.

Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten für die Erstellung von Nutzungsprofilen nach den Vorgaben des Telemediengesetzes nur verwendet werden, wenn die Daten pseudonymisiert werden. Unter Pseudonymisieren versteht man das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen (sog. Pseudonym), um die Bestimmung des Betroffenen entweder auszuschließen oder wesentlich zu erschweren. Dabei ist es generell untersagt, die pseudonymisierten Nutzungsprofile mit dem Träger des Pseudonyms zusammenzuführen.

Zudem muss der Betroffene über die Profilbildung unterrichtet werden und über sein Widerspruchsrecht („opt-out") aufgeklärt werden. Macht der Betroffene von seinem Widerspruchsrecht Gebrauch, ist die Erstellung eines solchen Nutzungsprofils unzulässig.

Bei der Erstellung des Profils dürfen alle Nutzungsdaten (nicht aber die Bestandsdaten) verwendet werden. Die Möglichkeit der Profilerstellung ist aber insoweit eingeschränkt, als diese nur zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Telemediums erfolgen darf. Die Profilerstellung für andere Zwecke ist ohne Zustimmung des Betroffenen ausgeschlossen.

Sobald verhaltensbezogene Daten jedoch personengenau erhoben werden, ist eine explizite und separate Zustimmung erforderlich. Als personenbezogene Verhaltensdaten gelten alle Daten, die Nutzungsdaten mit einer konkreten E-Mail Adresse verknüpfen, z.B. Klickdaten, Conversions oder Aktivitäten auf einer verlinkten Seite.

Wichtig ist ebenfalls die je nach Zustimmung differenzierte

Erhebung und Verarbeitung. Für Betroffene, die nicht zugestimmt haben, dürfen Verhaltensdaten, wie z.B. der letzte Klick, nicht erfasst oder verarbeitet werden.

- Nutzungsprofile dürfen grundsätzlich unabhängig von den o.g. Voraussetzungen erstellt werden, wenn und soweit der Betroffene wirksam (d.h. freiwillig auf Basis einer verständlichen und konkreten Einwilligungserklärung, siehe Frage 10) eingewilligt hat.

- Der Grundsatz der Datensparsamkeit und Datenvermeidung ist zu beachten, d.h., dass nur so viele verhaltensbezogene Daten gesammelt werden sollten, wie unbedingt benötigt werden.

Für „Big Data" bedeutet das Vorgesagte insbesondere, dass die im Pool enthaltenen Daten einzeln daraufhin zu überprüfen sind, welche Art der Daten vorliegt und ob im Einzelfall eine dementsprechende datenschutzrechtliche Rechtfertigung gegeben ist. Pauschal lässt sich das nicht beantworten.

artegic Bird&Bird

09

DARF MAN ALLE FORMEN VON DATENAUSWERTUNGEN DURCHFÜHREN?

Auf „Big Data" finden die allgemeinen Gesetze Anwendung. Daher dürfen ohne eine entsprechende datenschutzrechtliche Rechtfertigung nicht alle Formen von Auswertungen der im Daten-Pool enthaltenen Daten vorgenommen werden. Welche Form der Auswertung erlaubt ist, richtet sich nach der Art der im Daten-Pool befindlichen Daten (vgl. Frage 4). Soweit es sich – wie im Regelfall – (auch) um personenbezogene Daten handelt, bedarf es für die Verarbeitung einer datenschutzrechtlichen Rechtfertigung (vgl. insbesondere Fragen 4, 5). Dabei sollen die nachfolgend aufgeführten Beispiele als Orientierung dienen:

- Werden mit Hilfe von Web-Analyse Tools wie Google Analytics oder Piwik Verhaltensdaten wie Conversion Rate, Anzahl der Besuche auf einer Webseite, Klickrate, Klickreihenfolge, gesuchte Begriffe ausgewertet, ist dies zulässig, wenn der Betroffene zu Beginn des Vorganges, d.h. wenn sich die Webseite öffnet und noch bevor etwaige Daten von ihm gespeichert werden, über die Datenerhebung und –auswertung und das ihm zustehende Widerspruchsrecht zu informieren. Widerspricht der Betroffene der Verwendung seiner Daten bzw. dem Setzen des hierfür erforderlichen Cookies, dürfen seine Daten auch nicht verwendet werden.

Werden jedoch Cookies nur zu dem Zweck gesetzt, um damit das Funktionieren des Webseitenbesuchs zu ermöglichen (z.B. Session-Cookies), muss der Betroffene hierüber nicht informiert werden und hat hier auch kein Widerspruchsrecht.

Grundsätzlich dürfen bei der Webanalyse nur solche Datenauswertungen vorgenommen werden, die der Werbung und Marktforschung sowie der bedarfsgerechten Gestaltung der Webseite dienen.

