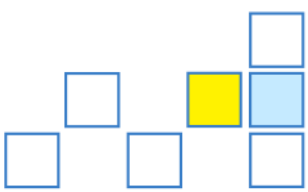
www.datenschutzzentrum.de

Datenschutz im Bereich Social Customer Relationship Management



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln
des Bundesministerium für Bildung und Forschung unter
dem Förderkennzeichen 01IS12039B gefördert.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Version 1.0

Verfasser:

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98
24103 Kiel

Tel: 0431 988 1200

E-Mail: mail@datenschutzzentrum.de
www.datenschutzzentrum.de

Inhaltsverzeichnis

1. Einführung

1.1 Abstract

Die vorliegende Studie zielt darauf ab, die rechtlichen Rahmenbedingungen festzustellen, unter denen Betreiber von Systemen für Kundenbeziehungsmanagement (Customer Relationship Management, im Weiteren CRM) Daten aus sozialen Netzwerken erheben, verarbeiten und nutzen dürfen (Social CRM). Sie entstand im Rahmen eines Projekts zur Erstellung einer Softwarekomponente für Social CRM-Systeme, die es ermöglichen soll, Entscheidungsträger bei Betreibern solcher Systeme zu warnen, bevor potentiell rechtswidrige Datenverarbeitungsvorgänge in Bezug auf Daten aus sozialen Netzwerken ausgelöst werden. Federführend bei dem Projekt war die bowi GmbH, Landau. Außerdem beteiligt war das Institut für Wirtschaftsinformatik (IWI) der Universität Leipzig (Lehrstuhl Prof. Dr. Rainer Alt). Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) begleitete das Projekt juristisch.

Soziale Medien haben in den vergangenen Jahren die Informationsgesellschaft vollständig verändert. Die plötzliche Verfügbarkeit von mehreren Milliarden neuen Datensätzen täglich hat sowohl das Interesse der Wirtschaft an deren Erhebung und Nutzung geweckt, als auch die Befürchtungen von Datenschützern, dass mithilfe dieser scheinbar freiwillig preisgegebenen Daten, Interessen und Meinungen und ihrer Verknüpfung eine Durchdringung des Privatlebens von Millionen Menschen möglich wird, wie sie in Rechtsstaaten bisher beispiellos ist.

Ein Problem in diesem Zusammenhang ist die Unsicherheit über die rechtlichen Voraussetzungen, unter denen eine Erhebung von Daten aus sozialen Medien möglich ist. Weder der europäische, noch der deutsche Gesetzgeber konnten bei ihren jeweils letzten Novellierungen datenschutzrechtlicher Vorschriften auch nur im Ansatz voraussehen, welchen Umfang die jederzeitige tatsächliche Verfügbarkeit von persönlichen Daten annehmen würde. Hinzu kommt, dass mehr und mehr Kundendaten in die Cloud ausgelagert werden, woraus ein Kontrollverlust entsteht, da Unternehmen oft nicht einmal wissen, in welchem Land der Server steht, auf dem die Daten ihrer Kunden gespeichert sind, geschweige denn, welche Personen im Einzelnen auf die Daten Zugriff haben. Die Regelungen des Bundesdatenschutzgesetzes bilden die Problemfelder des Internetzeitalters wie etwa User-Generated Content, Big Data und Cloud Computing nur bedingt ab.[1]Eine europäische Regelung, welche den neuen Gegebenheiten gerecht werden soll, steht zwar in Aussicht,[2] wird aber frühestens im Jahr 2018 in Kraft treten[3] Es ist daher notwendig, Wege zu finden, auch in dem vorhandenen europäischen und bundesrechtlichen Rahmen den Einzelnen vor Verletzungen seines Grundrechts auf informationelle Selbstbestimmung durch Social CRM zu schützen, ohne die berechtigten Interessen der Betreiber solcher Systeme zu missachten. Im rechtswissenschaftlichen Schrifttum finden sich bisher nur Klärungsversuche zu Einzelfragen im Gesamtkomplex. Von Schrifttum

[1] Vgl. Bull, NVwZ 2011, S. 257.

[2] Datenschutz-Grundverordnung, EU-Dok. 2012/0011 (COD), aktuelle Entwurfsfassung 9565/15 v. 11.06.2015, abrufbar unter http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf.

[3] EU-Minister einigen sich auf Datenschutzreform, Die Zeit v. 15.06.2015, abrufbar unter http://www.zeit.de/digital/datenschutz/2015-06/datenschutz-eu-reform-justizminister-luxemburg.

und Rechtsprechung breit durchdrungen sind etwa Anforderungen an datenschutz- und telemedienrechtliche Einwilligungserklärungen insbesondere im Zusammenhang mit der unmittelbaren Zusendung von Werbung. Diese Gegenstände werden daher zwar besprochen, verstehen sich aber nicht als Hauptteil der Studie. Kaum Beiträge finden sich dagegen bisher zu Fragen der Erhebung von Daten aus sozialen Netzen, zur Anreicherung von Kundendaten und zur Ansprache von Betroffenen (sei es zu Image- oder Servicezwecken) auf sozialen Netzen. Ebenfalls unterrepräsentiert sind bisher Fragen nach der dogmatischen Einordnung des nicht-kreditbezogenen Scorings und der Durchführung von statistischen Analysen durch Unternehmen aus eigenen Datensätzen. In diesen Fragen eine stimmige, alle rechtlichen Ebenen einbeziehende Linie zu entwickeln, ist Ziel und Schwerpunkt der vorliegenden Ausarbeitung.

In der betriebswirtschaftlichen Literatur wird Social CRM bisher fast ausschließlich unter dem Gesichtspunkt seiner Chancen zur Steigerung des Return-on-Investment behandelt, so dass der vorliegende Versuch einer umfassenderen rechtlichen Darstellung für die Praxis der Datenverarbeitung wie für die gesellschaftliche Diskussion von Interesse sein dürfte.

Indes sind die Anwendungsfälle von Social CRM so vielfältig und die Produkte und Methoden so flüchtig geworden, dass es nicht Ziel dieser Studie sein kann, sämtliche Hilfsmittel zur Datenerhebung auf sozialen Medien durch Unternehmen abzudecken. Die Studie wird sich daher, produktneutral, weitgehend auf diejenigen CRM-Funktionen konzentrieren, die erstens weit verbreitet und zweitens, wegen des steten und schnellen technischen Wandels, verallgemeinerbar sind. Ein besonderes Augenmerk gilt den Funktionen von gängiger, spezifischer CRM-Software. Es wird davon ausgegangen, dass diese Produkte sich in kurzer Zeit derart verändern werden, dass die juristische Analyse zeitnah gegenstandslos werden wird, aber die Betrachtung der zugrundeliegenden Mechanismen der Datengewinnung und -nutzung eine Begutachtung auch im Hinblick auf künftige Dienste und Technologien relevant bleiben werden. Letztere wird daher, soweit marktrelevant, in verallgemeinerter Form jeweils versucht werden.

Die Studie wird zunächst einen Abriss des Projekts geben. Sodann werden wichtige Zwecke von CRM und Typen sozialer Medien vorgestellt. Im Rahmen des Überblicks über soziale Medien wird diskutiert, wie auf den jeweiligen Plattformen Privatsphäre-Einstellungen gehandhabt werden. Danach wird die Studie im Einzelnen auf Funktionen von Social CRM und in diesem Zusammenhang eingesetzte Software (Tools) eingehen. Ein Abschnitt wird sich mit Mitteln der Informationsgewinnung durch von sozialen (Dritt-)Plattformen selbst zur Verfügung gestellte Software beschäftigen.

Kurz wird der bundes- und europarechtliche Rahmen skizziert, nach dem Datenverarbeitungsvorgänge zu beurteilen sind. Es folgt der Hauptteil der Studie, in dem nach der Abklärung der unabdingbaren Rahmenbedingungen eines rechtskonformen Social-CRM-Betriebs einzelne typische Funktionen im Social CRM auf ihre Vereinbarkeit mit geltendem Datenschutzrecht überprüft werden. Hierfür werden Stand der Literatur und Rechtsprechung zu einschlägigen Datenschutzfragen ausgewertet und geprüft, inwieweit er auf die Problematiken von Social CRM anwendbar ist und inwieweit er der Anpassung auf spezifische CRM-Probleme bedarf. Die Reihenfolge der besprochenen Probleme orientiert sich an der Systematik der gängigen Social-CRM-Komponenten. In diesem Rahmen werden einzelne Anwendungsszenarien vorgestellt, für die allgemeine rechtliche Aussagen getroffen werden können.

Der folgende Abschnitt geht auf die Anforderungen in Bezug auf Datenschutzmanagement und Datensicherheit ein. Es folgt ein Überblick über die Rechte des von einer Datenerhebung im SCRM Betroffenen und die Sanktionen, welche das Datenschutzrecht an eine unbefugte Datenverarbeitung knüpft.

Sodann wird die rechtliche Zulässigkeit der Datenschutzkomponente geprüft, die Gegenstand des Projekts war, wobei Aspekte der Rechtsberatung und der Vereinbarkeit von künstlicher Intelligenz und der juristischen Methode diskutiert werden.

1.2 Projekt SPHERE

Ausgangspunkt des Projekts SPHERE war der Wunsch einiger deutscher Unternehmen, an den neuen Möglichkeiten des partizipatorischen Web teilzuhaben, insbesondere von Usern verfasste Beiträge zum eigenen Unternehmen und Produkten zu sammeln und den vorhandenen Datenbestand im CRM mit ihnen anzureichern.

Diese Praxis entstand in den Vereinigten Staaten, wo im privaten Bereich keine mit dem europäischen Datenschutzniveau vergleichbare Gesetzgebung existiert. Hier werden Daten aus sozialen Netzwerken bald nach ihrer erstmaligen Verfügbarkeit unter Verwendung von Data-Warehouses im großen Umfang gesammelt und in unterschiedlicher Weise für die Geschäftszwecke der Erhebenden nutzbar gemacht. Dabei werden zu einer unüberschaubaren Vielzahl von Nutzern, die von der Datenerhebung ganz überwiegend keine Kenntnis haben, regelmäßig Profile mit Namen, demographischen Daten, Interessen und Einstellungen erstellt, was nach der Analyse mit Big Data-Algorithmen die Zusendung von individualisierter Werbung möglich macht.

Diese Vorgänge sind in Deutschland in verschiedener Hinsicht rechtswidrig, so dass eine direkte Übertragung durch CRM-Anbieter rechtlich nicht möglich ist. Gleichzeitig herrscht im deutschen und europäischen Datenschutzrecht eine Gesetzeslage, die nicht auf die vorgenannten Möglichkeiten zur massenhaften Datenverarbeitung ausgerichtet ist. Hieraus resultiert eine Unsicherheit darüber, welche Formen des Social CRM in Deutschland zulässig sind, und welche nicht.

Der CRM-Hersteller bowi GmbH plante daraufhin im Verbund mit dem Lehrstuhl von Prof. Dr. Rainer Alt, Universität Leipzig, die Entwicklung einer Software, welche die Datenbestände des Social Web für die Betreiber von CRMs fruchtbar machen sollte, ohne gegen deutsches und europäisches Datenschutzrecht zu verstoßen. Hierzu war im Vorlauf bereits ein CRM mit Elementen von „privacy by design“ konzipiert worden. Im vorliegenden Projekt wurde eine CRM-Komponente entwickelt, welche durch Analyse der Parameter eines Verarbeitungsvorgangs und mit Hilfe eines wissensbasierten Systems den Anwender warnen soll, falls die Gefahr besteht, dass ein geplanter Datenverarbeitungsvorgang datenschutzrechtlich unzulässig ist. Das ULD hatte als dritter Projektpartner eine datenschutzrechtliche Beratungsfunktion, in deren Rahmen die vorliegende Studie entstand. Das Bundesministerium für Bildung und Forschung förderte das Projekt, welches die Jahre 2013 und 2014 überspannte, im Rahmen des Förderprogramms „KMU-innovativ: Informations- und Kommunikationstechnologie (IKT)“.

1.3 Was ist CRM?

CRM (Customer Relationship Management) ist die betriebswirtschaftliche Querschnittsaufgabe, die Beziehung eines Unternehmens zu seinen Kunden zu regeln.[4] Dabei bezieht CRM eine ganzheitliche Perspektive und ist bemüht, sämtliche Phasen einer Kundenbeziehung von der Kundengewinnung über die Beziehung zu Bestandskunden bis hin zur Rückgewinnung abzudecken.[5] Die drei Hauptbereiche, in denen CRM-Technik zur Anwendung kommt, sind daher

- Marketing,
- Vertrieb (Sales),
- Kundenservice.

Überschneidungen ergeben sich im Bereich Marketing mit der allgemeinen Marktforschung, im Bereich Vertrieb mit der Ressourcenplanung (ERP), die jeweils keine CRM-Aufgaben im engeren Sinne darstellen. Marktführer bei CRM-Systemen ist derzeit das kalifornische Unternehmen Salesforce mit einem Gesamtumsatz im Jahr 2013 von ca. 3 Milliarden US-Dollar.[6]

1.3.1 Marketing

Eine praktisch bedeutsame Form von Marketing auf sozialen Medien ist das Dialogmarketing. Dabei versuchen Unternehmen, Verkaufsmöglichkeiten gegenüber Neu- und Bestandskunden durch Analyse der bei ihnen vorhandenen Datensätze unter Einbeziehung von Daten aus sozialen Medien auszuloten und den Betroffenen personalisierte Werbeansprachen zu unterbreiten. Bei Neukunden liegt das Hauptinteresse in der zielgenauen Generierung zukünftiger Käufer eines Produkts (Leads), bei Bestandskunden auf dem Verkauf weiterer Produkte des Unternehmens (Cross-Selling bzw. Up-Selling), bzw. der Rückgewinnung. Darüber hinaus werden Erkenntnisse aus sozialen Medien auch zum Management von nicht individualisierten (wohl aber auf Marktsegmente zugeschnittenen) Werbekampagnen benutzt. Eine weitere Funktion des Marketings im Rahmen des CRM ist das allgemeine Reputationsmanagement, insbesondere der Umgang mit Kritikern und die Gewinnung und Nutzbarmachung von einflussreichen Befürwortern der Marke (brand advocates).

1.3.2 Vertrieb

Die klassische Vertriebsaufgabe, die mit CRM gelöst wird, ist die der Vorbereitung von Geschäftsabschlüssen. Auch hier sollen gezielt geeignete Vertragspartner ermittelt werden. Im Gegensatz zum Marketing ist hier eine Nachfrage bereits vorhanden, so dass Zweck der Vertriebskomponente von CRM die Suche nach geeigneten Vertragspartnern zur Gewinnung von konkreten Aufträgen ist. Insofern handelt es sich bei den sozialen Medien, die zu diesem Zweck durchsucht werden, eher um professionelle Plattformen als

---

[4] Grützner/Jakob, in: Grützner/Jakob, Customer Relationship Management (CRM), in: ders., Compliance von A-Z.

[5] Bruhn, Kundenorientierung, Kap. 1, Abb. 1-3.

[6] Salesforce.com, Jahresbericht für die Investoren, S. 2, abrufbar unter http://www2.sfdcstatic.com/assets/pdf/investors/AnnualReport.pdf.

um jene Plattformen, welche dem Freizeitbereich zuzuordnen sind. Bei dieser Art von Verkaufsanbahnung ist es auch wahrscheinlicher als beim Dialogmarketing, dass der Betroffene entweder als Vertreter eines Gewerbebetriebs angesprochen wird, oder als natürliche Person (etwa als Freiberufler) an der Ansprache und dem Abschluss des Geschäfts bereits ein Interesse hat.

1.3.3 Kundenservice

Social Media bietet für Unternehmen als Plattform für den Kundenservice Vorteile.[7] Einerseits weil dem Kunden auf dieser Weise oft eine zügigere Lösung als auf traditionellen Wegen angeboten werden kann, andererseits, weil von der Öffentlichkeitswirkung des Supports auch ein Werbeeffekt ausgehen kann. Die Datenbankkomponente des CRM erlaubt durch Aufbereitung der Supportbeziehung und Schaffung von detaillierten Datensätzen zu jedem Servicefall (sog. Tickets) eine bedarfsgerechte Bearbeitung. Diese Daten können Servicemitarbeiter nutzen, um Beschwerden über Fehlfunktionen eines Produkts auf sozialen Medien nachzugehen.

1.4 Soziale Medien

Internetinhalte werden nicht nur von professionellen Autoren veröffentlicht, sondern zunehmend auch als „User Generated Content" von einfachen Nutzern.[8] Schließlich erweiterten Plattformen wie Facebook (und in Deutschland zunächst StudiVZ) die Funktionen einer Blog-Community, indem dem User erlaubt wurde, freiwillig ein umfassendes Bild von sich selbst der Außenwelt zu präsentieren und die eigenen Beiträge zur Beurteilung durch Dritte freizugeben. Auf dieser Basis entstand Facebooks Geschäftsmodell, durch Auswertung der Aktivitäten und Interessen der einzelnen Nutzer der Werbewirtschaft detaillierte Profile zur Verfügung zu stellen. Im Gegenzug werden vom Nutzer keine Gebühren erhoben. Mit diesem Geschäftsmodell erzielte Facebook 2013 einen Umsatz von nahezu acht Milliarden US-Dollar weltweit.[9]

Die zwischen einzelnen sozialen Netzwerken unterschiedlich stark ausgeprägte Möglichkeit der Profilbildung rief zumindest in der Europäischen Union bald rechtliche Bedenken hervor. Diesen suchten die sozialen Netzwerke zumeist dadurch aus dem Weg zu gehen, dass sie eine Niederlassung in einem Mitgliedstaat einrichteten, dessen Umsetzung der europäischen datenschutzrechtlichen Vorgaben und Aufsichtspraxis möglichst verarbeitungsfreundlich ausgestaltet war. Diese Praxis wurde erst 2014 durch das Urteil des Europäischen Gerichtshofs in Sachen Costeja Gonzalez ./. Google[10] (in diesem Gutachten als Google-Entscheidung bezeichnet) unterbunden, nach der es für die Anwendbarkeit nationalen Rechts eines Mitgliedsstaats ausreicht, wenn etwa durch nationale Niederlassungen Anzeigen in dem Mitgliedsstaat akquiriert werden. Dies ist für die großen sozialen Netzwerke in Deutschland der Fall.

---

[7] Kreutzer/Hinz, Working Papers of the Institute of Management Berlin at the Berlin School of Economics and Law (HWR Berlin), No. 58, S. 11.

[8] Reinemann/Remmertz, ZUM 2012, S. 216.

[9] Facebook meldet hohen Umsatz und Gewinn, PC Welt v. 30.01.2014, abrufbar unter http://www.pcwelt.de/news/Facebook_meldet_hohen_Umsatz_und_Gewinn-Quartalszahlen-8437407.html.

[10] EuGH, Urt. v. 13.05.2013, C 131/12 —Google Spain SL, Google Inc ./ AEPD v. Gonzales, Rn. 34.

1.4.1 Typen und Zwecke

Das erste „soziale Netzwerk" im heutigen Sinne, das Usenet, kann dem Typus des Forums zugerechnet werden. Dieser Typus existiert bis heute, wobei die meisten Foren sich einem speziellen Feld der Diskussion (z.B. Telekommunikation, Computerspiele) verschrieben haben. Auf Foren können Benutzer Beiträge zu einem bestimmten, üblicherweise durch eine Überschrift kenntlichen, Thema einstellen. Die Strukturierung erfolgt dabei in sogenannten Threads („Fäden"), d.h. Listen der Postings in der Sortierung einer Baumstruktur, wobei idealerweise immer kenntlich ist, auf welchen Beitrag ein bestimmtes Posting antwortet. Foren werden allerdings in zunehmendem Maße auch von Unternehmen insbesondere zur Erbringung von Kundenservice eingerichtet. Kunden werden eingeladen, Fragen und Probleme zu posten, die dann durch andere Forumsteilnehmer, sonst durch Sachbearbeiter des Unternehmens in Zusammenarbeit mit Support oder Vertrieb beantwortet werden können. Aus dieser Praxis ergibt sich ein beträchtlicher Publizitätseffekt der Supportleistung, die sie gelegentlich in die Nähe von Werbung rückt. Beiträge zu Foren erfolgen typischerweise unter einem vom Benutzer selbstgewählten Pseudonym, was der Rechtslage in Deutschland entgegenkommt (§ 13 Abs. 6 Satz 1 TMG). Zu den Foren im weiteren Sinne müssen auch Bewertungsseiten im Internet gezählt werden. Hierbei handelt es sich um Webseiten, auf denen über einzelne private Unternehmungen (etwa Hotels, Restaurants u.ä.), aber auch über natürliche Personen (Ärzte, Lehrer) grundsätzlich ohne deren Zutun eine Profilseite erstellt wird. Nutzern wird die Gelegenheit gegeben, diese sowohl in Form einer Art Punktzahl als auch durch schriftliche Kommentare zu bewerten. Die Bewertungen dienen anderen Nutzern als Entscheidungshilfe für die Wahl eines Dienstleisters oder eines Unternehmens. Der Einfluss dieser Internet-Bewertungen auf Konsumentscheidungen ist mittlerweile immens, die Abhängigkeit von diesen Kommentaren unbestimmter Herkunft ausgesprochen riskant, so dass ein großes Interesse der Unternehmen besteht, ihre Bewertungen auf diesen Plattformen so weit wie möglich zu verfolgen und zu beeinflussen. Hier stellt sich demnach besonders drastisch die Frage nach dem Recht der Unternehmen auf Intervention z.B. in Form der Namhaftmachung der Verfasser einzelner Kommentare und der Geltendmachung von Unterlassungsansprüchen gegen die Plattformbetreiber. Diese Maßnahmen sind in der Zwischenzeit schon mehrfach Gegenstand der Rechtsprechung gewesen.

Weblogs (Blogs) sind elektronische Listen von datierten Einträgen eines einzelnen oder eines Kollektivs von Verfassern, die oft mit Tagebüchern verglichen werden. Die Notwendigkeit, für Blogs eine eigene Webseite designen zu müssen, beschränkte das Blogging zunächst auf Spezialistenkreise. Interessierten Laien wurde das Blogging später mit dem Erscheinen von Anbietern wie WordPress, Squarespace oder Blogger auf dem Markt erleichtert.

Diese boten jedermann eine Umgebung sowie gegebenenfalls Speicherplatz zur Herstellung einfach zu formatierender Blogeinträge mit der Möglichkeit, Kommentare von Dritten zuzulassen und die eigene Sichtbarkeit zu steigern, indem den Einträgen Stichworte zur erleichterten Auffindbarkeit (sog. Tags) angehängt werden. Blogsoftware wurde sowohl für auf privaten Webseiten betriebene Blogs angeboten als auch im Rahmen von Blog-Communities, deren Nutzer untereinander über Postings und Kommentare Meinungen austauschten. Diese Gemeinschaften wiesen bereits Ähnlichkeiten mit Medien wie Facebook auf, die Blogfunktionen noch tiefer mit den Beiträgen „befreundeter" Nutzer integrieren. Die Grundstruktur von Blogs hat sich seit der Einführung der genannten Dienste nicht wesentlich verändert. Eine Unterform von Blogs ist das sogenannte Microblog, bei dem Nachrichten von telegrammartig begrenzter Län-

ge gepostet werden, und damit eine Rezeption durch Dritte nahezu in Echtzeit in Form eines Äußerungsstroms möglich wird. Der wichtigste Microblogging-Service ist der Dienst Twitter, dem neben Facebook in dieser Studie ein Hauptaugenmerk gelten wird, weil seine Funktionalitäten, die in ihrer Flexibilität weit über die Möglichkeiten herkömmlicher Blogs hinausgehen, paradigmatisch auch für andere soziale Dienste geworden sind. Die Angabe des Klarnamens ist dem Benutzer von Bloggingdiensten üblicherweise anheimgestellt, allerdings verlangt Facebook die Nennung des vollen Namens[11] und ist bereits gegen Zuwiderhandlungen durch Sperrung von Benutzerkonten vorgegangen[12].

Chats sind Plattformen, in denen sich Menschen, in größeren „Räumen" oder im Zwiegespräch, über einen kontinuierlich scrollenden Text in Echtzeit austauschen. Einige Chatseiten unterstützen Profile im oben bezeichneten Sinne, andere sind ohne Login und Registrierung nutzbar. Im Rahmen des CRM werden Chats oft zur Kundenberatung, bzw. zum Service eingerichtet. Chatplattformen sind im Vergleich zu umfassenderen sozialen Netzwerken weniger stark verbreitet. Klare Marktführer existieren nicht (mehr), was die Auswertung für Marketingzwecke wenig attraktiv macht. Bei Instant-Messenger-Diensten, d.h. Chatplattformen mit dediziertem Client, steht der Chat von Person zu Person unter Ausschluss der Öffentlichkeit im Vordergrund. Ein Beispiel ist hier die Smartphone-Software Whatsapp. Ein weiteres bedeutendes Mittel der Internetkommunikation, Skype, ist ein Hybrid zwischen einem Videotelefonie-Client und einem Messenger. Grundsätzlich sind Messenger-Accounts nicht öffentlich einsehbar und die Benutzer chatten ausschließlich mit Personen aus einem selbstgewählten Personenkreis. Zur Kontaktaufnahme sind regelmäßig weitere Informationen über den Kommunikationspartner nötig, wie etwa dessen Telefonnummer oder Accountbezeichnung. Die Nutzung dieser Messenger in der B2C-Kommunikation ist daher, außer durch Schalten von mehr oder weniger verhaltensbezogener Werbung, nicht sehr üblich.

Mit der Gründung von Wikipedia im Jahre 2001 wurde die Öffentlichkeit erstmals auf einen schon für einige Zeit existierenden besonderen Typus von kollaborativen sozialen Medien aufmerksam, dessen Idee darin bestand, bisher von einem Betreiber festgelegte Webseiteninhalte durch die Bearbeitung durch eine unbegrenzte interessierte Öffentlichkeit abzulösen. Diese Wikis können, teilweise ohne Anmeldung, grundsätzlich von jedermann bearbeitet werden. Auf diese Weise sollte „Schwarmwissen" genutzt werden und der Gedanke des offenen Wissens unter teilweisem Verzicht auf urheberrechtliche Ansprüche und unter Zuhilfenahme freier Lizenzen (Creative Commons ShareAlike, GNU Free Documentation) gefördert werden. So werden die meisten Wikis auch zur Information der Öffentlichkeit benutzt, etwa als Handbuch. Aber auch gewisse kollaborative Projekte, die sich nicht in der Herstellung des Wiki selbst erschöpfen, etwa in der freien Softwareentwicklung, nutzen Wikis als kostengünstigen Ersatz für proprietäre Prozessmanagementsoftware. Wikis enthalten zu jeder Hauptseite (bei Wikipedia: Artikelseite), auf der der eigentlich zu erstellende Inhalt abgelegt wird, in der Regel noch eine oder mehrere Diskussionsseiten bzw. Archive, in welchen Meinungsaustausch dezidiert öffentlich stattfindet. Wikis sind üblicherweise pseudonym ausgestaltet.

Funktionell können Soziale Netzwerke grob in zwei Kategorien geteilt werden: Die größere ist die Kategorie, die sich auf die Sozialsphäre des Nutzers bezieht. Auf derartigen Plattformen tauschen Menschen

---

[11] Nr. 4.1 der Nutzungsbedingungen von Facebook, abrufbar unter https://de-de.facebook.com/legal/terms.

[12] Etappensieg für Facebook im Streit über Klarnamenzwang, Heise v. 15.02.2013, abrufbar unter http://www.heise.de/newsticker/meldung/Etappensieg-fuer-Facebook-im-Streit-ueber-Klarnamenzwang-1804393.html.

zum Zwecke der Freizeitgestaltung, der Aufrechterhaltung sozialer Kontakte und der Erleichterung des Alltags ihre Interessen und Erkenntnisse aus. Hierunter fallen demnach nicht nur klassische soziale Medien wie Facebook, sondern etwa auch Bewertungsplattformen und Gesundheitsforen. Die kleinere, aber für das CRM ebenfalls bedeutende Kategorie ist diejenige, die beruflichen Beziehungen und Kontakten vorbehalten ist. Marktführer in Deutschland sind in dieser Kategorie XING und LinkedIn, jedoch ist inzwischen auch Twitter ein häufiges Umfeld für die Pflege beruflicher Kontakte. Auf rein professionellen Plattformen zielen Nutzer oft darauf ab, mit beruflichen Angeboten kontaktiert zu werden.

1.4.2 Funktionen

Ein gemeinsames Merkmal der meisten sozialen Medien ist das Vorhandensein zweier Grundbausteine: des Profils und der nutzergenerierten Inhalte.

Die Profilseite ist ein Bereich auf der Website, der vom Nutzer gestaltet werden kann. Es ist dafür eingerichtet, potentiellen Lesern die grundsätzlichen Daten über den Nutzer mitzuteilen. Außerdem kann das Ausfüllen eines Profils dazu dienen, von Dritten leichter gefunden zu werden. Ein ausgefülltes Profil kann enthalten:

- Name,
- Geburtsdatum,
- Wohnort, gegebenenfalls vollständige Adresse, Umzüge, Geburtsort;
- Telefonnummern, Messenger-Kontaktdaten,
- Beruf, Arbeitgeber, gegebenenfalls frühere Arbeitgeber,
- Interessen,
- Profilbild (oft ein Selbstporträt) und weitere Fotos,
- weitere Angaben zur äußeren Erscheinung (z.B. Größe, Gewicht)
- Kontakte im Rahmen des sozialen Netzwerks.

Facebook und ähnliche soziale Netzwerke verwenden für die Aufnahme dieser Daten Formulare, in denen jedes Datum der entsprechenden Kategorie zugeordnet wird, so dass die Daten strukturiert in einem Datenbanksystem abgelegt und jederzeit unproblematisch aufbereitet werden können. Twitter, und mit ihm mehrere neuere soziale Netzwerke, bieten dem Nutzer neben den verpflichtenden Anmeldedaten (z.B. die mit dem Account verknüpfte E-Mail-Adresse) teilweise auch ein Feld an, in dem dieser einen formfreien, selbstverfassten Absatz zu seiner Person einfügen kann. Zu dessen Auswertung ist somit eine semantische Analyse erforderlich.

Soziale Netzwerke wie Facebook erlauben es, einen Freundeskreis einzurichten. Es handelt sich um einen vom Nutzer selbst gewählten Kreis von Personen. Durch gegenseitige Vereinbarung werden die jeweils veröffentlichten Inhalte automatisch dem Kreis zugänglich. Es ist in den meisten Netzwerken prinzipiell möglich, die Einsehbarkeit der eigenen Seite auf einen bestimmten Freundeskreis zu beschränken. Unterbleibt eine solche Beschränkung jedoch, können auch Fremde die eigene Seite einsehen und gegebenenfalls Nachrichten an den Nutzer schicken.

Der Inhaltsteil besteht aus den Beiträgen der Nutzer selbst. Dies können bloße Äußerungen sein, allerdings auch geteilte Links, Bilder oder Videos. Die Beiträge können mit thematischen Stichworten (Tags) kategorisiert werden, damit Dritte sie wiederfinden können. Eine von Twitter-Usern entwickelte Form der Kategorisierung (Tagging) in der Nachricht selbst ist die Verwendung der Raute # (Englisch: hash sign) in Verbindung mit dem Stichwort. Dieses inzwischen als sogenanntes Hashtag bekannte Verfahren hat sich auch auf anderen sozialen Medien eingebürgert. Tagging erlaubt es, Postings zum selben Thema zu sammeln und Themen in dieser Weise zu verfolgen.

Die meisten sozialen Netzwerke verfügen neben einer internen Suchfunktion über Möglichkeiten auch für automatische Datenverarbeitungsanlagen, auf die nicht geschützten Inhalte in sozialen Netzwerken zuzugreifen. Foren haben in der Vergangenheit hierfür oft den Standard RSS (Rich Site Summary) oder das ähnliche Atom eingesetzt, bei denen in strukturierter Form (XML)[13] in der Regel die neuesten Postings automatisiert abrufbar waren. Diese Praxis wurde bei großen sozialen Netzwerken mehr und mehr durch nichtstandardisierte, proprietäre Schnittstellen (APIs)[14] ersetzt. Diese APIs erlauben häufig den Abruf von einzelnen Postings nahezu in Echtzeit (Stream), wobei eine Speicherung beim Empfänger möglich, aber nicht notwendig ist. Wie viele Profildaten in den einzelnen Datensätzen mitübertragen werden können, hängt von der API ab, oft sind dies aber zumindest der Name oder Benutzername und das Porträtbild, die Zeit des Postings sowie unter Umständen die benutzte Client-Software und Standortdaten. Manche APIs erlauben darüber hinaus das Herunterladen sämtlicher Standortdaten, Reaktionen und Kommentare von Dritten zu einem Posting. Ob all diese Daten tatsächlich abgerufen werden, oder ob von vornherein eine Auswahl getroffen wird, ist gegebenenfalls auch eine Frage der CRM-seitig verwendeten Software (des Clients).

1.4.3 Privatsphäre-Einstellungen

Das Geschäftsmodell vieler sozialer Netzwerke beruht auf der Zugänglichkeit von Daten. Dies entspricht sowohl der Konzeption des globalen Austauschs als auch der Bestrebung der Social Media-Anbieter, möglichst attraktiv für Marketingvorhaben von Unternehmen zu sein. Umfassende Möglichkeiten des Nutzers, die Leserbarkeit seiner Profil- und Inhaltsdaten zu begrenzen, stehen diesen Geschäftszielen zumeist entgegen. Die Standardeinstellung von Twitter-Accounts sieht etwa vor, dass Profildaten und Beiträge frei zugänglich sind und von Suchmaschinen gefunden und indexiert werden können. Die Standardeinstellung „öffentlich" bestand bis 2014 auch bei Facebook, wurde aber jedenfalls für verfasste Beiträge auf neuen Accounts aufgegeben. Vielen Nutzern, ist die Öffentlichkeit eines Beitrags nicht bewusst. Bei Facebook wird der Empfängerkreis eines Postings etwa nur durch ein kleines Welt-Symbol an den betreffenden Elementen kenntlich. Teilweise sind die Privatsphäre-Einstellungen zudem bewusst kompliziert formuliert und übergranular: Wenn die Kenntnisnahme unerwünschter Dritter von Profildaten und Inhalten ausgeschlossen werden soll, musste dies bei Facebook jedenfalls bis 2014 für jede Kategorie (Interessen, Freunde, Fotos, Beiträge…) einzeln geschehen. Die Folge ist, dass viele Nutzer entweder die Motivation verlieren, oder eine oder mehrere Kategorien übersehen.