- Werden auf der eigenen Webseite sog. Social Media Plugins eingebunden (z.B. Facebook „Gefällt mir"-Button), so werden, unabhängig davon, ob der Betroffene diesen Button betätigt oder nicht, an die sozialen Medien Daten übermittelt. Dies gilt auch für Betroffene, die gerade nicht bei der Plattform eingeloggt sind oder solche, die gar nicht bei dem Dienst registriert sind. Die rechtliche Einordnung der Buttons ist höchst umstritten. Da hier jedenfalls die IP-Adresse erhoben und auch gespeichert wird, sodass der Betroffene bei späteren Besuchen wiedererkannt wird sowie die Daten auch an die sozialen Netzwerke weitergegeben werden, ist eine Zustimmung des Betroffenen jedenfalls dann zu empfehlen, wenn man der konservativen Ansicht (und den meisten Datenschutzbehörden, siehe Frage 5) folgt, und die IP-Adresse als personenbezogenes Datum behandelt. Hierzu bietet sich die sog. Zwei-Klick-Lösung an. Mit dem ersten Klick auf die Buttons werden diese zunächst aktiviert. Vorher findet noch keine Datenübertragung statt. In der Aktivierung liegt die Zustimmung des Betroffenen. Mit dem zweiten Klick kann der Betroffene dann die hinter dem Button stehende Funktion nutzen.

- Soweit es für die Inanspruchnahme eines Webangebots erforderlich ist, dass etwa eine Geolokalisierung erfolgt (z.B. bei Diensten die dem Betroffenen ortsgebundene Angebote machen wie. z.B. „Wo ist das nächste Kino") oder der Betroffene wieder erkannt wird, so ist dies im Rahmen derar-

tiger Dienste zulässig, wenn eine Verknüpfung der Daten mit dem Betroffenen zwingend für die Erbringung des Dienstes notwendig ist. Dies ist beispielsweise ausgeschlossen, soweit eine Profilbildung zu Marketingzwecken erfolgen soll. Ob ein zwingendes Erfordernis vorliegt, bemisst sich grundsätzlich nach dem Einzelfall (also nach der Art des Dienstes). Abgesehen von der „Terminal Device Detection" und der „Geolokalisierung", welche im Einzelfall ohne Einwilligung zulässig sein können, sind Dienste wie etwa „Social Activity Detection" oder „Advanced Fingerprinting" die sonstigen Dienste nur mit Einwilligung des Betroffenen möglich. Einer solchen Einwilligung bedarf es insbesondere, wenn Nutzerprofile durch ein drittes Unternehmen erstellt werden.

artegic Bird&Bird

10

WANN BENÖTIGE ICH EIN OPT-IN (EINWILLIGUNG) ZUR DATENSPEICHERUNG UND DATENANALYSE?

WELCHE PUNKTE MUSS DIE EINWILLIGUNG FÜR EIN OPT-IN ZUR VERWERTUNG VON DATEN ENTHALTEN?

Grundsätzlich gilt, dass nicht immer eine Einwilligung des Betroffenen zur Erhebung und weiteren Verwendung von Daten erforderlich ist. Die Erhebung und Verwendung kann auch im Rahmen eines gesetzlichen Erlaubnistatbestandes datenschutzrechtlich zulässig sein (vgl. Frage 4). Entbehrlich ist sie daneben bei rein anonymer Nutzung (siehe Frage 5).

Wenn eine Einwilligung des Betroffenen erforderlich ist, muss diese freiwillig und für den Betroffenen transparent sein und ausdrücklich erteilt werden.

- Die Einwilligung muss freiwillig, also ohne Zwang, erteilt werden. Nicht freiwillig sind Einwilligungen, bei denen der Betroffene keine andere Wahl hat, die keine schweren Nachteile für ihn bedeutet. Freiwilligkeit wird beispielsweise verneint bei Druck des Arbeitgebers auf den Arbeitnehmer sowie bei der Kopplung von Einwilligungen an den Bezug essentieller Waren oder Dienstleistungen (insbesondere Daseinsvorsorge wie etwa Energie, Versorgung, Bankkonto), nicht aber im normalen Geschäftsleben. Nach herrschender und richtiger Ansicht kann ich als normaler Anbieter meine Leistungen von datenschutzrechtlichen Zustimmungen abhängig machen.

- Für eine rechtskonforme Einwilligung muss ein Empfänger explizit der Verarbeitung seiner Daten zustimmen. Eine Einwilligung kann nicht Teil vorformulierter Vertragsbedingungen sein oder aus einem anderen Zusammenhang heraus abgeleitet werden. Soll die Einwilligung zusammen mit einer anderen Erklärung schriftlich erklärt werden, ist sie besonders zu kennzeichnen bzw. hervorzuheben. Die Einwilligung sollte daher am besten immer separat und aktiv erfolgen, d.h. das erforderliche Häkchen (Opt-In) darf nicht schon automatisch gesetzt werden, so dass der Kunde es entfernen müsste.

- Der Kunde muss über den Zweck der Datenverarbeitung aufgeklärt werden, also z.B. Erhebung von Standortdaten oder Auswertung von Click-Verhalten für kundenspezifische Sonderangebote. Werden die Daten für mehrere Zwecke erhoben oder verarbeitet, so sind die verschiedenen Zwecksetzungen zu benennen.

- Im Rahmen der Einwilligung muss der Kunde außerdem über sein Widerrufsrecht informiert werden. Dieses Widerspruchsrecht ist bei Big Data nicht unproblematisch, da ein Widerspruch jederzeit möglich ist und die Daten des Betroffenen dann aus dem Datensatz entfernt werden, oder zumindest separiert werden müssen.

Für einen rechtssicheren Nachweis der Einwilligungen ist nach der deutschen Rechtsprechung im E-Mail-Umfeld nur das sogenannte Double-Opt-In Verfahren geeignet. Es wird argumentiert, dass nur so sichergestellt werden kann, dass auch wirklich derjenige seine Einwilligung abgibt, der über den E-Mail Account verfügt. Durch das Verfahren wird verhindert, dass ein Unbefugter den Empfänger – über ein frei zugängliches Formular – beispielsweise für einen Newsletter einträgt. Jede Einwilligung des Empfängers muss präzise protokolliert werden, damit der Versender jederzeit nach-

weisen kann, dass er eine legitime Einwilligung vorliegen hat. Für eine rechtskonforme Einwilligung per Double-Opt-In müssen im Einzelnen folgende Punkte erfüllt werden:

- Der Empfänger muss nach der Anmeldung eine Bestätigungs-E-Mail geschickt bekommen, in der er über einen Link erneut zur Bestätigung der Einwilligung aufgefordert wird.

- Die Bestätigungsmail darf keine kommerziellen Inhalte enthalten.

- Die Protokollierung muss Art und Umfang der Einwilligung (d.h. die konkrete Datennutzungserklärung, welcher der Empfänger zugestimmt hat) sowie Zeitpunkt der Einwilligung, IP-Adresse und erhobene Daten umfassen.

Für „Big Data" begründet eine Einwilligungserfordernis – neben dem bereits angesprochenen Widerspruchsrisiko – insbesondere die Problematik, dass der Zweck der Datenverarbeitung möglicherweise erst später hinzutritt oder dass für alle im Daten-Pool enthaltenen Daten die Einholung einer Einwilligung aus praktischen Gründen gar nicht mehr möglich ist. Dennoch ist es ratsam, Einwilligungen, soweit möglich, einzuholen.

„Erfolgreiches Marketing ist heute stark datengetrieben. Der Markt verändert sich und Kunden erwarten eine deutlich persönlichere und relevantere Ansprache. Das geht nur mit einer validen und substantiellen Datenbasis. Sie ist notwendige Voraussetzung, um Marketingmaßnahmen digital, reaktionsschnell und zielgerichtet zu steuern und zu optimieren.

Big Data ist jedoch nicht nur das Sammeln und Verstehen von Daten. Die tatsächliche Möglichkeit des Einsatzes dieser Daten für Marketing wird zur wichtigen dritten Säule. Diese Nutzbarmachung bedeutet insbesondere die Planung und Umsetzung von datenschutzrechtlichen Aspekten. Konkret geht es um die rechtssichere Erfassung von Zustimmungen und die datenschutzkonforme Verarbeitung von Daten: Legal Big Data.

Wer die Einholung geeigneter Einwilligungen für personenbezogenes, datengestütztes Marketing verpasst, kann ansonsten den eigenen Datenschatz womöglich später gar nicht heben. Rechtssicherheit im Big Data Kontext wird so zu einem entscheidenden Wettbewerbsfaktor."

STEFAN VON LIEVEN (CEO ARTEGIC AG)
lieven@artegic.de

artegic Bird & Bird

11

WELCHE DATEN AUS EINER VERTRAGSBEZIEHUNG DARF ICH FÜR ANALYSEN ODER DIE KUNDEN-PROFILIERUNG NUTZEN?

Für alle Daten, die im Rahmen einer Vertragsbeziehung erlangt werden, gelten die allgemeinen Grundsätze (vgl. insbesondere die Fragen 3, 4). Allein das Bestehen einer Vertragsbeziehung begründet keine datenschutzrechtliche, urheberrechtliche oder sachenrechtliche Rechtfertigung, siehe auch Frage 19.

artegic Bird & Bird

12

WIE IST MIT AUTOMATISIERTEN ENTSCHEIDUNGEN AUS DER ANALYSE UMZUGEHEN?

Im Umgang mit der automatischen Analyse von Daten gelten für „Big Data" die gleichen Grundsätzen, die auch bei anderen Daten gelten.