[13] Extensible Markup Language, eine Sprache zur Darstellung hierarchisch strukturierter Daten.

[14] Application Programming Interface, also eine Programmierschnittstelle für Anwendungen.

Twitter ist aufgrund der beschränkteren Veröffentlichungsmöglichkeiten in dieser Hinsicht einfacher zu handhaben. Allerdings werden auch aus geschützten Profilen (wie bei Facebook) pseudonyme oder pseudonymisierte Daten durch Twitter selbst erhoben und Werbekunden angeboten. Die automatisierte Abrufbarkeit der Daten schränkt zudem den Selbstdatenschutz ein, weil vom Nutzer textlich gesetzte Hinweise auf gewünschte Vertraulichkeit nicht zur Geltung kommen.

1.5 Social-CRM-Tools und weitere Hilfsmittel

Im Folgenden sollen typische Werkzeuge vorgestellt werden, die die Einbindung von sozialen Medien in die CRM-Strategie ermöglichen. Da Social CRM-Systeme häufig sehr modular arbeiten, können einige Systeme auf einige der genannten Werkzeuge verzichten, manche Komponenten können Teilfunktionen verschiedener Tools in sich vereinigen oder Abläufe aus anderen Geschäftsbereichen übernehmen.

1.5.1 Social-CRM-Tools

Zunächst sind die Funktionen der CRM-Systeme, so wie sie im Durchschnitt von den Herstellern angeboten werden, darzustellen.

1.5.1.1 CRM im engeren Sinne

Das eigentliche CRM ist die Kundendatenbank.[15] Hier sind insbesondere abgelegt:

- Stammdaten der Kunden (z.B. Name, Geschlecht, Alter, Kontaktdaten),
- Vertrags- und Servicehistorie,
- insbesondere bei längerfristigen und/oder darlehensbasierten Vertragsverhältnissen Angaben zur ordnungsgemäßen Vertragsabwicklung und zum Zahlungsverhalten,
- Status laufender Servicefälle,
- etwaige Korrespondenz (E-Akte),
- abgegebene Einwilligungen.

Die Stammdaten wurden typischerweise beim Kunden selbst bei Abschluss eines Vertrages erhoben und dienen der Abwicklung. Sie sind meist mit dessen Zustimmung und aufgrund eigener Aktivität des Kunden erhoben worden, während Daten etwa zur Zahlungsmoral typischerweise aus Drittquellen (z.B. Auskunfteien) hinzugespeichert werden. Die Verkettung der erhobenen Daten zur Historie der Kundenbeziehung wird von der verantwortlichen Stelle zur Gewinnung neuer Daten und zur Erstellung detaillierter Profile der Bestandskunden genutzt. Datensätze aus dem CRM im engeren Sinne dienen auch zur Unterstützung von Service und Marketing.

CRM-Systeme können lokal (on-premise) installiert werden, werden aber zunehmend in Form von Software-as-a-service- (SaaS-) Produkten in der Cloud angeboten. Da die Cloud-Server sich oft im Ausland

[15] BPatG, Urt. v. 11.12.2013, 29 W (pat) 104/12, Anm. II.1.f.cc.

befinden, stellen sich hier, neben allgemeinen Fragen der Auftragsdatenverarbeitung, auch solche des grenzüberschreitenden Datenschutzes.

1.5.1.2 Business Intelligence/Business Analytics

Das Business Intelligence-Tool ist ein Rechenzentrum, in dem die bei einem Unternehmen anfallenden Rohdaten, auch solche aus verschiedenen Quellen („Data Warehouse"), aufbereitet und für Analysen und Marketingzwecke nutzbar gemacht werden können. Es kommen statistische und empirisch-soziologische Methoden zum Einsatz, für die Voraussagen auch Modellberechnungen. Durch Aggregation der Daten Betroffener und der Segmentierung nach eigenen Kriterien verschafft sich die verantwortliche Stelle einen Überblick über die Kundeninteressen. Eine weitere wichtige Aufgabe ist die Erstellung von Leistungskennzahlen zur Reichweite eines Produkts oder einer Marketingkampagne auf Basis der Häufigkeit ihrer Nennungen. Der Berechnung der Haltung von Social Media-Nutzern gegenüber einem Produkt dient schließlich die semantische Analyse ihrer Äußerungen. Durch die statistische Analyse von Auffälligkeiten und Mustern („Data Mining") können bisher unbekannte Tatsachen über Betroffene aus den Rohdaten gewonnen werden und umfassende Profile erstellt werden. Durch die mittel- und langfristige Analyse kann die Business Intelligence-Software Trends erkennen und Voraussagen z. B. über die Marktentwicklung treffen. Schließlich enthält Business Intelligence-Software eine Visualisierungskomponente und eine Funktion zur Generierung von Berichten, entweder zu allgemeinen Themen oder als Antwort zu bestimmten Fragen in Form der analytischen Datenverarbeitung (*online analytical processing,* OLAP). Eine weitere wichtige Funktion ist die Berechnung von Scores, Punktzahlen, welche automatisch nach mathematischen Modellen für bestimmte Inhalte eines Profils oder eines oder mehrerer Postings vergeben werden. Mit Scores wird klassischerweise die Bonität eines Betroffenen überprüft, gleichzeitig werden sie aber in einer Vielzahl anderer Bereiche eingesetzt, etwa zur Vorbereitung von Werbeansprachen („Werbescoring") und der Festsetzung von Preisen gegenüber Endverbrauchern.

1.5.1.3 Community Management

Beim Community Management handelt es sich zunächst um die Koordination der unternehmenseigenen Plattformen, soweit diese soziale Funktionen aufweisen. Typischerweise handelt es sich hierbei um Foren, es können aber auch zum Kommentieren freigegebene Blogs oder bearbeitbare Wikis hierunter fallen. Das Community Management ist weitgehend von Menschen gesteuert, hier geht es insbesondere um die Verhinderung negativer Stimmung im Forum und die effiziente Bearbeitung gezielter Anfragen. Daten aus dem CRM im eigentlichen Sinne und dem Support fließen oft in das Community Management ein.

Daneben existieren Fälle des Community Management auf Plattformen, die von Dritten zur Verfügung gestellt werden. Inwieweit der CRM-Betreiber hier telemedienrechtlich und datenschutzrechtlich (mit-)verantwortlich ist, ist derzeit noch umstritten. Bekanntestes Beispiel sind die sogenannten „Fan-Seiten" bei Facebook, die Fallgruppe umfasst aber alle vom Unternehmen selbst unterhaltene Profile auf sozialen Plattformen.

1.5.1.4 Social Media Management

Social Media Management ist die Leitungsfunktion über den operativen Einsatz von sozialen Medien. Auch dies ist eine weitgehend von Menschen wahrgenommene Aufgabe. Sie umfasst einerseits die Entscheidung, auf welchen Plattformen Accounts eingerichtet werden und was auf diese gepostet wird.

Andererseits obliegt dem Social Media Manager auch die Verantwortung für die Durchführung von ganzen Marketingkampagnen auf sozialen Medien und die Entscheidung, wie das Feedback auf die Kampagne zu handhaben ist, um einen positiven Effekt für das Unternehmen zu erzielen. Eine datenschutzrechtlich entscheidende Funktion des Social Media Managements liegt in der Interaktion mit Kunden, sei es zu Werbezwecken, zur Verhinderung oder Eindämmung von Wellen negativer Stimmung oder, in Zusammenarbeit mit der entsprechenden Abteilung, zum Zwecke des Service. Dabei kann auch von den nicht unmittelbar werblichen Ansprachen ein sekundärer Werbeeffekt ausgehen.

1.5.1.5 Social Media Monitoring/Social Listening

Die Social Media Monitoring- bzw. Social Listening-Software ist aus datenschutzrechtlicher Sicht diejenige Datenverarbeitungsanlage, die die automatisierte Erhebung von Daten aus sozialen Medien durchführt.[16] Die Software ist der Business Analytics-Software vorgeschaltet und versorgt diese mit Rohdaten. Dazu verfolgt das Social Media Monitoring-Tool mithilfe der API des sozialen Mediums meist den gesamten Datenstrom und filtert mithilfe von Stichwortsuchen relevante Posts heraus. Viele Social Media Monitoring-Tools verfügen über eine Funktion, die den zuständigen Sachbearbeiter warnt, falls ein definiertes Stichwort (z.B. der Name eines Produkts) genannt wird, damit dieser bei Bedarf hierauf entweder selbst reagieren kann, oder den betreffenden Post an die Supportabteilung weiterleiten kann. Einige Komponenten dieser Art können zudem selbst semantische Analysen vornehmen, und dadurch den Betreiber warnen, falls eine Äußerung zu einem Suchbegriff von der Software als negativ beurteilt wird, insbesondere, wenn solche negativen Meinungsäußerungen sich häufen. Die von dem Monitoring-Tool erhobenen Daten können, müssen aber nicht im Data Warehouse gespeichert werden. Die pauschale Speicherung *aller* Nennungen eines Unternehmens ist häufig anzutreffen, wird aber von der Wirtschaft inzwischen kritisch gesehen, weil ihr oft kein konkreter Plan zur Datennutzung angeschlossen ist und die Daten kaum mehr als Ballast darstellen. Sie ist aufgrund des Mangels an Zwecksetzung auch aus datenschutzrechtlicher Sicht kritisch zu betrachten.

1.5.1.6 Social Network Analysis

Nutzer sozialer Netzwerke bilden Freundeskreise. Die Analyse dieser Freundeskreise, soweit sie verfügbar sind, ist interessant für die Unternehmen, da sich Meinungen zu Produkten oft entlang von Freundschaftsbeziehungen fortpflanzen. Die Social Network Analysis-Software kann Freundschaftsbeziehungen als Netzwerke visualisieren und den Einfluss von Meinungsführern und aktiven Gruppen innerhalb dieser Netzwerke darstellen und nach weiteren Kriterien sortieren. Dabei wird gelegentlich eine Pseudonymisierung durchgeführt, in anderen Fällen bleiben die Nutzer unter ihren Klarnamen sichtbar.

1.5.1.7 Social Search

Die Social-Search-Funktion hat Gemeinsamkeiten mit dem Social Media Monitoring, da auch hier Daten und Aussagen erhoben und gegebenenfalls automatisch zur Generierung von Kennzahlen genutzt werden. Der Unterschied zum Social-Media-Monitoring liegt darin, dass Social Search keine Beobachtung in Echtzeit ermöglicht, sondern nur ein statisches Bild eines Augenblicks mit (einstellbar weitem) Blick in die Vergangenheit ergibt. Es handelt sich um eine (interne oder externe) Suchmaschine, die zu Stichwörtern

[16] Vgl. Hoeren/Siebert/Holznagel, Multimedia-Recht, Teil 21.1, Rn. 44.

die in letzter Zeit erfolgten Nennungen zurückgibt. Neben den von CRM-Anbietern bereitgestellten Social-Search-Engines kommen auch solche von Drittanbietern zum Einsatz, insbesondere diejenigen, die von den Plattformen selbst zur Verfügung gestellt werden.

1.5.2 Weitere Mittel der Datengewinnung auf sozialen Plattformen

1.5.2.1 Apps

Zum Teil werden sogenannte Apps als kompakte Anwendungen in soziale Netzwerke integriert, die auch von einem anderen Anbieter als dem Betreiber des sozialen Netzwerks stammen können.[17] Der Anbieter einer solchen App ist Telediensteanbieter (§ 2 Nr. 1 TMG)[18], er ist damit den Vorschriften des Telemedienrechts unterworfen. Gegen die Gewährung der Nutzung der Anwendung erhält der Betreiber in der Regel in Form von Zugang zu Profildaten wesentlich mehr Informationen, als für das Bereitstellen der Applikation notwendig ist. Deswegen ist eine ordnungsgemäße Einwilligung nach dem Telemediengesetz für den Betrieb jeder App erforderlich.

1.5.2.2 Social Plugins

Durch Setzen eines kleinen, vom Browser in der Regel automatisch geladenen Skripts des sozialen Netzwerks auf einer großen Anzahl verschiedener Webseiten können die Browsing-Gewohnheiten der Besucher verfolgt werden. Angezeigt wird beispielsweise ein Button, mit dessen Drücken der Nutzer seinen Gefallen an der Webseite ausdrücken kann. Tut er dies, während er auf dem Netzwerk eingeloggt ist, wird dies auf seiner Seite angezeigt. Gleichzeitig wird bereits während die Webseite mit dem Code lädt, die IP-Adresse des Nutzers automatisch an das soziale Netzwerk übertragen und ein eventuell schon vorhandener Cookie ausgelesen. Dies ist auch dann der Fall, wenn der Betroffene nicht auf den Button klickt. Ist der Betroffene während dieser Zeit eingeloggt, kann der Besuch der Website ihm eindeutig zugeordnet werden. Soziale Netzwerke bereiten diese Daten auf und stellen sie (unter Umständen pseudonymisiert bzw. anonymisiert) Werbetreibenden, und damit auch CRM-Betreibern zur Verfügung. Eine andere Form der Datengewinnung auf diese Art ist die Verknüpfung des Logins eines beliebigen Internetdienstes (z.B. eines Musikanbieters) mit einem Social Media-Account. D.h., um den Dienst in Anspruch nehmen zu können, muss der Betroffene sowohl an den Social Media-Anbieter Daten zur Nutzung des Dienstes übermitteln, als auch dem Dienst die Daten des eigenen Accounts zur Verfügung stellen.

1.5.2.3 Cookies

Ein HTTP-Cookie ist eine Textdatei, die durch den Header einer Website an einen Webbrowser übermitteln wird, und in der grundsätzliche Informationen zur Wiedererkennung des Browsers gespeichert werden können.[19] Es gibt zwei grundsätzliche Formen von Cookies, die sich funktional nach ihrem Einsatzzweck und technisch durch die Festlegung eines Ablaufdatums unterscheiden. Der Session-Cookie dient,

---

[17] Z.B. die Facebook-App der Europäischen Union, vgl. Kommissionsdokument COM/2014/0687 final v. 31.02.2014, Ziff. 2.1.

[18] Hoeren, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 18.2, Rn. 53; Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 TMG, Rn. 2; LG München I, WRP 2005, S. 1042; LG Memmingen, MMR 2004, S. 769; LG Berlin, WRP 2004, S. 1198.

[19] Ausf. Bonk, Technische Möglichkeiten der Datenerhebung, S. 29 f.

etwa im Rahmen eines Logins gesetzt, dazu, einen einzelnen Nutzer (bzw. den jeweiligen Nutzer des Webbrowsers) über unterschiedliche Seiten einer Domain hinweg wiederzuerkennen. So wird verhindert, dass ein einmal eingeloggter Nutzer sich bei jedem Wechsel der eingesehenen Seite, etwa in einem Webshop, neu authentifizieren muss.[20] Ein häufiger Anwendungsfall sind Authentifizierungscookies, mit denen Nutzer identifiziert werden, nachdem sie sich angemeldet haben.[21] Session Cookies enthalten kein Ablaufdatum und werden daher von den meisten Browsern spätestens bei Schließen des Browsers, ansonsten nach Log-out gelöscht.[22]

Ein Permanenter Cookie hingegen besitzt ein Ablaufdatum. Bis dahin kann sein Inhalt bei Aufruf der Tracker-Domain oder einer Webseite, auf der ein Skript der Tracker-Domain ausgeführt wird, eingesehen und unabhängig von einer bestehenden Session z.B. zur Analyse der Browsinggewohnheiten des Betroffenen ausgewertet werden.[23] Teilweise verlängert sich das Ablaufdatum permanenter Cookies dadurch, dass die zugehörige Website erneut aufgerufen wird, sodass ein dauerhafter Einsatz erfolgen kann.[24] Permanente Cookies waren früh ein Werkzeug der Werbung auf Internetseiten, wobei sie bald nicht mehr auf die Verfolgung von Nutzern über nur eine Webseite beschränkt waren. Insbesondere Werbenetzwerke verwenden sog. Third-Party-Cookies. Darunter werden Cookies verstanden, die von einer anderen Partei gesetzt werden als der, die den Webserver betreibt, mit dem der Hauptinhalt dargestellt wird.[25] Hierbei wird ein Skript des Werbenetzwerks auf mehreren voneinander unabhängigen Webseiten ausgeführt, welches die Seitenaufrufe registriert und zusammenführt. Die dabei gewonnenen Nutzerprofile enthalten eine umfassende Aufstellung der Interessen, Gewohnheiten und Standorte einer Person, sodass sie zielgerichtete Werbung ermöglichen.[26] Betroffene haben hiervon in den meisten Fällen keine Kenntnis. Die Ergebnisse dieser Erhebungen lassen ein umfassendes Profil über das Surfverhalten entstehen, das sich bei der betreffenden Domain in Echtzeit erweitert und üblicherweise zur Anzeige verhaltensbasierter Werbung (behavioral advertising) genutzt wird. Langlebige permanente Cookies müssen in der Regel manuell oder mit Hilfe der entsprechenden Browserfunktion durch den Betroffenen selbst gelöscht werden. Die Möglichkeit zur Nutzung von Cookies ist in Europa durch die ePrivacy-Richtline[27] geregelt, der jedoch nur europäische Unternehmen unterfallen. In den USA existieren hingegen keine umfassenden Gesetze zur Datenerhebung zu Werbezwecken.[28] Die Industrie reguliert sich über Standards von Organisationen wie der Digital Advertising Alliance (DAA) und der Direct Marketing Association (DMA) weitgehend selbst.

---

20 Art. 29-Datenschutzgruppe, WP 188, S. 8; WP 194, S. 7.

21 Art. 29-Datenschutzgruppe, WP 188, S. 8; WP 194, S. 7.

22 Art. 29-Datenschutzgruppe, WP 194, S. 4.

23 Art. 29-Datenschutzgruppe, WP 171, S. 6.

24 Art. 29-Datenschutzgruppe, WP 171, S. 7.

25 Art. 29-Datenschutzgruppe, WP 171, S. 7; WP 194, S. 5.

26 Art. 29-Datenschutzgruppe, WP 171, S. 7 f.

27 Richtlinie 2002/58/EG.

28 Vgl. Arning/Haag, in: Heidrich/Forgó/Feldmann, Heise Online-Recht, Kap. II, Rn. 160.

Da die Werbebranche im Internet an einer möglichst umfassenden Datensammlung interessiert ist, gab es in den letzten Jahren Bestrebungen, das Löschen von Cookies zu erschweren oder ganz zu unterbinden. Der erste Ansatz waren sogenannte Locally Shared Objects (LSOs), welche von Multimedia-Objekten des Formats Adobe Flash generiert werden.[29] In diesem Typ von Cookies können wegen des größeren Speicherplatzes (100 KB statt 4 KB) noch detailliertere Information zum Browsing als in einem klassischen Cookie abgelegt werden. Außerdem werden LSOs nicht, wie HTTP-Cookies, im Browserverzeichnis, sondern in den allgemeinen Anwendungsdaten abgelegt, so dass sie browserübergreifend zur Verfügung stehen. LSOs sind von Browsern mit den Standardeinstellungen oft überhaupt nicht, und manuell nicht ohne vertiefte Kenntnisse löschbar.

Zusätzlich wurde ein Verfahren für ein Zusammenwirken von HTTP- und LSO entwickelt, indem für jedes HTTP-Cookie ein LSO mitgeneriert wurde, dessen Inhalt den des HTTP-Cookies spiegelte. Das LSO konnte erkennen, wenn das HTTP-Cookie gelöscht wurde, und generierte es in diesem Fall erneut (ugs. sog. Zombie-Cookie).[30] Dadurch wurden Cookies nahezu unlöschbar. In welchem Maße solche selbsterhaltenden Cookies derzeit gegenüber Nutzern in Deutschland verwendet werden, ist unklar. LSOs, die für sich bereits eine umfassende Profilbildung erlauben, sind dagegen in sehr vielen populären sozialen Medien anzutreffen, hervorzuheben sind hier insbesondere YouTube, Vimeo und andere videobasierte Plattformen, die auf HTML5 beziehungsweise Flash aufbauen.

Der Flash-Standard wird vielerorts nach und nach durch HTML5 ersetzt. Die Möglichkeiten durch dessen Web Storage (DOM Storage)-Funktionalität gehen jedoch über die herkömmlicher Cookies noch weit hinaus, Webseiten erhalten noch größeren Speicherplatz (mindestens 5 MB) zum Ablegen beliebiger Daten, die durch den Benutzer praktisch nicht gesteuert werden können. Ein Verfallsdatum wie bei HTTP-Cookies gibt es bei Web Storage nicht. Bereits heute wird Web Storage insbesondere auf großen amerikanischen Webseiten zum Zwecke der Reichweitenanalyse umfassend genutzt.

1.5.2.4 Tracking-Pixel

Ein Tracking-Pixel oder Web Bug ist eine Bilddatei in der kleinstmöglichen Größe von 1x1 Pixel, welche unauffällig in E-Mails und auf Webseiten platziert werden kann und analog zu den Grafiken im Cross-Site-Tracking auf einem zentralen Server gespeichert ist. Dieser Server registriert, wenn der Pixel abgerufen wird und speichert den Abruf mitsamt der IP-Adresse des Betroffenen und anderen die Bestimmbarkeit ermöglichenden Merkmalen in einer Logdatei. Durch Gebrauch eines Tracking-Pixels kann sicher festgestellt werden, dass und von welchem Anschluss die Seite oder E-Mail tatsächlich geladen wurde.

Ein Unternehmen, welches mehrere Webseiten betreibt, kann für alle Seiten denselben Trackingpixel verwenden und den Betroffenen somit leicht über mehrere Webseiten verfolgen. Wenn, wie üblich, der Tracking-Pixel als einfache Bilddatei ohne Ausführung eines Skripts konzipiert ist, kann sich der Betroffene gegen diese Verfolgungsmethode in der Regel nur schützen, wenn er das Laden von Bilddateien auf Webseiten unterbindet, was in der Praxis kaum geschieht, schon, weil damit eine erhebliche Einschränkung der Funktionalität vieler Webseiten einhergeht.

---

[29] Art. 29-Datenschutzgruppe, WP 171, S. 6 f.

[30] Art. 29-Datenschutzgruppe, WP 208.

Tracking-Pixel in E-Mails sind ein beliebtes Mittel des Direktmarketings um die Reichweite der eigenen Werbung zu messen. In diesem Fall bestätigt das Laden des Pixels, dass die E-Mail zumindest geöffnet wurde. In früheren Zeiten galten als einzig wirksame Gegenmaßnahmen, entweder einen E-Mail-Client zu benutzen, welcher keine HTML-Elemente sondern nur Plaintext verarbeiten konnte. Das Tag zur Einbindung von Grafiken bei der Anzeige der E-Mail wird dort schlicht ignoriert. Alternativ kann die E-Mail nur offline geöffnet werden, damit kein Download des Pixels möglich ist. Gegebenenfalls kann auf letztere Weise auch die Einbindung von Tracking-Pixeln erkannt werden, da der Client eine nicht geladene Grafik durch ein entsprechendes (größeres) Icon an unerwarteter Stelle anzeigen würde.

Moderne E-Mail-Clients besitzen meist die Standardeinstellung, Grafiken nur auf Aufforderung zu laden. Zwar ist es technisch nicht möglich, den Nutzer vor einem Tracking-Pixel zu warnen, aber die Möglichkeit, E-Mails aus kommerzieller Quelle zunächst in reiner Textform zur Kenntnis zu nehmen, bringt für den Betroffenen einen deutlichen Kontrollgewinn mit sich. Sie veranlasst die verantwortlichen Stellen auch dazu, den Kern ihrer Mitteilung als (HTML-)Text und nicht als Grafik, welche Text nur darstellt, zu fassen, wodurch das Nachladen von Inhalten von gegebenenfalls problematischen Quellen an Bedeutung verliert.

1.6 Gesetzlicher Rahmen der Nutzung von Social CRM

Sodann sind die für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Social CRM-Aktivitäten heranzuziehenden Bestimmungen darzustellen. Die derzeit wichtigste Quelle für den Datenschutz in Deutschland ist das Bundesdatenschutzgesetz. Es beruht seit dem Volkszählungsurteil vom 15.12.1983[31] auf dem Recht auf informationelle Selbstbestimmung. Dieses Grundrecht fußt seinerseits auf dem Allgemeinen Persönlichkeitsrechts nach Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG und beinhaltet das Recht des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden.

Das Gericht wies in diesem Zusammenhang darauf hin, dass die überkommene Eingriffsdogmatik zum Allgemeinen Persönlichkeitsrecht der neuen Bedrohungen automatisierter Datenverarbeitungen nicht Herr werden könne.[32] Die Anreicherung von Datensätzen mit „öffentlichen" Daten macht eine Profilbildung oft überhaupt erst möglich[33]. Folge ist neben dem Kontrollverlust ein Verlust an Zwanglosigkeit beim Bewegen in der Öffentlichkeit, der auf die Grundrechtsausübung belastend wirken kann und dadurch, vom Grundgesetz nicht beabsichtigte, Konformität im Verhalten auslösen kann. Diesen spezifischen Gefahren der Datenverarbeitung muss seitdem jede Eingriffsbegründung Rechnung tragen. Diese Konkretisierung ist für die sozialen Medien mit ihren Massen an „allgemein zugänglichen" und daher scheinbar „nur" die Sozialsphäre der Betroffenen tangierenden Daten von zentraler Bedeutung. Dieser grundrechtliche Schutz wurde dem Betroffenen grundsätzlich auch gegenüber nicht-öffentlichen Stellen zugebilligt, da Abwehrrechte nach der vom Bundesverfassungsgericht im Lüth-Urteil[34] aufgestellten

[31] BVerfGE 65, 1.

[32] BVerfGE 65, 1, Ls. 1.

[33] BVerfGE 65, 1 (3); Becker, in: Hill/Schliesky, E-Volution des Rechts- und Verwaltungssystems, S. 62.

[34] BVerfGE 7, 198.

Formel eine objektive Werteordnung aufstellen und so mittelbar in ausfüllungsbedürftige Normen, etwa Generalklauseln, einstrahlen (mittelbare Drittwirkung). Spätere verfassungsgerichtliche Rechtsprechung bestätigte die horizontale Wirkung des Grundrechts zwischen Privaten.[35] Die verfassungsrechtliche Rechtsprechung wurde konkretisiert durch den Erlass des Bundesdatenschutzgesetzes,[36] wodurch seine Kerngedanken in einfachem Bundesrecht verankert wurden.

Aufgrund der zunehmenden Technisierung und Globalisierung der Datenverarbeitung befand die Europäische Gemeinschaft in den neunziger Jahren, dass der Datenschutz im Binnenmarkt einer Regelung bedürfe, welche die Übermittlung personenbezogener Daten innerhalb der Gemeinschaft risikoärmer machen solle. So entstand 1995 die Datenschutz-Richtlinie[37] (im Weiteren DSRL), die durch Anpassungen der Datenschutzgesetze des Bundes und der Länder umgesetzt wurde. Die Richtlinie setzt zwar nicht selbst Recht in Deutschland, das Bundesdatenschutzgesetz in seiner heutigen Form ist jedoch wesentlich an der Struktur der Richtlinie orientiert. Im Übrigen sind nationale Regelungen stets richtlinienkonform auszulegen, um dem Gemeinschaftsrecht zur Wirksamkeit zu verhelfen (effet utile).[38] Zur Datenschutzrichtlinie kam 2002 die ePrivacy-Richtlinie[39] hinzu, welche sich an Betreiber von Kommunikationsdiensten wendet und umfassend die zulässige Kundendatenverarbeitung regelt. Besondere Bedeutung hat im Zusammenhang von CRM die Vorschrift über die Zusendung unbestellter Werbenachrichten (Spam) in Art. 13 der ePrivacy-Richtlinie. Die Bestimmungen der Richtlinie sind im Telekommunikations-, Telemedien- und Wettbewerbsrecht umgesetzt.

Europäisches Datenschutzrecht ist an Art. 8 der EU-Grundrechtecharta zu messen, der mit dem Wirksamwerden des Vertrags von Lissabon Geltung erhielt. Eine weitere supranationale datenschutzrechtliche Vorschrift ist Art. 8 der Europäischen Menschenrechtskonvention (EMRK) des Europarats. Dieser Artikel hat in Deutschland zwar nur den Rang eines einfachen Gesetzes, muss aufgrund seiner materiellen Grundrechtsgleichheit jedoch in der Auslegung der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) bei der Interpretation anderer einfacher Gesetze berücksichtigt werden.

Pflichten der Betreiber von Telemediendiensten sind heute im Telemediengesetz[40] normiert, welches bei Social CRM-Systemen insbesondere beim Betrieb eigener Plattformen die gesetzlichen Grundlagen enthält, auf derer eine Datenerhebung, -speicherung und -verwertung im Rahmen von Telemedien zulässig sein kann. Das Telemediengesetz enthält neben dem Telekommunikationsgesetz (TKG) die wichtigsten Vorschriften für Diensteanbieter von Telekommunikationsdiensten und Telemedien, insbesondere sind

---

35 Siehe nur BVerfG, Beschluss v. 17. Juli 2013, 1 BvR 3167/08, Rn. 13.

36 BVerfG, NJW 1984, 422; Gola/Schomerus, BDSG, § 4 Rn. 1.

37 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

38 Mayer, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Art. 19 EUV Rn. 57 f.

39 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

40 BGBl. 2007, 179.

hauptsächlich in diesen Gesetzen Inhalte der e-Commerce-Richtlinie[41] und der ePrivacy-Richtlinie[42] umgesetzt.

Datenschutzverstöße werden von der Rechtsprechung zunehmend als wettbewerbswidriges Marktverhalten im Sinne des § 4 Nr. 11 des Gesetzes gegen den unlauteren Wettbewerb (UWG) beurteilt, was zu Unterlassungs- und Schadensersatzansprüchen sowie staatlichen Sanktionen führen kann. Außerdem enthält das UWG in § 7 insbesondere zur Zusendung von unverlangter Werbung eigene datenschutzrechtliche Vorschriften. Daher hat das Wettbewerbsrecht in den letzten Jahren bei der Beurteilung von Datenschutzverstößen einen wesentlichen Bedeutungsgewinn erfahren.

[41] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr").

[42] Richtlinie 2002/58/EG.

2. Datenschutzrechtliche Anforderungen für typische Konstellationen im CRM

2.1 Reichweite der Studie

2.1.1 Gegenstand des Datenschutzrechts – personenbezogene Daten

Gemäß § 1 Abs. 2 BDSG gilt das Bundesdatenschutzgesetz nur für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Dieses Tatbestandsmerkmal wird in § 3 Abs. 1 BDSG genauer definiert: Personenbezogene Daten sind danach Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), juristische Personen müssen ihre Geheimnissphäre (etwa Betriebs- und Dienstgeheimnisse) daher anhand anderer Vorschriften schützen.[43]

Einzelangaben sind jede Art von Information über eine Person, solange sie in irgendeiner Form gemessen oder aufgezeichnet werden (mündlich, schriftlich, elektronisch).[44] Auf den Wahrheitswert oder die Sensibilität der Information kommt es nicht an.[45] Auch negative Angaben unterfallen dem. Verhältnisse sind alle Aspekte, die den Betroffenen als Menschen und Teil der Gesellschaft beschreiben[46] (nicht nur Eigenschaften, sondern auch etwa Aktivitäten, Erlebnisse, Lebensereignisse, Aussehen, Standorte, Präferenzen). Bestimmt ist eine Person, wenn eine eindeutige Zuordnung des Datums allein zu ihr unmittelbar möglich ist, z.B. durch Namensnennung. Bestimmbar ist jede Person, deren Zuordnung zu einem bestimmten Datensatz, gegebenenfalls unter Berücksichtigung von Zusatzwissen, ohne unverhältnismäßige Schwierigkeiten möglich ist.[47]

Die Nichtbestimmbarkeit der Bezugsperson eines Datums wird Anonymität genannt. Dabei geht das BDSG (§ 3 Abs. 6), komplementär zum Bestimmbarkeitsbegriff, nach ganz herrschender Meinung[48] von einem relativen Anonymitätsbegriff aus. Die Bestimmbarkeit muss daher nicht absolut ausgeschlossen sein, sondern muss nur „einen unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" erfordern.[49] Dabei ist vom Stand der Technik auszugehen. Weil die Anonymität gegen jedermann (absolut) wirken muss, handelt es sich bei der Unverhältnismäßigkeit um ein objektives Kriterium: Ob die verantwortliche Stelle eine Herstellung der Bestimmbarkeit anstrebt, oder ob sie über die Mittel hierzu verfügt, ist irrelevant. Der Begriff des anonymen Datums ist eng auszulegen. Wenn Daten erhoben werden, die nach objektiver Betrachtung keine Bestimmbarkeit aufweisen, spricht man von anonymen Daten, wenn die verantwortliche Stelle eine Anonymisierung personenbezogener Daten selbst vornimmt oder von

[43] Gola/Schomerus, BDSG, § 3 Rn. 3.

[44] Gola/Schomerus, BDSG, § 3 Rn. 3.

[45] Becker/Ambrock, JA 2011, S. 561.

[46] Gola/Schomerus, BDSG, § 3 Rn. 5.

[47] Vgl. BGH, NJW 1991, S. 568; Caspar, DÖV 2009, S. 967; Dammann, in: Simitis, BDSG, § 3 Rn. 22ff.

[48] Gola/Schomerus, BDSG, § 3 Rn. 44 m.w.N.; Kühling/Klar, NJW 2013, S. 3613.

[49] Dammann, in: Simitis, BDSG, 8. Aufl., § 3, Rn. 196.

einem Auftragsdatenverarbeiter vornehmen lässt, von anonymisierten Daten. Nur die Erhebung anonymer Daten bedarf keiner Rechtsgrundlage. Da neue Methoden der Analyse sowie Zusammenführung mit anderen Daten den Personenbezug gegebenenfalls herstellen können, ist die Anonymität vor der Weiterverarbeitung oder -nutzung stets zu überprüfen.