Werden Daten automatisch gesammelt und ausgewertet, ohne dass eine individuelle Entscheidung der datenverarbeitenden Stelle über den einzelnen Vorgang nötig ist, so z.B. beim automatischen Abgleich der Daten von Neukunden mit Bestandsdaten, stellt das Gesetz besondere Anforderungen an die Verwendung der Ergebnisse.

Grundsätzlich sieht das Bundesdatenschutzgesetz vor, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht auf die automatisierte Auswertung personenbezogener Daten gestützt werden dürfen. Dieser Grundsatz trägt dem Problem Rechnung, dass die automatisierte Auswertung von Daten auf das Erkennen gewisser Muster angelegt ist, die möglicherweise Spezialitäten des Einzelfalles nicht erkennen können. Dies ist insbesondere bei Scoring-Verfahren der Fall, bei denen aufgrund von mathematisch-statistischen Verfahren die Kreditwürdigkeit einer Person bewertet werden soll.

Ausnahmsweise dürfen automatisierte Entscheidungen jedoch dann herangezogen werden, wenn

- die Entscheidung im Rahmen eines Vertrags- oder anderen Rechtsverhältnisses zu treffen ist und zugunsten des Betroffenen ergeht; oder
- die Wahrung der Interessen des Betroffenen anderweitig gewährleistet ist.

Bedeutsam sind die Ausnahmen insbesondere beim automatisierten Vertragsabschluss im Internet, d.h. wenn einem Angebot des Betroffenen auf Abschluss eines Vertrages stattgegeben wird.

Die Wahrung berechtigter Interessen hat insbesondere dadurch zu erfolgen, dass das Verfahren zur automatisierten Einzelentscheidung einer Vorabkontrolle unterzogen wird, wenn es z.B. darum geht, die Persönlichkeit des Betroffenen zu bewerten.

Das BDSG gewährt dem Betroffenen außerdem einen Auskunftsanspruch hinsichtlich des logischen Aufbaus der automatisierten Datenverarbeitung.

Das TMG enthält darüber hinaus eine Pflicht der datenverarbeitenden Stelle, den Betroffenen darüber zu unterrichten, wenn eine Datenverarbeitung mittels automatisierter Verfahren erfolgt.

artegic Bird&Bird

13

GIBT ES BESTIMMTE REGULIERUNGEN FÜR DEN UMGANG MIT WAHRSCHEINLICHKEITEN FÜR EIN VERHALTEN?

Spielen bei der Verarbeitung von „Big Data" bestimmte Wahrscheinlichkeiten eine Rolle, so gelten hier keine Besonderheiten. Es sind vielmehr die allgemeinen Vorschriften des BDSG zum Umgang mit Wahrscheinlichkeiten zu beachten. Hierbei sind mehrere Szenarien zu unterscheiden.

Erfolgt lediglich eine Analyse von anonymen Daten, z.B. zu dem Zweck, die Besucher auf einer Webseite zu zählen o.ä., sind keine speziellen datenschutzrechtlichen Anforderungen zu beachten.

Werden die personenbezogenen Daten von Betroffenen allerdings derart ausgewertet, dass ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten ermittelt wird (sog. „Scoring"), so stellt das Gesetz folgende Anforderungen an ein solches Verfahren auf:

- die Berechnung muss mittels eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens erfolgen;
- nur Daten, die sich zur Berechnung des Verhaltens überhaupt eignen, dürfen verarbeitet werden; so dürfen Wahrscheinlichkeiten z.B. nicht allein aufgrund der Anschriftendaten ermittelt werden oder die Hautfarbe zugrunde gelegt werden;
- wenn Anschriftendaten verwendet werden, muss der Betroffene vorher über die Verwendung der Daten unterrichtet werden und die Unterrichtung ist zu dokumentieren;
- die Ermittlung der Wahrscheinlichkeiten muss dazu dienen, eine Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses zu treffen.

Hierbei ist zu berücksichtigen, dass die Daten zur Bildung dieses Wahrscheinlichkeitswerts selbst jedoch zunächst rechtmäßig (also mit Einwilligung des Betroffenen, vgl. Frage 4) erhoben und gespeichert werden müssen.

Diese Anforderungen gelten z.B. nicht bei kundenspezifischer Werbung anhand des bisherigen Kaufverhaltens („Behavioural Advertising").

Es besteht auch die Möglichkeit, die Wahrscheinlichkeiten von einem Dritten ermitteln zu lassen, beispielsweise einer Auskunftei (Schufa).

- Werden der Auskunftei eigene Daten übermittelt, ist zu beachten, dass der Kunde der Übermittlung zustimmen muss.

artegic Bird & Bird

14

SPIELT DAS LAND, IN DEM ICH DIE DATEN SPEICHERE BZW. AUSWERTE, EINE ROLLE?

Das Land, in welchem Daten verarbeitet werden, spielt eine Rolle, datenschutzrechtlich, urheberrechtlich und sachenrechtlich.