Nach diesen Definitionen ist eine große Mehrheit der in sozialen Netzwerken vorhandenenDaten personenbeziehbar: So fallen ohne weiteres statische IPs hierunter,[50] solange eine Zuordnung der Session zu der natürlichen Person beim Provider möglich ist. Die Auffassungen zur Personenbezogenheit dynamischer IPs gehen auseinander. In der früheren Rechtsprechung wurde diese oft allgemein abgelehnt. Eine differenzierte Ansicht hat das Landgericht Berlin[51] vertreten, welches einen Personenbezug dann für gegeben hält, wenn der verantwortlichen Stelle zusätzliche Daten, etwa aus einem Anmeldeformular, vorliegen. Dies verkennt, dass bei der Bestimmung des Personenbezugs das Zusatzwissen Dritter zu berücksichtigen ist und daher ein Personenbezug begrifflich erst dann wegfallen kann, wenn das Protokoll des Zugriffs auch beim Hostprovider gelöscht ist, was auch nach Abschaffung der Vorratsdatenspeicherung aus Gründen der Abwehr von Gefahren für das Kommunikationsnetz eine Woche in Anspruch nehmen darf.[52] Während dieser Zeit besteht der Personenbezug. Im Übrigen kann ein Forumsbetreiber eine statische von einer dynamischen Adresse in aller Regel nicht unterscheiden, die Eigenschaft als statisch oder dynamisch ist daher als Kriterium für die zulässige Speicherung praktisch unbrauchbar. Gegen das zitierte landgerichtliche Urteil ist inzwischen Berufung zum Bundesgerichtshof eingelegt worden, welcher wiederum[53] dem EuGH die Frage zur Vorabentscheidung (Art. 267 AEUV) vorgelegt hat, ob dynamische IPs personenbezogen im Sinne von Art. 2a) der Datenschutzrichtlinie seien. Die Entscheidung steht noch aus[54]. Es ist dabei wahrscheinlich, dass der EuGH die Personenbezogenheit von IPs bejahen wird, da er diese bereits in einer vorherigen Rechtssache ohne Differenzierung zwischen statischen und dynamischen Adressen angedeutet wurde.[55]

Problematisch ist der Fall der Wirkung von vom Benutzer gewählten Benutzernamen oder falschen Namen auf nicht unternehmenseigenen sozialen Plattformen. Datenschutzrechtlich handelt es sich hierbei um eine Pseudonymisierung, also den Austausch von Identifikationsmerkmalen mit einem Kennzeichen, wenn dadurch die Bestimmung des Betroffenen ausgeschlossen oder wesentlich erschwert wird (§ 3 Abs. 6a BDSG). Durch eine erfolgreiche Pseudonymisierung ist der Betroffene nur für den Besitzer der Zuordnungsfunktion, in diesem Fall dem Nutzer selbst, bestimmt. Die Bestimmbarkeit bleibt jedoch auch für Dritte stets erhalten, die Pseudonymisierung führt daher nicht zur Unanwendbarkeit von Datenschutzrecht. Stattdessen führt die Pseudonymisierung zu erleichterten Verarbeitungsbefugnissen in Fällen, in denen die Interessen der Betroffenen zu schützen sind. Eine ausdrückliche Privilegierung pseudonymer Daten findet sich zudem im Telemedienrecht (§ 15 Abs. 3 TMG) oder in landesrechtlichen Vorschriften (§

---

50 Überblick zu dem Personenbezug statischer IPs vgl. hierzu Meyerdierks, MMR 2013, S. 705 ff.; Krüger/Maucher, MMR 2011, S. 434; Gabriel/Cornels, MMR 11/2008, XIV, XVI; Dammann, in: Simitis, BDSG, § 3 Rn. 63; Steidle/Pordesch, DuD 2008, S. 327.

51 LG Berlin, Urt. vom 31. Januar 2013, 57 S 87/08, nicht rechtskräftig.

52 BGH, Urteil vom 03.07.2014, III ZR 391/13.

53 Beschl. v. 28.10.2014.

54 Breyer, ZD 2014, S. 400.

55 EuGH, Urt. vom 24.11.2011, C-70/ 10 - Scarlet ./. SABAM.

11 Abs. 6 LDSG SH), wo sie allerdings nur eingreift, wenn der Dienst tatsächlich (§ 13 Abs. 6 BDSG) zur pseudonymen Nutzung angeboten wird. Diese Vorschrift gilt also nur im Verhältnis zwischen Plattformanbieter und Nutzer, nicht aber gegenüber Nutzer und CRM-Betreiber. Aber auch in letzterem Verhältnis kann eine effektive Verwendung von Pseudonymen jedoch zumindest ein Indikator zugunsten der Zulässigkeit von Datenverarbeitungsvorgängen sein.

Dazu wäre es allerdings notwendig, dass die Bestimmbarkeit für den CRM-Betreiber tatsächlich wesentlich erschwert wird. Je ausführlicher das Profil ist, dessen Daten erhoben werden, und je attraktiver daher seine Erhebung in wirtschaftlicher Hinsicht ist, desto einfacher wird die Person bestimmbar und desto ineffektiver wird die Pseudonymisierung. Eine Person, von der bei Unkenntnis ihres Namens nur ein einziges, allgemeines Datum bekannt ist, z.B. ihr Geburtstag, ist nur schwer bestimmbar. Eine Person, von der die verantwortliche Stelle zwar nicht den Namen kennt, von der aber bekannt ist, dass sie in A-Stadt lebt, sich ein mongolisches Restaurant im Erdgeschoss ihres Hauses befindet, und sie Mitglied des örtlichen Karatevereins ist, wird verhältnismäßig leicht bestimmbar. Aber auch die Verknüpfung von mehreren an sich generischen Daten kann, gegebenenfalls unter Einbeziehung für die Öffentlichkeit unzugänglicher Register, die Bestimmung eines Betroffenen ermöglichen, so die Angabe „fährt weißen VW Golf" und „Verfahren beim Landgericht Augsburg anhängig". Auch der gewählte Zeichensatz kann für die Pseudonymisierung relevant werden. So stellt etwa der Zeichensatz Unicode Zeichen zur Verfügung, bei denen die Buchstaben des betreffenden Namens gekippt oder gespiegelt dargestellt werden. Bekannt ist auch der Leet-Speak, bei denen aus den Zeichen des ASCII-Codes für einzelne Buchstaben ähnlich aussehende Zeichen substituiert werden. In dieser Art geschriebene Nutzernamen mögen für maschinelle Datenverarbeitung unlesbar sein, ein Mensch kann die Zuordnung dagegen unproblematisch vornehmen.

Es ist daher festzuhalten, dass Pseudonymisierung nicht mit der Verwendung eines falschen Namens gleichzusetzen ist und dies auf sozialen Medien selten zu einer Privilegierung führen wird.

2.1.2 Anwendbarkeit deutschen Rechts

2.1.2.1 Anwendbarkeit des BDSG

Sodann ist eine Eingrenzung des Gegenstands der vorliegenden Studie dahingehend vorzunehmen, dass auf die in ihr behandelten Fälle deutsches Datenschutzrecht anwendbar sein muss. Die relevante Vorschrift zur territorialen Geltung ist § 1 Abs. 5 BDSG und Ergebnis einer Umsetzung der Art. 4 Abs. 1 a) und c) der EG-Datenschutzrichtlinie.

Entscheidender Anknüpfungspunkt für die Anwendung nationalen Rechts auf Unternehmen, die in einem anderen Mitgliedstaat der EU oder des EWR gelegen sind, ist die Niederlassung im Inland (§ 1 Abs. 5 Satz 1 BDSG). Gleiches gilt in Anwendung von Art. 4 Abs. 1 a) der Richtlinie 95/46/EG für Unternehmen außerhalb der EU und des EWR, die eine Niederlassung im Inland unterhalten. Den Ansatz einer Konkretisierung leistet Erwägungsgrund 19 der Richtlinie 95/46/EG, der bestimmt, dass eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraussetzt, wobei die Rechtsform nicht maßgeblich sein soll. Der EuGH hat im Google-Urteil[56] die Anwendbarkeit nationa-

[56] EuGH, Urt. v. 13.05.2014, C-131/12.

len Rechts auch für Fälle bejaht, in denen nur eine Nebentätigkeit im Geschäftsbetrieb (hier: Anzeigenakquise) in einem Mitgliedsstaat betrieben wird. Keine Niederlassung ist dagegen ein bloßer Server.[57]

Das BDSG wird ferner für anwendbar erklärt, soweit ein Unternehmen, welches nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des EWR belegen ist, personenbezogene Daten in Deutschland erhebt, verarbeitet oder nutzt (§ 1 Abs. 5 Satz 2 BDSG). Es handelt sich um die Umsetzung von Art. 4 Abs. 1 c) der Richtlinie 95/46/EG, wonach nationales Datenschutzrecht eines Mitgliedsstaats anwendbar ist, wenn auf Mittel zurückgegriffen wird, die auf dem Gebiet des Mitgliedsstaats belegen sind. Dabei wird im Schrifttum und Teilen der Rechtsprechung für ausreichend gehalten, dass Cookies auf dem Computer eines Betroffenen installiert werden.[58]

2.1.2.2 Anwendbarkeit des TMG

Das Telemediengesetz enthält in seinen §§ 2a und 3 eigene Regelungen zur Unterstellung von Diensteanbietern unter deutsches Recht. Dabei wird eine ausführliche Differenzierung danach vorgenommen, welche europarechtlichen Normen für das Telemedium einschlägig sind. Grundsätzlich gilt im Gegensatz zum Niederlassungsprinzip des BDSG (s.o.) für das TMG das Sitzlandprinzip. Für CRM-Dienste findet in der Regel die Richtlinie 2000/31/EG (E-Commerce-Richtlinie) Anwendung. Dementsprechend ist gemäß § 2 Abs. 1 Satz 1 TMG entscheidend, wo der Diensteanbieter seine Geschäftstätigkeit tatsächlich ausübt. Nach § 2 Abs. 1 Satz 2 TMG ist dabei entscheidend wo sich der Mittelpunkt der Tätigkeit des Diensteanbieters im Hinblick auf das Telemedienangebot befindet. Das TMG gilt daher grundsätzlich nur für Unternehmen mit Sitz in Deutschland. Die Anwendbarkeit deutschen Rechts bleibt bestehen, wenn sich der Sitz des Diensteanbieters in Deutschland befindet, sich das Angebot aber an Personen in Drittländern richtet (§ 3 Abs. 1 TMG). Für den umgekehrten Fall, also für Diensteanbieter mit Sitz in einem anderen Staat des Europäischen Wirtschaftsraums gilt dies nur, wenn es zum Schutz der öffentlichen Sicherheit oder Ordnung, der öffentlichen Gesundheit und des Verbraucher- und Anlegerschutzes angemessen ist (§ 3 Abs. 5 TMG). Außereuropäische Diensteanbieter wie Facebook oder Twitter unterfallen nicht dem Anwendungsbereich der Richtlinie 2000/31/EG. Dementsprechend treffen diese Anwender auch nicht die Pflichten des TMG.[59] Verantwortliche Stellen, die außereuropäische Diensteanbieter nutzen und über diese Plattformen CRM-Systeme einsetzen, sind als innereuropäische Anbieter allerdings an das TMG gebunden. Deswegen sind europäische Betreiber einer Seite in einem außereuropäischen sozialen Netzwerk (z.B. einer Facebook-Fanpage) verpflichtet, ein Impressum einzufügen[60].

2.2 Grundbedingungen des Betriebs von Social CRM-Systemen

Im Folgenden sollen Aspekte des Betriebs von Social CRM-Systemen betrachtet werden, welche unabhängig von der direkten Interaktion mit sozialen Medien zu berücksichtigen sind. Sie sind somit nicht

---

[57] Art. 29-Datenschutzgruppe, WP 179, S. 15.

[58] Siehe etwa Weichert, in: Däubler/Klebe/Wedde/Weichert, § 1, Rn. 17, KG Berlin, Urt. v. 24.01.2014, 5 U 42/12, S . 26.

[59] Nordmeier, in: Spindler/Schuster, Recht der elektronischen Medien, § 2 TMG, Rn. 6.

[60] OLG Düsseldorf, MMR 2008, S. 682; LG Berlin, Beschl. v. 14.07.2004, Az. 102 O 161/04; KG Berlin, GRUR-RR 2007, S. 326; s.a. LG Aschaffenburg, MMR 2012,S. 38; LG Frankfurt a. M., B. v. 19. 10. 2011 – 3-08 O 136/11.

Social-Media-spezifisch. Trotzdem ist ihre Beachtung bei der Einrichtung neuer Verfahren (Einrichtung neuer Erhebungsmethoden, Nutzung neuer Software, Outsourcing) auch für die rechtliche Absicherung der verantwortlichen Stelle unverzichtbar. Eine Verbindung der allgemeinen Ausführungen mit Besonderheiten der sozialen Medien wird nach Möglichkeit hergestellt.

2.2.1 Datenschutzmanagement

Erste Voraussetzung des Betriebs jedweden Datenverarbeitungssystems von der Größenordnung eines CRM ist die Etablierung eines Datenschutzmanagements. Grundsätzliches Ziel des Managements sollte es sein, die folgenden Schutzziele des Datenschutzrechts optimal zu verwirklichen:[61]

- Vertraulichkeit (nur Befugte haben Zugriff auf Daten),
- Integrität (Vollständigkeit und Aktualität von Datengrundlagen),
- Verfügbarkeit (Daten stehen zum Abruf rechtzeitig und vollständig bereit),
- Intervenierbarkeit (Betroffenenrechte können effizient ausgeübt werden),
- Transparenz (Prüfbarkeit von Daten und Methoden),
- Nichtverkettbarkeit (Datenverarbeitungsvorgänge sind so konzipiert, dass getrennt erhobene Datensätze möglichst nicht zusammengeführt werden können).

Hierbei stellen die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) eine Hilfe im Sinne einer Best Practice-Anleitung dar. Deren Empfehlungen für das Datenschutzmanagement[62] lassen sich in folgende Gruppen einteilen:

Das schutzzielübergreifende Prozessmanagement erfordert zunächst die Einrichtung eines grundlegenden Mechanismus, welcher durch Vergleich von Sollen und Sein verbesserungsbedürftige Aspekte benennt und die Verbesserungen im Rahmen eines kontinuierlichen Monitorings beobachtet. Hierzu gehört auch ein Konzept zum Management von Datenlecks. Eine klare Aufteilung der Leitungsaufgaben ist unerlässlich, die Gesamtverantwortung muss auf der obersten Ebene angesiedelt sein.

Der nächste Schritt ist die Einrichtung eines Datenschutzkonzepts, welches der Sicherung der Rechtmäßigkeit der Datenverarbeitungsvorgänge selbst dient. Es soll umfassende Regeln formeller und materieller Natur enthalten, die den ordnungsgemäßen Datenkreislauf von den technischen Voraussetzung über Erhebung, Verarbeitung und Nutzung bis zu der Sicherstellung von Berichts-, Auskunfts-, Berichtigungs- und Löschpflichten sicherstellen sollen, ferner Maßnahmen zu Bekanntmachung und Umsetzung der festgelegten Regeln.

Über die Umsetzung des Datenschutzkonzepts soll ein betrieblicher Datenschutzbeauftragter wachen. Die Bestellung eines Datenschutzbeauftragten ist u. a. für nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten und bei denen mindestens zehn Personen regelmäßig mit Datenverarbeitungsvorgängen betraut sind, vorgeschrieben (§ 4f Abs. 1 BDSG). Der Datenschutzbeauftragte muss

---

[61] Instruktiv zu den einzelnen Schutzzielen siehe Rost in: Schmidt/Weichert, Grundlagen, Entwicklungen und Kontroversen, S. 353 ff.; Weichert, ZD 2013, S. 256 f; Weichert, SVR 2014, S. 244.

[62] Abrufbar unter www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02501.html.

weisungsfrei sein, die für die Ausübung seiner Tätigkeit notwendigen Mittel und Ausstattung erhalten und jederzeit Zugang zur Leitungsebene haben. Er muss sowohl neue Datenverarbeitungsprozesse als auch etablierte Prozesse überwachen**.** Daher muss er vor Etablierung eines neuen Datenverarbeitungsvorgangs beteiligt werden. Ihm obliegt zudem die Unterrichtung und Fortbildung der mit der Datenverarbeitung befassten Personen.

Ein gesetzlich vorgegebenes, spezifisches Prüfinstrument ist die Vorabkontrolle (§ 4d Abs. 5 f. BDSG). Sie findet statt, wenn besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG), z.B. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, verarbeitet werden sollen, oder wenn die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten (Profiling oder Scoring), oder vergleichbar einschneidende Maßnahmen getroffen werden sollen. Allgemein ist schon wegen der automatisierten Erhebung der Inhalte ganzer Profile nie auszuschließen, dass die regelmäßig vorhandenen Daten nach § 3 Abs. 9 BDSG verarbeitet werden. Formen von Profiling sind bei der Verarbeitung von Daten aus sozialen Netzwerken ein häufiges Szenario (z.B. Werbescoring, Leadgenerierung), so dass die Pflicht zu Vorabkontrolle von Verarbeitungsprozessen im SCRM-Bereich den Regelfall darstellen wird.