Sowohl im Datenschutz- als auch im Urheberrecht gilt das Territorialitätsprinzip, d.h. es gilt das Recht des Landes, in dem die relevante Handlung (Speicherung oder andere relevante Nutzung, siehe Frage 3) vorgenommen wird. Dementsprechend ist deutsches Urheberrecht und grundsätzlich auch deutsches Datenschutzrecht (zur Ausnahme zugleich) immer zu beachten, wenn die Daten in Deutschland gespeichert oder genutzt werden.

Daneben gilt deutsches Datenschutzrecht, wenn Daten vom Anbieter in Deutschland gesammelt oder mithilfe von technischen Hilfsmitteln aus Deutschland erhoben werden.

Schließlich gilt deutsches Sachenrecht, wenn Daten aus in Deutschland befindlichen Black Boxen oder anderen im Eigentum des Betroffenen stehenden Trägern bezogen werden.

Eine Ausnahme vom Territorialitätsprinzip gilt im Datenschutzrecht, wenn ein im europäischen Wirtschaftsraum (EWR) ansässiges Unternehmen Daten in einem anderen EWR Staat erhebt, verarbeitet oder nutzt. In diesem Fall gilt (nur datenschutzrechtlich) das Herkunftslandprinzip. Hintergrund ist die aus Sicht der (von den EWR Staaten übernommenen) EU-Datenschutzrichtlinie ausreichende Harmonisierung des Datenschutzrechts in der EU/EWR, die es genügen lässt, wenn sich ein Anbieter an sein lokales Recht hält.

Schließlich gelten für Datenerhebungen und -verarbeitungen außerhalb des EWR verschärfte datenschutzrechtliche Anforderungen, wenn die Daten nicht vom Betroffenen selbst, sondern von Dritten aus dem EWR exportiert werden (z.B. bei der Zusammenführung von EWR Daten in einen US-Datenpool oder bei dem Fernzugriff auf EWR-Datenpools durch Stellen außerhalb des EWR). Der Transfer zu nicht EWR Stellen von in der EWR erhobenen Daten, oder der Zugriff auf diese durch nicht EWR Stellen, darf nur erfolgen, wenn die zusätzliche Anforderungen dafür gemäß der EU-Datenschutzrichtlinie erfüllt sind. Im Bereich von Big Data sind hier namentlich die sogenannten EU Standardvertragsklausel sowie die sogenannten „Safe Harbor"-Regeln relevant. Erstere sind von der EU abgesegnete, vorgefertigte Vertragsklauseln, die zwischen dem in der EWR gelegenen Datenexporteur und dem nicht in der EWR gelegenen Datenimporteur abgeschlossen werden und in denen sich der Importeur im Prinzip zur Einhaltung europäischer Datenschutzstandards bezüglich der exportierten Daten verpflichtet, inklusive – als Vertrag zugunsten Dritter – des Rechts der Betroffenen, bei Verstößen selbst gegen den Importeur vorzugehen. Letztere ist eine Selbstverpflichtung, die – auf Basis einer bilateralen Vereinbarung zwischen USA und der EU und der Aufsicht durch die US Federal Trade Commission – es (nur) US-amerikanischen Unternehmen (mit Ausnahme einiger Branchen wie Telekommunikation und Banken, für die die FTC nicht zuständig ist) ermöglicht, sich den EU-Datenschutzgrundsätzen in Bezug auf aus der EU erhaltene Daten zu unterwerfen.

Zusätzlich ist der Betroffene zu Beginn des Datenverarbeitungsvorgangs darüber zu unterrichten, wenn eine Datenverarbeitung außerhalb des EWR erfolgt.

artegic Bird & Bird

15

KANN EIN KUNDE DER DATENSPEICHERUNG WIDERSPRECHEN?

Ungeachtet dessen, ob eine Datenspeicherung im Rahmen von „Big Data" erfolgt oder nicht, gelten für eine eventuelle Widerspruchsmöglichkeit des Betroffenen die nachfolgenden Regelungen:

- Erfolgt die Datenspeicherung aufgrund einer vom Betroffenen erteilten Einwilligung, muss dieser die Möglichkeit haben, der Speicherung seiner Daten zu widersprechen. Aus der Weigerung, in die Datenspeicherung einzuwilligen, darf dem Kunde auch kein Nachteil erwachsen.

- Handelt es sich um Daten, die zur Durchführung eines Vertragsverhältnisses erforderlich sind (vgl. Frage 11) oder bereits anonymisiert wurden (vgl. Fragen 16, 18), besteht kein Widerspruchsrecht des Betroffenen.

artegic Bird&Bird

16

IST EINE PSEUDONYME/ANONYME VERARBEITUNG VON DATENMENGEN ZU MARKTFORSCHUNGSZWECKEN GESTATTET?