Neben der Kontrolle der Rechtmäßigkeit einzelner Datenverarbeitungsvorgänge, soll das Datenschutzkonzept den an der Datenverarbeitung Beteiligten auch dabei assistieren, die in § 9 BDSG i.V.m. der Anlage zum BDSG gesetzlich vorgegebenen sog. technisch-organisatorischen Maßnahmen umzusetzen und zu überwachen. Diese Maßnahmen sollen dabei helfen, die Schutzziele zu verwirklichen. Vorgeschrieben sind zunächst folgende Maßnahmen:

- zur Sicherung der Vertraulichkeit eine Kontrolle des Zutritts zu Anlagen,[63] des Zugang zu Systemen und des Zugriffs auf Daten,[64]
- zur Sicherung von Vertraulichkeit, Integrität und Transparenz der Schutz vor unbefugter Einsicht und Veränderung von Daten durch Dritte während des Transports mit Hilfe von Verschlüsselung,
- zur Sicherung der Transparenz die Gewährleistung der Prüfbarkeit, wer welches Datum in einer Datei wann eingefügt, verändert oder gelöscht hat,[65]
- zur Sicherung der Verfügbarkeit der Schutz gegen zufällige Zerstörung oder Verlust;[66]

Besonderes Augenmerk ist zudem auf das Schutzziel der Nichtverkettbarkeit zu legen,[67] welches in Nr. 8 der Anlage zu § 9 BDSG angedeutet wird. Demnach ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Die Nichtverkettbarkeit als Schutzziel erweitert diese gesetzliche Anforderung, indem personenbezogene Daten nicht oder nur mit unverhältnismä-

63 Gola/Schomerus, BDSG, § 9 Rn. 22; Ernestus, in: Simitis, BDSG, § 9 Rn. 83.

64 Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 30.

65 Federrath/Pfitzmann, DuD 2010, S. 704; Rost/Pfitzmann, DuD 2009, S. 355.

66 Bock/Meissner, DuD 2012, S. 427.

67 Rost/Pfitzmann, DuD 2009, S. 355f.

ßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet oder genutzt werden dürfen. Die Verkettung von Daten birgt eine besondere Gefahr für den Betroffenen.[68] Durch die Zuspeicherung von Daten zu bestehenden Datensätzen ergeben sich über die Aussagegehalte der Grunddatensätze hinausgehende neue Einzelangaben über Verhältnisse des Betroffenen, deren Erhebung ihn in seinem Grundrecht auf Selbstbestimmung wesentlich stärker beeinträchtigen kann als die Einzeldaten.[69] Dies gilt umso mehr im Hinblick von „Big Data"-Anwendungen, die in großem Umfang Informationen miteinander verknüpfen.[70] Daher darf eine Verkettung nur unter Beachtung der vom Gesetz vorgesehenen Bedingungen erfolgen.[71]

Um dies abzusichern, sieht das Gesetz für die praktische Umsetzung den Grundsatz der Getrenntspeicherung vor. Danach müssen Maßnahmen getroffen werden, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Der Maßstab des Erhebungszwecks rührt von dem Prinzip der Zweckbindung her, das das ganze Datenschutzrecht durchzieht. Bevor eine Datenerhebung stattfinden kann, muss ein (legitimer) Erhebungszweck festgelegt werden (§ 28 Abs. 1 Satz 2 BDSG), d.h. es muss bereits zu diesem Zeitpunkt festgelegt werden, welche Verarbeitungs- und Nutzungsschritte durchgeführt werden sollen. Fehlt ein solcher Zweck, etwa weil ein Unternehmen sich Daten aus sozialen Netzwerken nur als Vorrat sichern will, ist eine Erhebung in aller Regel rechtswidrig. Eine Zweckänderung ist nach § 28 Abs. 2 Nr. 1 BDSG zwar möglich, muss aber neu begründet werden. Eine Verkettung von Daten, die mit ursprünglich unterschiedlichen Zwecken erhoben wurden, ist daher regelmäßig nur denkbar, wenn auch die Verarbeitung der durch Verkettung neu entstandenen Daten vom Erhebungszweck gedeckt ist. Der Grundsatz der Getrenntspeicherung ist somit die technisch-organisatorische Entsprechung zum Zweckbindungsgrundsatz, die gleichzeitig die unkontrollierte Verkettung alter und damit die unkontrollierte Erhebung neuer Daten wirksam verhindern soll.

Gemäß § 3a BDSG sind Datenverarbeitungsanlagen so einzurichten, dass sie möglichst wenige personenbezogene Daten erheben (Datenvermeidung) und personenbezogene Daten nach technischer Möglichkeit nur in dem Umfang verarbeiten und nutzen, wie es nach dem Nutzungszweck notwendig ist (Datensparsamkeit). Eine Methode zur Implementierung der Datensparsamkeit, auf die § 3a Satz 2 BDSG hinweist und die in der Praxis der Business Intelligence-Analyse häufig anzutreffen ist, ist die Anonymisierung (insb. durch Aggregation) oder Pseudonymisierung. Geschäftsprozesse müssen unter dem Vorbehalt der technischen und wirtschaftlichen Verhältnismäßigkeit darauf überprüft werden, ob eine solche Anonymisierungs- oder Pseudonymisierungspraxis in Frage kommt. Wie alle Datenmanagement-Vorschriften macht die Nichtbeachtung dieser Vorschrift einen einzelnen Datenverarbeitungsvorgang nicht stets rechtswidrig, kann aber gegebenenfalls ein Indiz für die Rechtswidrigkeit sein.[72] Im Übrigen

[68] Becker/Ambrock, JA 2011, S. 561.

[69] Hansen/Meissner, Verkettung digitaler Identitäten, S. 15 ff.

[70] Schefzig, K&R 2014, S. 772.

[71] BVerfGE 65, (3).

[72] BT-Drs. 16/3657, S. 17; Bäumler, DuD 1999, S. 260; Zscherpe, in: Taeger/Gabel, BDSG, § 3a, Rn. 20 ff.

kann die verantwortliche Stelle von der zuständigen Aufsichtsbehörde zur Einhaltung der Vorschrift angehalten werden.[73]

Nicht zu den technisch-organisatorischen Maßnahmen, aber dennoch auf die Ebene des Datenmanagements gehört schließlich die Verpflichtung des SCRM-Betreibers, im Rahmen der Sicherstellung des Schutzziels der Intervenierbarkeit Geschäftsprozesse zu entwickeln, die einerseits die Einhaltung von Aufklärungspflichten gegenüber dem Betroffenen sicherstellen, andererseits die effiziente Durchsetzung von Betroffenenrechten ermöglichen. Hierbei sind die zur Herstellung der Datenverfügbarkeit und Transparenz zu unternehmenden Schritte mit denen eines effektiven Antragsmanagements zu verknüpfen. Zu beachten ist, dass eine Auskunftserteilung im Rahmen des Social CRM unentgeltlich erfolgen muss (§ 34 Abs. 8 Satz 1 BDSG). Dasselbe gilt für die Verwirklichung von Ansprüchen der Betroffenen.

Eine besondere Pflicht trifft die verantwortliche Stelle dabei nach § 42a BDSG. Danach hat sie der zuständigen Aufsichtsbehörde unverzüglich mitzuteilen, wenn bei ihr gespeicherte Daten im Sinne des § 3 Abs. 9 BDSG, Daten, die einem Berufsgeheimnis unterliegen, sowie Bankdaten unberechtigten Dritten zur Kenntnis gekommen sind (sog. Leaks).

Letzte Grundvoraussetzung für die Einrichtung eines Social CRM ist das Management der Dokumentationspflichten, die dem Schutzziel der Transparenz dienen. Hierunter fallen etwa die Führung von Verfahrensverzeichnissen (§§ 4d, 4e BDSG), die Dokumentation von Zugriffsrechten und, im Bereich der Online-Werbung entscheidend, die Protokollierung von elektronischen Einwilligungen (§§ 28 Abs. 3a BDSG, 13 Abs. 2 TMG).

Software, welche in CRM-Systemen zum Einsatz kommt, könnte vom Anwender durch bestehende Voreinstellungen oder die Art der Bedienung zu datenschutzkonformen, als auch zu datenschutzwidrigen Zwecken verwendet werden. SindDatenschutzverstöße auf Softwarefehler (Bugs) zurück zu führen, ist sicher zu stellen, dass solche Fehler schnellstmöglich (z.B. durch kontinuierliche Updates) behoben und insgesamt nahezu ausgeschlossen werden können.

Treten die Fehler im Laufe des regulären Verfahrensablaufs auf, ist zunächst zu fragen, ob die Software modular angelegt ist, so dass die Datenschutzverstöße auf eine Komponente rückführbar sind. Ist dem so, kann das Verfahren datenschutzkonform gestaltet werden, indem auf Einsatz dieser Komponente verzichtet und die Reaktivierung durch einzelne Sachbearbeiter technisch unmöglich gemacht wird. Gemäß § 9 Satz 2 BDSG sind technische und organisatorische Maßnahmen zur Aufrechterhaltung der Datensicherheit so auszugestalten, dass ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Art und Umfang der Datensicherungsmaßnahmen sind demnach auf den konkreten Einzelfall zuzuschneiden.[74] Entscheidend ist, dass die Schutzwirkung der Maßnahme einen hinreichend großen Mehrwert aufweist, der den Aufwand rechtfertigt.[75] Ob dies der Fall ist, hängt zum einen vom der Wahrscheinlichkeit und der Intensität der Bedrohung ab. Zum anderen ist die konkrete Schutz-

[73] Gola/Schomerus, BDSG, § 3a, Rn. 2.

[74] Gola/Schomerus, BDSG, § 9 Rn. 7.

[75] Vgl. Nungesser, HessDSG, § 10 Rn. 8.

bedürftigkeit der einzelnen gespeicherten Daten für die Beurteilung heranzuziehen.[76] Die Empfindlichkeit der Daten für den Betroffenen ist daher zentrales Kriterium für den Umfang der erforderlichen technischen und organisatorischen Maßnahmen.[77] Letztlich ist in Anwendung von § 9 BDSG i.V.m. der Anlage zum BDSG zu verlangen, dass die datenschutzrechtlich verantwortliche Stelle eine angemessene Sicherheitskonzeption führt, in welcher der Einsatz der Informationstechnik und die Sicherheitsmaßnahmen dokumentiert und laufend überprüft werden. Zur Dokumentation der Sicherheitsmaßnahmen zählt auch die Feststellung möglicher Gefährdungen, die von eingesetztem Personal, der Beschaffenheit von Räumen, von informationstechnischen Geräten und Programmen und bestehender Vernetzungen der Informationstechnik ausgehen. Nicht ausschließbare Gefährdungen (i.d.R. vorsätzliches Handeln des Personals) ist in einer Restrisiko-Dokumentation festzuhalten.

Bei der Bewertung der Zulässigkeit sind u.a. folgende Punkte relevant:

- Datenschutzverstöße sind im regelmäßigen Ablauf objektiv nahezu ausgeschlossen.
- Sowohl die verantwortliche Stelle als auch der Softwarehersteller haben alles Zumutbare unternommen, um Datenschutzverstöße im regelmäßigen Ablauf auch in der weiteren Nutzung auszuschließen.
- Es sind klare Verantwortlichkeiten (Geschäftsleitung, Datenschutzbeauftragter) für den Betrieb der Software festgelegt.[78]
- Der Betrieb der Software wird dauernd überwacht, Datenschutzverstöße protokolliert und gemeldet und es ist sichergestellt, dass im Falle einer unvorhergesehenen Häufung von Verstößen diese abgestellt oder die Nutzung der Software beendet werden kann.[79]
- Es findet eine effektive Eingabekontrolle (Nr. 5 der Anlage zu § 9 BDSG) statt.[80]

Die Zulässigkeit des Betriebs eines CRM-Systems ist stets eine Frage der Risikoabwägung im Einzelfall. Die o.g. Darstellung versteht sich nicht als abschließender Katalog von Zulässigkeitskriterien. Für die Frage der Missbrauchsmöglichkeiten gilt Ähnliches. Die verantwortliche Stelle hat alles Zumutbare zu unternehmen, um einen Missbrauch zu verhindern. Dies bedeutet insbesondere die Pflicht der Einrichtung einer Benutzerverwaltung mit der Blockade von Funktionen im CRM, von denen erkennbar ist, dass sie Datenschutzverstöße produzieren können. Fehlt der Software eine solche Einstellungsmöglichkeit, ist ihr Einsatz schon nach dem oben Ausgeführten nicht zulässig. Zu alledem sollte eine Schulung der Mitarbeiter über ihre datenschutzrechtlichen Verpflichtungen und den datenschutzkonformen Einsatz der Software verbunden mit der Aufstellung konkreter Verhaltensregeln kommen. Verstöße gegen die arbeitgeberseitigen Regeln zur Nutzung der Software müssen für das Personal dienstliche Konsequenzen nach sich ziehen.

---

[76] Gola/Schomerus, BDSG, § 9. Rn. 9.

[77] Ambs, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 9 BDSG Rn. 2.

[78] Kramer/Meints, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, Teil 1 6.5, Rn. 32.

[79] Vgl. Hansen, DuD 2012, S. 409.

[80] Zu den technischen Möglichkeiten Gola/Schomerus, BDSG, § 9, Rn. 26 ff.

2.2.2 Auftragsdatenverarbeitung und Auslandsbezug

2.2.2.1 Outsourcing

Es entspricht der wirtschaftlichen Notwendigkeit und der arbeitsteiligen Natur des Marktes, dass CRM-Software in aller Regel von Drittanbietern bezogen wird. Bis vor kurzem vorherrschend war die On-Site-Lösung, bei der die Software auf lokalen Rechnern des Unternehmens gespeichert und in einem Client-Server-Modell für die Abteilungen zugänglich war. Der CRM-Anbieter bot für diese Systeme meist nur Wartungsarbeiten, Updates und Support an. Solange in solchen Systemen Daten innerhalb desselben Unternehmens im Inland weitergegeben werden, ist dies datenschutzrechtlich weniger problematisch, weil keine Übermittlungen im Rechtssinne erfolgen (die Abteilungen sind untereinander nicht „Dritte"). Das Unternehmen behält als verantwortliche Stelle zu jeder Zeit die Kontrolle über die Daten.

On-Site-Lösungen sind jedoch vergleichsweise teuer, weil bei ihnen eine Lizenz der Software erworben werden muss, für den erforderlichen Speicherplatz selbst zu sorgen ist, und in der Regel noch ein gesonderter, entgeltlicher Wartungs- und Supportvertrag zu schließen ist. Im Übrigen kann eine notwendige Reparatur von der Beauftragung bis zur Durchführung zeitaufwändig sein, was nicht unbeträchtlichen entgangenen Gewinn zur Folge haben kann.

Als Alternative findet daher „Software as a Service" (SaaS) Verwendung. Nach diesem Konzept betreibt der CRM-Anbieter die gesamte Software einschließlich Datenbank und Social-Media-Komponenten auf eigenen Webservern und gewährt dem Kunden die Möglichkeit des Online-Zugriffs auf die Software selbst, sowie das Einpflegen der eigenen Daten. Da es dem CRM-Anbieter in aller Regel einfacher möglich ist, Speicherplatz in der Masse preiswert anzubieten, werden die Kosten gesenkt. Etwa notwendige Reparaturen nimmt der Anbieter an zentralen, eigenen Servern vor, so dass die Ausfallzeiten minimiert werden.

SaaS-Lösungen werden teilweise im Rahmen von Cloud Computing angeboten.[81] Nachteile ergeben sich dann daraus, dass der CRM-Betreiber oft nicht nachvollziehen kann, in welchem Staat sich der Cloud-Server befindet, der einen bestimmten Datenverarbeitungsschritt vornimmt. Dieses Wissen ist indes für die Beurteilung der datenschutzrechtlichen Zulässigkeit der Verarbeitungsvorgänge wesentlich. Ein weiterer Nachteil ist die geringere Einflussmöglichkeit auf die technischen Umstände der Datenverarbeitung. Es bedarf somit spezieller vertraglicher Vereinbarungen, um die Einhaltung datenschutzrechtlicher Vorschriften in Bezug auf Kundendaten einzuhalten.

In anderen Fallkonstellationen wird nicht nur Software bereitgestellt, sondern die Datenerhebung und -analyse vollständig von Dritten ausgeführt und dem Auftraggeber wieder zur Verfügung gestellt. Hier arbeitet der Auftragnehmer teilweise nach genauen Anweisungen des Auftraggebers.[82] Die Weisungsgebundenheit ist jedoch oftmals auch nicht gewährleistet.[83] Wieder andere Stellen, z.B. das amerikanische Unternehmen Gnip, inc., betätigen sich als sogenannte Datenbroker und liefern dem Unternehmen nach

---

[81] Grünwald/Döpkens, MMR 2011, 287; Schulz, MMR 2010, S. 78.

[82] Z.B. kann Gegenstand des Auftrages sein, die ungeschützten Facebook-Seiten aller oder bestimmter Kunden aufzufinden und nach bestimmten Gesichtspunkten auszuwerten.

[83] Heidrich/Wegener, MMR 2010, S. 806.

Auftrag historische Daten aus sozialen Netzwerken. Andere Anbieter liefern ganze, nach Kategorien wie „Reise-Enthusiast" sortierte Persönlichkeitsprofile, deren Datengrundlage aus verschiedensten Quellen stammt.[84]

2.2.2.3 Die Auftragsdatenverarbeitung

Wird die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von einem Unternehmen auf ein zweites übertragen, so liegt darin oftmals eine Auftragsdatenverarbeitung.[85] Diese ist in § 11 BDSG besonderen Voraussetzungen[86] und auch besonderen Privilegien unterworfen. Im Grundsatz ist bei einer weisungsgebundenen Datenerhebung, -verarbeitung oder -nutzung durch Dritte immer ein schriftlicher Vertrag mit bestimmten, in § 11 Abs. 2 Satz 2 BDSG genannten, Inhalten zu schließen. Die Vergabe von Aufträgen zur Datenverarbeitung, die nicht § 11 BDSG entspricht, ist gemäß § 43 Abs. 1, Nr. 2b, 1. Alt. BDSG bußgeldbewehrt.