Sowohl anonymisierte als auch pseudonymisierte Daten dürfen jedenfalls unter bestimmten Umständen zu Marktforschungszwecken verwendet werden. Dabei gilt:

- Die Verarbeitung anonymer Daten ist grundsätzlich ohne Einwilligung des Betroffenen möglich (vgl. Fragen 5 und 8).

- Die Verarbeitung pseudonymer Daten ist ebenfalls ohne Zustimmung des Betroffenen möglich, soweit lediglich Nutzungsdaten betroffen sind (d.h. Merkmale zur Identifikation des Betroffenen, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Betroffenen in Anspruch genommenen Telemedien). Der Betroffene ist jedoch über die Datenverarbeitung zu Marktforschungszwecken zu unterrichten und über sein Widerspruchsrecht zu belehren.

Im Rahmen von „Big Data" ist daher gegebenenfalls nach der Art der Daten zu differenzieren.

artegic Bird&Bird

17

MUSS EINER PERSON ERMÖGLICHT WERDEN, DER DATENANALYSE (PROFILIERUNG) SEINER PERSONENBEZOGENEN DATEN ZU WIDERSPRECHEN?

Die Datenanalyse darf grundsätzlich nur mit der Zustimmung des Betroffenen oder aufgrund einer gesetzlichen Erlaubnis erfolgen. Für die Beurteilung der Zulässigkeit eines Widerspruchs ist daher je nach der Rechtsgrundlage für die Datenerhebung und -speicherung zu differenzieren:

- Ist die Datenerhebung und Speicherung nur mit einer Einwilligung des Kunden möglich, können die Daten ohne diese Einwilligung nicht verarbeitet werden.

- War zwar die Erhebung der Daten für die Eingehung oder Durchführung eines Vertrages mit dem Betroffenen erforderlich, wird diese Erlaubnis sich kaum auf die Analyse der Daten erstrecken, da nicht davon ausgegangen werden kann, dass gerade die Datenanalyse auch für die Durchführung des Vertrages erforderlich ist.

- Handelt es sich um pseudonymisierte Daten, ist über den Widerspruch im Rahmen einer Interessenabwägung zu entscheiden. Dabei ist das Interesse des Betroffenen an der Nichterfassung seiner Daten gegen das Interesse des Unternehmens abzuwägen. Hierbei kann z.B. der Zeitpunkt des Widerspruchs eine Rolle spielen oder auch die Art der Datenverwendung durch die datenverarbeitende Stelle. Siehe auch Frage 16.

Der Betroffene ist bei der Erhebung bzw. Speicherung seiner Daten darüber aufzuklären, zu welchem Zweck die Daten erhoben bzw. gespeichert werden. Daher ist als Zweck auch die Verarbeitung der Daten und Erstellung eines Profils zu benennen. Der Betroffene ist ebenfalls darüber aufzuklären, dass er eine einmal erteilte Einwilligung jederzeit widerrufen kann.

artegic Bird&Bird

18

DÜRFEN AUF BASIS PERSONENBEZOGENER DATEN KLASSEN FÜR EINE ZIELGRUPPE BESTIMMT WERDEN (CLUSTERING)?

Beim Clustering wird jeder Betroffene aufgrund seines Verhaltens einer bestimmten Gruppe von Betroffenen zugeteilt. Rechtlich stellt dieser Vorgang ein Verändern von Daten dar, da durch die Zuordnung zu einer Nutzergruppe der Informationsgehalt der Daten inhaltlich umgestaltet wird.

Die Anforderungen, die das Bundesdatenschutzgesetz an das Verändern von Daten stellt, stimmen mit denen überein, die für das Verarbeiten von Daten gelten. D.h., dass jedenfalls eine datenschutzrechtliche Rechtfertigung, entweder in Form einer Einwilligung des Betroffenen oder eines gesetzlichen Erlaubnistatbestandes vorliegen muss.

Auch wenn eine datenschutzrechtliche Rechtfertigung für das Clustering vorliegt, ist hiervon nicht notwendigerweise auch die Nutzung der so gewonnenen Daten für die Kundenprofilierung oder für Direktmarketing erfasst. Hierfür ist eine eigene datenschutzrechtliche Rechtfertigung erforderlich (vgl. auch Checkliste zu E-Mail Marketing).

artegic Bird&Bird

19

KANN ICH DIE DATENERHEBUNG UND AUSWERTUNG IN EINER BLACKBOX OHNE ZUSTIMMUNG DURCHFÜHREN?

Auch für die Auswertung von Daten in einer Blackbox gelten die allgemeinen Bestimmungen: sie bedarf einer datenschutzrechtlichen Rechtfertigung, entweder in Form eines gesetzlichen Erlaubnistatbestandes oder der Einwilligung des Betroffenen. Dies gilt nur dann nicht, wenn die Daten vollständig anonymisiert sind.

Soll allerdings die Auswertung z.B. eines Unfalldatenschreibers aus dem Pkw erfolgen, ist eine datenschutzrechtliche Rechtfertigung erforderlich.