Wesentlicher Teil der Auftragsdatenverarbeitung ist daher der Vertrag zwischen dem CRM-Nutzer (Auftraggeber) und dem von ihm ausgewählten CRM-Dienstleister (Auftragnehmer). Der schriftliche Auftragsdatenverarbeitungsvertrag muss entsprechend § 11 Abs. 2 S. 2 BDSG mindestens folgende Punkte regeln:

- Gegenstand und Dauer des Auftrags, Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, Art der Daten und der Kreis der Betroffenen;
- Verpflichtung des Auftragnehmers auf die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 Satz 1 BDSG iVm der Anlage zum BDSG;
- Auftragskontrolle, also die Kontrolle, ob Daten nur nach Weisung verarbeitet werden können (vom Prüfgegenstand ist also nicht nur die tatsächliche Verarbeitung nach Weisung zu überprüfen, sondern es sind auch Missbrauchsmöglichkeiten nach Möglichkeit auszuschließen. Abweichungen sollen sanktionsbewehrt sein, typischerweise mithilfe einer Konventionalstrafe);
- Verpflichtung des Auftragnehmers zur effektiven Durchsetzbarkeit von Betroffenenrechten,
- Einrichtung einer deutschem Recht entsprechenden Kontrolle durch den Auftragnehmer, typischerweise durch einen Datenschutzbeauftragten;
- Festlegung der Berechtigung des Auftragnehmers zum Einsatz von Subunternehmern. Es sind zwei Konstruktionen denkbar:
  a) Der Auftraggeber schließt einen eigenen Vertrag gemäß § 11 BDSG mit dem Subunternehmer, so dass die Pflichten originär auf diesen übergehen, oder

---

[84] Vgl. das Gutachten des Office of Oversight and Investigations, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Washington Dezember 2013; Federal Trade Commission: Data Brokers – A Call for Transparency and Accountability, Washington, Mai 2014.

[85] Grundlegend hierzu Gola/Schomerus, BDSG, § 11, Rn. 1 ff.

[86] Für Behörden existieren weitere gesetzliche Regelungen wie z.B. § 17 LDSG SH oder die datenschutzrechtlichen Regelungen im SGB X.

b) der Auftragnehmer wird vertraglich verpflichtet, jedem Subunternehmer seinerseits die Pflichten des § 11 BDSG aufzuerlegen, dies ist jederzeit nachweisbar zu machen;

- die Bedingungen der Nachprüfung durch den Auftraggeber und des Datenschutzbeauftragten, Duldungs- und Mitwirkungspflichten des Auftragnehmers. Wegen des Weisungsrechts muss die Befugnis zur Kontrolle der Einhaltung der Vertragspflichten in Bezug auf die CRM-Daten unbeschränkt sein;
- Verpflichtung zur Mitteilung von festgestellten Verstößen durch den Auftragnehmer (im Ergebnis eine Selbstanzeigepflicht);
- Regelung der Löschung und Herausgabe von Daten bei Vertragsende.

Außerdem gelten für den Auftragnehmer direkt das Datengeheimnis (§ 5 BDSG) sowie die Bußgeld- und Strafvorschriften hinsichtlich der o.g. genannten Pflichten (§ 11 Abs. 4 Nr. 2 BDSG), soweit Datenverarbeitung auf dem Gebiet der Bundesrepublik stattfindet.

Bei der Beurteilung der tatsächlichen Vertragsklauseln ist ein strenger Maßstab anzulegen, bei Zweifeln müssen sie als unwirksam angenommen und der Auftragnehmer als Dritter angesehen werden. Die Gewähr für die Einhaltung der Vertragsklauseln sollte der Auftragnehmer im Voraus durch Vorlage von Prüfberichten und Zertifikaten nachweisen.

Liegt kein solcher Vertrag und auch keine Einwilligung für eine Übermittlung durch den jeweils Betroffenen vor, ist auch die zugrundeliegende Maßnahme (Speicherung, Übermittlung) in aller Regel unzulässig, weil durch die Umgehung der Vorschriften ein ausreichendes Schutzniveau nicht gegeben ist und daher kein nach § 28 Abs. 2 Nr. 1 und Nr. 2 BDSG erforderliches überwiegendes Interesse bestehen kann.

Auf der anderen Seite bietet die Auftragsdatenverarbeitung jedoch auch Privilegien für die verantwortliche Stelle. Zwar enthebt die Schließung eines Auftragsdatenverarbeitungsvertrags sie nicht von der Notwendigkeit der Prüfung der Rechtmäßigkeit einzelner Maßnahmen. Jedoch bietet der Abschluss eines solchen Vertrages eine gewisse Gewähr, dass die Rechtmäßigkeit der Übertragung, soweit sie innerhalb des Europäischen Wirtschaftsraums stattfindet, jedenfalls nicht an dem zu geringen Datenschutzniveau beim Auftragnehmer scheitert.

In rechtlicher Hinsicht liegt der Mehrwert der Auftragsdatenverarbeitung aber vor allem darin, dass bei Vorliegen eines wirksamen Vertrages gemäß § 11 Abs. 2 BDSG die Weitergabe von Daten keine Übermittlung im Sinne von § 3 Abs. 4 Nr. 3a) darstellt. Eine Weitergabe der Daten an einen Auftragnehmer ist daher gegenüber dem Betroffenen nicht gesondert rechtfertigungsbedürftig. Bei ordnungsgemäßer Beauftragung ist der im EWR belegene Empfänger der Daten gemäß § 3 Abs. 8 Satz 3 BDSG nicht Dritter. Die Auftragsdatenverarbeitung enthebt den Auftraggeber trotzdem nie von der datenschutzrechtlichen Verantwortlichkeit. Er muss vielmehr seine fortbestehenden Pflichten auf den Auftragnehmer spiegeln. Der Auftragnehmer muss vor allem weisungsgebunden sein, damit der Auftraggeber seiner originären Verantwortung für die Rechtmäßigkeit der Datenverarbeitung nachkommen kann. Die Auftragsdatenverarbeitung ist abzugrenzen von der Funktionsübertragung, bei der dem Empfänger Aufgaben zur selbstverantwortlichen Erledigung mit eigenen Handlungsspielräumen übertragen werden.

2.2.2.4 Weitergabe von Daten außerhalb des EWR

Keine Privilegierung durch die Regeln der Auftragsdatenverarbeitung ist dagegen möglich, wenn der empfangende Betrieb außerhalb des Europäischen Wirtschaftsraums angesiedelt ist.[87] Obwohl also praktisch die Voraussetzungen der Auftragsdatenverarbeitung vorliegen, insbesondere die Weisungsgebundenheit, wird die Weitergabe von Daten dort als Übermittlung im Sinne des Datenschutzrechts angesehen. Auch mit Cloud-Dienstleistern, bei denen nicht klar ist, ob die Server, auf denen die konkrete Datenverarbeitung stattfinden soll, innerhalb oder außerhalb des EWR stehen, ist keine Umgehung der Übermittlungsregeln möglich.[88] Schließlich scheidet die Privilegierung noch dort aus, wo Cloud-Dienstleister sowohl Server außerhalb als auch innerhalb des EWR anbieten und eine klare Begrenzung der Speicherung eigener Daten auf den EWR nicht möglich ist.

Das Europarecht, und in Umsetzung auch das deutsche Recht, gehen davon aus, dass ein gleichmäßiger Schutz der Privatsphäre des Einzelnen nur beim Datenfluss innerhalb von EU-Staaten und von Staaten, die sich vertraglich verpflichtet haben, die Datenschutzrichtlinie umzusetzen, gewährleistet ist. Letzteres betrifft insbesondere die EFTA-Staaten Schweiz und Norwegen. Deswegen existiert das Privileg der Auftragsdatenverarbeitung für eine außerhalb dieses Europäischen Wirtschaftsraums gelegene Stelle nicht. Die rechtliche Vermutung der Unsicherheit von Drittländern begründet das grundsätzliche Verbot der Übermittlung nach § 4b Abs. 2 S. 2 BDSG, weil der Betroffene grundsätzlich ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Trotzdem ist unter den folgenden Voraussetzungen eine Übermittlung auch ins Nicht-EWG-Ausland möglich:

Grundvoraussetzung ist in jedem Fall, dass die laufenden und geplanten Datenverarbeitungsvorgänge und die Weitergabe nach den allgemeinen Vorschriften zulässig wären. Es ist daher im selben Umfang wie bei einer Weitergabe von Daten innerhalb des EWR-Raums zu prüfen, ob die beabsichtigte Maßnahme selbst durch eine Rechtsgrundlage (z.B. eine Einwilligung oder einen gesetzlichen Erlaubnistatbestand) gedeckt ist, bevor in die Prüfung der Zulässigkeit der Weitergabe außerhalb des Europäischen Wirtschaftsraums eingetreten werden kann.[89]

Im zweiten Schritt ist die Zulässigkeit der Übermittlung ins Ausland zu prüfen. § 4b Abs. 2 Satz 2 i. V. m S. 1 BDSG bestimmt, dass eine Übermittlung ins Ausland unterbleiben muss, wenn der Betroffene am Ausschluss der Übermittlung ein schutzwürdiges Interesse hat, insbesondere, wenn beim Empfänger kein angemessenes Datenschutzniveau herrscht.

Die Europäische Kommission führt eine Liste mit Staaten, in denen ein der EU vergleichbares Datenschutzniveau festgestellt wurde. Findet sich der Zielstaat auf dieser Liste, greift nach dem klaren Wortlaut von § 3 Abs. 8, 2. Hs. BDSG jedoch nicht die Privilegierung der Auftragsdatenverarbeitung. Die Aufnahme auf die Liste der Staaten mit angemessenem Datenschutzniveau ermöglicht dafür aber grundsätzlich die

---

87 Vertiefend hierzu Gola/Schomerus, BDSG, § 11, Rn. 16 ff.

88 Art. 29-Datenschutzgruppe, WP 196, S. 8 f.; AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder/AG Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, S. 14 f.

89 So auch Düsseldorfer Kreis, Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen, Beschl. v. 11./12. September 2013

Weitergabe von Daten an Auftragnehmer außerhalb der EU. Die Feststellung eines angemessenen Datenschutzniveaus ist allerdings nicht nur über die Liste der Kommission möglich, sondern kann auch durch die Prüfung all derjenigen rechtlichen Rahmenbedingungen, die nach nationalem Recht für die beauftragte Stelle selbst gelten. Sind diese geeignet, ein angemessenes Schutzniveau zu sichern, so ist eine Übermittlung jedenfalls nicht wegen §§ 4b, 4c BDSG unzulässig.

Soll eine Übermittlung in einen Staat erfolgen, für den kein der EU vergleichbares Schutzniveau festgestellt ist, bedarf es für eine Übermittlung einer Rechtfertigung nach § 4c BDSG. § 4c Abs. 1 Satz 1 Nr. 1 BDSG nennt die Einwilligung des Betroffenen als mögliche Legitimationsgrundlage. Die Wirksamkeit der Einwilligung scheitert jedoch häufig an der Freiwilligkeit der Erklärung. Zudem sind Einwilligungen frei widerruflich. Als alternativer Erlaubnistatbestand kommt die behördliche Genehmigung nach § 4c Abs. 2 S. 1 BDSG in Betracht. Danach kann die zuständige Aufsichtsbehörde „einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an *(nicht-öffentliche Stellen außerhalb des EWR)* genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben".

Ein Maßnahmenbündel kann auf diese Weise nur genehmigt werden, wenn zur Wahrung des Persönlichkeitsrechts der Betroffenen ausreichende Garantien gegeben werden. Als nicht abschließende Leitbeispiele nennt das Gesetz Vertragsklauseln und verbindliche Unternehmensregeln. Erstere stellen den Regelfall bei nichtverbundenen Unternehmen und bipolarer Weitergabe dar, letztere kommen vor allem bei Konzernen zum Einsatz.

Mit dem Begriff „Vertragsklauseln" hat der Gesetzgeber zunächst einmal die Standardvertragsklauseln der EU im Blick. Diese wurden von der Kommission zuletzt 2010 in überarbeiteter Form[90] veröffentlicht. Es bestehen unterschiedliche Gepflogenheiten bei den deutschen Aufsichtsbehörden über die Genehmigungspflicht von Datenübermittlungen auf Basis von Standardvertragsklauseln. Werden die Klauseln unverändert übernommen, gehen einige Behörden davon aus, dass keine Genehmigungspflicht besteht[91]. Eine alternative Form der Gewährleistung eines angemessenen Datenschutzniveaus nach der Datenübermittlung ins Ausland kann der Einsatz von Bindung Corporate Rules sein.[92] Dabei handelt es sich jedoch um eine konzerninterne Lösung, die nur Datenübermittlungen innerhalb eines Unternehmensverbunds betrifft.[93]

2.2.2.5 Sonderfall USA

Besonderheiten gelten für die Übermittlung in die Vereinigten Staaten, für welche ein vergleichbares Datenschutzniveau nicht besteht. Die Europäische Kommission führte deshalb in Zusammenarbeit mit der US-Wettbewerbsbehörde (Federal Trade Commission, FTC) den sogenannten Safe-Harbor-

[90] Alle bisherigen Entscheidungen der EU-Kommission zu den Standardvertragsklauseln sind abrufbar unter: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

[91] Innenministerium Baden-Württemberg, Hinweise zum BDSG für die Privatwirtschaft Nr. 40, B 2.8, RDV 2002, S. 153.

[92] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 10; Weichert, DuD 2010, S. 686.

[93] Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 43; Holtorf, MPR 2013, S. 197.

Mechanismus ein. Danach können Unternehmen mit Sitz in den Vereinigten Staaten Selbstverpflichtungserklärungen bezüglich der Einhaltung europäischer Datenschutzstandards abgeben. Durch diese Selbstzertifizierung wird rechtlich eine Weitergabe von Daten aus der EU möglich, die mit einer Weitergabe innerhalb des EWR gleichbehandelt wird. Eine Überprüfung der tatsächlichen Einhaltung der Erklärungsinhalte durch die FTC oder die Kommission findet nur sporadisch statt.

Die Konferenz der Datenschutzbeauftragten wies 2010 wegen der fehlenden Überprüfung dieser Selbstverpflichtungen jedoch darauf hin, dass die Zertifizierung eines Unternehmens nach den Safe-Harbor-Prinzipien zur Bestimmung der tatsächlichen Gewährleistung des EU-kompatiblen Datenschutzniveaus ungeeignet ist.[94] Es wurde vielmehr gefordert, dass ein Unternehmen, welches eine Weitergabe von Daten in die Vereinigten Staaten plant, sich von der tatsächlichen Einhaltung der Standards zumindest bei Vertragsschluss überzeugt. Die Einbeziehung von Standardvertragsklauseln wurde dringend empfohlen.[95] Auf der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 regierten die Aufsichtsbehörden auf die Enthüllungen von Edward Snowden und stellten in einer Entschließung fest, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.[96] Die Schutzwirkung der Safe Harbor Grundsätze ist damit derzeit nicht ausreichend, um eine Übermittlung in die USA zu legitimieren. In einem derzeit vor dem EuGH laufenden Verfahren (Rechtssache C-362/14) ist ebenfalls die Frage Gegenstand, ob die Selbstzertifizierung nach Safe Harbor eine ausreichende Grundlage für die Datenübermittlung der irischen Facebook-Niederlassung an die US-amerikanische Firmenzentrale in den USA sein kann.

2.3 Die datenschutzrechtliche Einwilligung im Rahmen des Social CRM

Das Datenschutzrecht operiert mit dem in § 4 Abs. 1 BDSG und auch § 12 Abs. 1 TMG niedergelegten Prinzip des Verbots mit Erlaubnisvorbehalt. Die Verarbeitung ist folglich grundsätzlich verboten und nur ausnahmsweise zulässig. Diese Ausnahmen können sich entweder aus dem Gesetz ergeben, oder auf einer Einwilligung basieren. Im Gegensatz zu den im Anwendungsbereich begrenzten gesetzlichen Erlaubnistatbeständen kann die Einwilligung auf eine Vielzahl denkbarer Sachverhalte angewandt werden. Im Rahmen der folgenden Darstellung ist es daher angezeigt, die Konstellationen und Bedingungen unter denen eine Datenverarbeitung aufgrund einer Einwilligung zulässig werden kann darzustellen, bevor auf die allgemeineren Rechtfertigungstatbestände eingegangen werden wird.

---

[94] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 11; Düsseldorfer Kreis, Beschluss v. 28./29.04.2010, überarbeitete Fassung v. 23.08.2010; Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Titel „Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten“, abrufbar unter http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.

[95] Düsseldorfer Kreis, Beschluss vom 28./29.04.2010 idF v. 23.08.2010, verfügbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html

[96] Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden „Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA“, abrufbar unter: https://www.datenschutz-mv.de/datenschutz/themen/beschlue/89_DSK/Ent_SafeHarbor.html

Dabei wird unterstellt, dass der Social-CRM-Betreiber die Verarbeitungsschritte entweder selbst unternimmt, oder im Wege der Auftragsdatenverarbeitung unternehmen lässt. Die Fallgruppe, dass eine Datenverarbeitung ohne strikte Weisungsgebundenheit, und damit in Form von Funktionsübertragung durch einen Dritten geschieht, und der verantwortlichen Stelle die Daten nur übermittelt werden, soll gegen Ende dieser Studie besprochen werden.