Zusätzlich stellt sich hier das Problem der eigentumsrechtlichen Zuordnung dieser Daten, die z.B. bei privaten Automobilien naheliegend der Berechtigung als Führer, Halter oder Eigentümer des Pkw folgen wird. Auch daraus ergibt sich ein Einwilligungserfordernis hinsichtlich der Datenverarbeitung.

artegic Bird&Bird

20

MUSS ICH EINER PERSON EINSICHT IN DIE VON IHR GESPEICHERTEN DATEN GEBEN?

Hinsichtlich der Auskunftsrechte des Betroffenen ergibt sich auch in Bezug auf „Big Data" nichts anderes als bei anderen Datenerhebungen und -verarbeitungen.

Der Betroffene hat grundsätzlich ein Auskunftsrecht gegen jeden, der seine Daten erhebt, speichert, verarbeitet und an Dritte übermittelt. Auf Verlangen des Betroffenen sind Auskünfte darüber zu erteilen:

- welche Daten zu seiner Person gespeichert sind;
- wo diese Daten erhoben wurden;
- an wen diese Daten weitergegeben werden;
- zu welchem Zweck sie gespeichert wurden.

Die Auskunft über die Herkunft der Daten darf verweigert werden, wenn ansonsten ein Geschäftsgeheimnis preisgegeben werden müsste, dessen Schutz die Interessen des Betroffenen an der Preisgabe überwiegt.

Die Auskunft ist auf Anfrage des Betroffenen einmal jährlich unentgeltlich zu erteilen. Für weitere Auskünfte kann dem Kunden ein Entgelt berechnet werden. Er ist darüber zu informieren.

Die Einräumung dieser umfassenden Auskunftsrechte und die damit einhergehenden praktischen und organisatorischen Hürden können dadurch vermieden werden, dass nur anonymisierte Daten gespeichert und verarbeitet werden.

artegic Bird&Bird

21

WIE SCHNELL UND UMFANGREICH MUSS ICH DAS LÖSCHEN VON DATEN (PERSONENBEZOGENEN DATEN) ERMÖGLICHEN?

BZW. WIE LANGE DÜRFEN DIESE DATEN AUFGEHOBEN WERDEN?

Die Anforderungen, die das BDSG an die Löschung von Daten stellt, richten sich nach dem Einzelfall. Grundsätzlich dürfen die Daten jedoch so lange aufbewahrt werden, wie eine datenschutzrechtliche Rechtfertigung besteht. Der Zeitpunkt der Löschung ist an den Grundsatz der Zweckbindung gekoppelt: sobald der Zweck, für den die Daten erhoben wurden, erfüllt oder weggefallen ist, sind die Daten zu löschen. Der Zweck ergibt sich dabei zumeist aus den vertraglichen Beziehungen. Danach sind die Daten vollständig zu löschen.

Für „Big Data" bedeutet dies, dass theoretisch für alle Daten im Zweifel separat festgelegt werden muss, ob und wie lange eine datenschutzrechtliche Rechtfertigung für deren Aufbewahrung besteht. In der Praxis wird man aber Gruppierungen vornehmen müssen, da es anders nicht machbar ist.

Allerdings dürfen solche Daten, die zu Sicherungszwecken gespeichert wurden, noch für einen angemessenen, meist technisch bedingten Zeitraum gespeichert bleiben. In diesem Fall muss sichergestellt werden, dass diese Daten nur im Sicherungsfall wieder rekonstruiert werden.

Jedenfalls darf keine unbefristete Speicherung personenbezogener Daten erfolgen; auch nicht mit Einwilligung des Betroffenen.

artegic Bird&Bird

22

WELCHE TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN MUSS ICH TREFFEN, UM DIE DATEN ZU SCHÜTZEN?

INSBESONDERE AUCH VOR Z.B. INTERNEN STELLEN?

Für „Big Data" gelten auch hinsichtlich der technischen und organisatorischen Maßnahmen die allgemeinen Regelungen des BDSG. Zum Schutz von Daten schreibt das BDSG in § 9 vor, dass beim Umgang mit Daten alle erforderlichen Maßnahmen zu treffen sind, um die Anforderungen des BDSG zu erfüllen. Im Einzelnen ist sicherzustellen, dass

- Unbefugte (räumlich) keinen Zutritt zu Datenverarbeitungsanlagen erhalten;
- Unbefugte keinen Zugriff auf die Verarbeitung der Daten haben, d.h. nicht auf den Vorgang der Datenverarbeitung einwirken können (dies kann insbesondere durch Verschlüsselung gewährleistet werden) - im Bereich „Big Data" ist die Zugriffskontrolle von besonderer Bedeutung. Die einzelnen Daten des Daten-Pools sind dergestalt aufzubewahren oder der Zugriff zu beschränken, dass jede für den Datenpool freigeschaltete Person auch tatsächlich nur die Daten einsehen und bearbeiten können, für die eine Berechtigung besteht;
- die für die Datenverarbeitung berechtigten Personen nur Zugang zu Daten haben, die von ihrer Berechtigung umfasst sind (dies kann insbesondere durch Verschlüsselung gewährleistet werden);
- die Daten auch im Falle ihrer Weitergabe vor dem Zugriff Unbefugter geschützt sind (dies kann insbesondere durch Verschlüsselung gewährleistet werden);
- die Eingabe und Verarbeitung von Daten dahingehend überprüft werden kann, ob und durch wen diese Tätigkeiten erfolgt sind;
- im Falle der Auftragsdatenverarbeitung eine ordnungsgemäße Auswahl und Überwachung des Auftragsnehmers und dessen Tätigkeiten stattfindet;
- die Daten vor zufälliger Zerstörung (z.B. durch Blitzeinschlag, Stromausfall, Wassereinbruch o.ä.) geschützt werden;
- gewährleistet ist, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt werden verarbeitet werden;
- Mitarbeiter, die mit Daten anderer in Berührung kommen, auf das Datengeheimnis verpflichtet werden.

artegic Bird & Bird

23

WELCHE ANFORDERUNGEN AN BIG DATA ERGEBEN SICH AUS DEM AKTUELLEN STAND DER EUROPÄISCHEN DATENSCHUTZVERORDNUNG?

Derzeit ist noch nicht endgültig sicher, ob es die geplante Europäische Datenschutzgrundverordnung geben wird. Wird allerdings die (im Entstehen befindliche) europäische Datenschutz-Grundverordnung in ihrer jetzigen Form (durch das Europäische Parlament am 12.03.2014 vorgeschlagene modifizierte Fassung des Vorschlags der Europäischen Kommission vom 25.01.2012) in Kraft treten, ergeben sich hinsichtlich „Big Data" wichtige Änderungen, insbesondere:

- Die Datenschutz-Grundverordnung bestimmt klarer, als das derzeitige deutsche Recht, wann personenbezogene Daten vorliegen (vgl. Fragen 4 und 5). Insbesondere bei Kennnummern, Standortdaten oder Online-Kennungen soll es sich nur dann um personenbezogene Daten handeln, wenn die datenverarbeitende Stelle nicht nachweisen kann, dass kein Personenbezug vorliegt. Hinsichtlich der IP-Adresse folgt die Regelung, dass diese immer dann ein personenbezogenes Datum darstellt, wenn sie nicht für ein Unternehmen erteilt wurde.

- Bei Fragen der Verarbeitung von Daten zu eigenen Geschäftszwecken wird der derzeitige Vorschlag dahingehend interpretiert, dass die Möglichkeit der nachträglichen Zweckänderung der Datenerhebung (vgl. Frage 6) durch die Verordnung eingeschränkt wird. Der aktuelle Entwurf der europäischen Datenschutz-Grundverordnung sieht vor, dass Daten nur dann zu einem anderen Zweck verarbeitet werden dürfen als der zu dem sie erhoben wurden, wenn die Einwilligung des Betroffenen vorliegt oder eine vertragliche Grundlage besteht.

- Werden Daten nicht selbst verarbeitet, sondern an Dritte zur Verarbeitung weitergegeben (sog. „Auftragsdatenverarbeitung"), sind nach der europäischen Datenschutz-Grundverordnung Auftraggeber und Auftragnehmer gemeinsam für die Einhaltung datenschutzrechtlicher Anforderungen verantwortlich. Nach bisherigem deutschen Recht haftet der Auftraggeber gegenüber dem Betroffenen allein und hat die Einhaltung des Datenschutzrechts durch den Auftragnehmer zu überwachen. Die stärkere (Mit)haftung des Auftraggebers ist auch im Rahmen von „Big Data", jedoch insgesamt für die Nutzung von Daten zu Werbezwecken ein Problem.

KONTAKT

artegic unterstützt Sie im erfolgreichen
Dialogmarketing mit E-Mail, RSS, Mobile und Social Media.
Nehmen Sie unverbindlich Kontakt auf unter
www.artegic.de, Telefon +49(0)228 22 77 97 0
oder per **E-Mail info@artegic.de**

Kennen Sie schon unseren Praxisnewsletter mit vielen
nützlichen Tipps im Online Dialogmarketing?
Den monatlichen Newsletter können Sie hier
kostenlos abonnieren:
www.artegic.de/newsletter

artegic AG
Zanderstraße 7
53177 Bonn
www.artegic.de

Tel: +49(0)228 22 77 97 0
Fax: +49(0)228 22 77 97-900

In Zusammenarbeit mit Bird&Bird:

Bird & Bird LLP
Carl-Theodor-Straße 6
40213 Düsseldorf
Tel: +49 (0)211 2005 6000
Fax: +49 (0)211 2005 6011

artegic