2.3.1 Rechtsnatur

Die einzelnen Aspekte der Einwilligung gemäß § 4a BDSG sind in der Literatur[97] teilweise heftig umstritten: Vorrangig ist dieser Streit an die Normen des BDSG angeknüpft, betrifft jedoch auch andere datenschutzrechtliche Vorschriften, beispielsweise solche des TMG oder des TKG. Die Regelungen des Bürgerlichen Gesetzbuches werden allerdings in weiten Teilen durch spezialgesetzliche Vorschriften verdrängt.

Anwendbar bleibt das BGB, soweit Einwilligungen Bestandteil von Allgemeinen Geschäftsbedingungen (AGB) geworden sind,[98] da AGB zwar auf einen Rechtsfolgenwillen abzielen und daher Willenserklärungen enthalten, diese jedoch nicht an den spezifisch bürgerlich-rechtlichen Willenserklärungsbegriff gebunden sind. Anwendbar sind die Wertungen des bürgerlichen Rechts ferner zum Teil, soweit das Datenschutzrecht für die Einwilligung Formvorschriften vorgibt. Wichtige Änderungen gegenüber dem BGB ergeben sich für Einwilligungen dagegen insbesondere in den folgenden Bereichen:

Für ihre Wirksamkeit kommt es anders als im bürgerlichen Recht (§ 104 ff. BGB) nicht auf die Geschäftsfähigkeit des Betroffenen an. Das Datenschutzrecht knüpft vielmehr nach ganz allgemeiner Meinung an die Einsichtsfähigkeit an.[99] Deren Beurteilung hat sich neben dem Alter des Betroffenen an der Tiefe des datenschutzrechtlichen Eingriffs, der von der Einwilligung legitimiert werden soll und der Möglichkeit des minderjährigen Betroffenen, die Folgen seiner Erklärung zu übersehen, zu orientieren.[100] So kann eine Vierzehnjährige, die an einem Preisausschreiben auf einem sozialen Netzwerk teilnimmt, eher in die Verarbeitung von für die Zusendung des Preises erforderlichen Daten einwilligen, während ein Sechzehnjähriger hinsichtlich einer umfassenden und für den Hauptzweck des Vertrages nicht erforderlichen Profilbildung zur Zusendung von Werbung als noch zu unerfahren gelten kann. Wer eine Einwilligung einholt, indem er die geschäftliche Unerfahrenheit des Betroffenen ausnutzt, begeht außerdem eine unlautere geschäftliche Handlung gemäß § 4 Nr. 2 UWG mit der Folge von Abmahnungen und Bußgeldern.

Auch die bürgerlich-rechtlichen Vorschriften zur Genehmigung, d.h. der Heilung eines an sich unwirksamen Rechtsgeschäfts durch nachträgliche Einverständniserklärung, gelten im Datenschutz nicht. Die Einwilligung muss vor Beginn des Datenverarbeitungsvorgangs vorliegen.[101] Ein Fehlen der Einwilligung zum Zeitpunkt der Erhebung macht, falls kein weiterer Rechtfertigungstatbestand in Betracht kommt, die

---

97 Walz/Simitis, in: Simitis, BDSG, § 4 m.w.N. auf das vertretene Meinungsspektrum; Helfrich, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 16.1, Rn.37 ff.

98 Scheja/Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 5, Rn. 97.

99 Simitis, in: Simitis, BDSG, § 4a, Rn. 20; Scheja/Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 5, Rn. 78..

100 Dies wird etwa ab dem vierzahnten Lebensjahr angenommen.

101 Art. 29-Datenschutzgruppe, WP 208, S. 3.

Datenverarbeitung deshalb stets rechtswidrig. Das kann erhebliche Auswirkungen auf die Erhebungspraxis in sozialen Netzwerken haben.

Auch die Lösung eines Betroffenen von einer einmal gegebenen Einwilligung wird datenschutzrechtlichen Spezialvorschriften unterstellt. So tritt an die Stelle einer Anfechtung (§§ 119 ff. BGB) der Widerspruch (§ 4a Abs. 1 Satz 1 BDSG, 28 Abs. 4, 35 Abs. 5 BDSG).

2.3.2 Anwendungsbereich

Einwilligungen im Rahmen des Social CRM sind insbesondere in folgenden Szenarien denkbar:

- bei Abschluss eines von der Einwilligung unabhängigen Vertrages, z.B. eines Kaufvertrages; Eine solche Einwilligung kann online oder offline erfolgen.
- bei Anmeldung zu einem unternehmenseigenen Forum oder vergleichbaren sozialen Medium, üblicherweise online;
- regelmäßig bei der Anmeldung zur Nutzung einer Software mit Social-Media-Elementen, z.B. einer Facebook-App;
- u.U. durch bestimmte Formen schlüssigen Verhaltens auf sozialen Medien.

Für den Betreiber des CRM irrelevant ist dagegen eine Einwilligung, die ein Betroffener gegenüber dem Betreiber einer Drittplattform abgegeben hat, des Inhalts, dass öffentlich gemachte Daten an Dritte weitergegeben werden dürfen. Ein solcher Fall kommt in der CRM-Praxis praktisch nicht vor, da die sozialen Netzwerke zwar (pseudonymisierte) Profile an Werbekunden weitergeben, nicht aber an CRM-Betreiber.

2.3.2.1 Zusendung von Werbung

Zwingend ist eine Einwilligung in den Fällen einzuholen, in denen Zweck von Erhebung oder Speicherung die Zusendung von Werbung ist. Entsprechend der in der Werberichtlinie der EU[102] enthaltenen Definition ist Werbung „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern". Diese Formel entspricht im Wesentlichen auch der Definition der kommerziellen Kommunikation in § 2 Satz 1 Nr. 5 TMG.

Der Äußerungsbegriff ist nicht im Sinne einer zweiseitigen Kommunikation zu verstehen. Es ist ausreichend, dass die Werbeansprache sich an einen unbestimmten Personenkreis richtet, etwa in der Form der Wiedergabe von Meinungen als personenbezogenes Testimonial. Zur Präzisierung zieht die Rechtsprechung[103] zudem Erwägungsgrund 7 zur Richtlinie über unlautere Geschäftspraktiken (2005/29/EG) hinzu, der die Grundlage der derzeitigen Formulierungen der werbebezogenen Wettbewerbsvorschriften im Bundesrecht darstellt. Danach ist Werbung, soweit sie nach ihrer wettbewerbsrechtlichen Lauterkeit beurteilt werden soll, wie folgt definiert: „Geschäftspraktiken, die in unmittelbarem Zusammenhang mit der

[102] Richtlinie 2006/114/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über irreführende und vergleichende Werbung, ABl. Nr. L 376 S. 21.

[103] Vgl. OLG Köln, NJOZ 2013, S. 692.

Beeinflussung der geschäftlichen Entscheidungen des Verbrauchers in Bezug auf Produkte stehen." In den Werbebegriff einzubeziehen sind demnach auch Umfragen zur Kundenzufriedenheit und Reichweitenanalysen, die einen indirekten Reputationsgewinn zur Folge haben. Diese Definition ist auch für den restlichen Datenschutz anwendbar, denn nach der Rechtsprechung gelten inzwischen viele Datenschutzverstöße auch als Verstoß gegen eine Marktverhaltensregel gemäß § 4 Nr. 11 UWG,[104] so dass eine Synchronizität der Werbebegriffe im Wettbewerbs- und Datenschutzrecht hergestellt werden muss, um Wertungswidersprüche zu vermeiden.

Entsprechend § 7 Abs. 2 Nr. 2 und 3 UWG stellt das Bewerben eines Produktes durch einen Unternehmer über Telefon, E-Mail oder Fax ohne ausdrückliche Einwilligung des Betroffenen eine wettbewerbsrechtlich unzumutbare Belästigung dar. Hier gilt das sogenannte Opt-In-Erfordernis, welches verlangt, dass eine Einwilligung durch positives Tun vor Beginn der Ansprache zwingend vorliegen muss.[105] Diese Wertung ergibt sich nicht ausdrücklich aus dem Wortlaut des § 7 UWG, ist jedoch Ergebnis einer richtlinienkonformen Auslegung[106]. Das Markieren eines Feldes wird hier ausdrücklich genannt. Es liegt dabei nahe, jedenfalls sog. Direktnachrichten auf sozialen Plattformen oder das Anzeigen auf Facebook-Chroniken durch Unternehmen diesen Tatbeständen gleichzusetzen.

Diese Wertung findet zudem auch ihre Stütze in der Sphärendogmatik des Bundesverfassungsgerichts:[107] Hiernach sind zumindest partiell dienstlich genutzte E-Mail-Konten oder Faxanschlüsse im Einzelfall der Sozialsphäre des Grundrechtsträger zuzuordnen. Bei Inhalten von Facebook-Zeitleisten hingegen oder bei Postfächern in Social Networks ist die Nutzung ausschließlich auf den freizeitgeneigten Bereich begrenzt. Dieser ist der Privatsphäre des Grundrechtsträgers zuzuordnen und damit vor unzumutbaren Belästigungen durch Werbung zu schützen. Eine Ausnahme gilt entsprechend § 7 Abs. 3 UWG für jene Fälle, in denen eine bestehende Geschäftsverbindung zum Zwecke des Cross-Selling von Produkten verwendet wird, die zu den bereits verkauften vergleichbar sind. Hier sind werbende Ansprachen per E-Mail oder per Nachricht in sozialen Netzwerken[108] erlaubt, soweit

- die E-Mail-Adresse rechtskonform erlangt wurde,
- nur Produkte derselben Art beworben werden und
- der Kunde bei Erhebung und jeder Verwendung auf sein kostenloses Widerspruchsrecht hingewiesen wurde (Opt-Out).

Das Opt-Out-Verfahren ist nach der Rechtsprechung des BGH auch ausreichend, wenn Werbung per Post auf Basis der Teilnahme an einem Kundenkartenprogramm zugesandt werden soll.[109]

---

[104] Überblick über die Rspr. bei Zech, WRP 2013, S. 1434.

[105] Ausnahmen ergeben sich ggfs., wenn innerhalb einer Vertragsbeziehung auf Neuigkeiten hingewiesen wird (s.u.).

[106] Dies folgt aus Art. 13 Abs. 3 der Richtlinie 2002/58/EG; siehe BGH, Urtl v. 10.02.2011, Az. I ZR 164/09, Entscheidungsgründe Nr. 3. a).

[107] Beispielhaft etwa BVerfGE 101, 361.

[108] Ohly, in: Ohly/Sosnitza, UWG, § 7, Rn. 65.

[109] St. Rspr., statt aller BGH, NJW 2008, S. 3055.

2.3.2.2 Sonstige werbliche Zwecke

Für die Erhebung und Verarbeitung von Daten aus sozialen Netzwerken zu Werbezwecken ist die Einholung einer Einwilligung grundsätzlich notwendig. § 28 Abs. 3 BDSG bestimmt abschließend, unter welchen Voraussetzungen Unternehmen personenbezogene Daten zu Werbezwecken verarbeiten oder nutzen dürfen, ohne hierfür eine Einwilligung einholen zu müssen. Nach § 28 Abs. 3 S. 2 BDSG ist eine Verarbeitung oder Nutzung personenbezogener Daten zu Werbezwecken zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken. Dabei darf pro „Liste" immer nur eines der Listenmerkmale der Gruppenzugehörigkeit hinzugespeichert werden.[110] Bereits diese Voraussetzung ist bei der Erhebung von Rohdaten aus sozialen Medien praktisch nie gegeben: Meist werden ganze Profile oder Aussagen erhoben, in keinem Fall findet üblicherweise eine Beschränkung auf Listendaten statt.

Gemäß § 28 Abs. 3 Satz 3 BDSG darf die verantwortliche Stelle für Zwecke nach § 28 Abs. 3 Satz 2 Nr. 1 BDSG zu den dort genannten Daten weitere Daten hinzuspeichern. Der verantwortlichen Stelle soll mit dieser Regelung ermöglicht werden, weitere Daten neben den Listendaten zum Zwecke der eigenen Werbung zu bearbeiten, um Kunden gezielter ansprechen zu können.[111] Eine Erweiterung der in § 28 Abs. 3 Satz 2 BDSG genannten Datenliste war vom Gesetzgeber dabei nicht beabsichtigt.[112] Ein Recht zur Hinzuspeicherung besteht nur dann, wenn die entsprechenden personenbezogenen Daten rechtmäßig erhoben wurden und eine weitere Verarbeitung der Daten zulässig ist. § 28 Abs. 3 Satz 3 BDSG ist dabei keine Erhebungsgrundlage, sondern setzt die rechtmäßige Erhebung der Daten voraus. Als Erhebungsgrundlage kommt § 28 Abs. 1 Satz 1 Nr. 1 BDSG in Betracht, wenn die verantwortliche Stelle die Daten im Rahmen der Kundenbeziehung erhalten hat.

Neben der Prüfung der Erhebungsgrundlage ist die Zulässigkeit des Hinzuspeicherns zusätzlich an § 28 Abs. 3 Satz 6 BDSG zu messen. Demnach ist u.a. eine Verarbeitung, und damit auch ein Speichern (§ 3 Abs. 4 Satz 1 BDSG) nach § 28 Abs. 3 Satz 2 bis 4 BDSG nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Bei den in sozialen Netzwerken eingestellten Interaktionen zwischen Nutzern im Rahmen von sog „Chats" und durch „Posts" sowie im Rahmen der individuellen Kommunikation von Beteiligten in Diskussionsforen rechnen die Betroffenen in der Regel nicht damit, dass die öffentlich gestellten Kommunikationsinhalte für Werbezwecke hinzugespeichert werden sollen. Es besteht grundsätzlich ein schutzwürdiges Interesse der Betroffenen, dass ihre Kommunikationsinhalte nicht gezielt für Werbemaßnahmen gespeichert werden. Weiterhin ist zu beachten, dass der Anwendungsbereich von § 28 Abs. 3 Satz 3 BDSG sehr begrenzt ist, indem nur Merkmale zur besseren Ansprache des Betroffenen für Werbezwecke hinzugespeichert werden dürfen.[113] Bereits die Speicherung einer Telefonnummer oder einer E-Mail-Adresse ist nur dann nach Maßgabe von § 28 Abs. 3 Satz 6 BDSG zulässig, wenn die

[110] Simitis, in: Simitis, BDSG, § 28, Rn. 233

[111] BT-Drs. 16/12011, S. 28; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 108.

[112] Gola/Schomerus, BDSG., § 28 Rn. 55.

[113] Meltzian, DB 2009, S. 2645.

Nutzung dieser Angaben nach § 7 Abs. 2 Nr. 2 UWG bzw. § 7 Abs. 2 Nr. 3 UWG i.V.m. § 7 Abs. 3 UWG statthaft ist.[114] Insbesondere eine Hinzuspeicherung von Angaben, welche als zusätzliche Gruppenmerkmale im Rahmen der Datenliste nach § 28 Abs. 3 Satz 2 BDSG angesehen werden müssten (z.B. Angaben zum Freizeitverhalten, zu Hobbys, zu käuflich erworbenen Gegenständen), ist unzulässig, da sonst eine von Gesetzgeber nicht beabsichtigte Erweiterung des Listenprivilegs erfolgen würde.[115]

Ein wichtiger Aspekt moderner Werbekonzepte ist es, gleichermaßen durch vom klassischen Marketing unabhängige Funktionen des Betriebsablaufs einen Kundenbindungseffekt zu erzielen. Für Social CRM-Tätigkeiten hat der Supportbereich hierbei besondere Relevanz: *„Service is the new marketing"* lautet ein verbreitetes Motto der Unternehmenskultur (nicht nur) auf sozialen Netzwerken.[116] Rechtlich entscheidend ist dabei die Frage, unter welchen Umständen der nicht primäre, aber wirtschaftlich immer erwünschte Werbeeffekt von Servicemaßnahmen zu einem Einwilligungserfordernis führt. Zu bedenken ist dabei nicht nur der Supportfall an sich, sondern auch die weitere Nutzung bei dieser Gelegenheit erhobener Daten.

Soweit der Support Bestandteil der ordnungsgemäßen Vertragsabwicklung bleibt (so z.B. im Falle der Nachbesserung, § 439 BGB), wird er vom BDSG privilegiert (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Wenn die Datenverarbeitung also ausschließlich Zwecken der Vertragserfüllung dient und sich auf das Erforderliche beschränkt, ist ein dabei entstehender Werbeeffekt nicht von einer Einwilligung des Kunden abhängig.

Folgende Fallgruppen mit Werbeeffekt sind insofern denkbar:

- Nach Bearbeitung einer Beschwerde in einem sozialen Netzwerk erfolgt die rechtlich geschuldete Nachbesserung. Hierbei werden lediglich die zur Nachbesserung erforderlichen Daten erhoben und gespeichert. Im Anschluss hieran beschließt das Unternehmen den Fall des Betroffenen unter Erschwerung der Bestimmbarkeit durch Dritte als erfolgreichen Supportfall zu publizieren, z.B. im Blog des Unternehmens. Hier ist eine Einwilligung auch nach Erschwerung der Bestimmbarkeit erforderlich, sofern keine Anonymisierung erfolgt ist.
- In einer zweiten Konstellation leistet das Unternehmen aus Kulanz kostenlosen Support auf Basis von Gewährleistungsansprüchen, obwohl der Betroffene hierauf keinen Anspruch hat, etwa, weil ein gekauftes Gerät erst nach Übergabe mangelhaft wurde. Dazu postet es öffentlich einsehbar in dem sozialen Netzwerk:

@Betroffener: Eigentlich wäre das kostenpflichtig, aber wir kümmern uns eben um unsere Kunden!

[114] Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Düsseldorfer Kreises, „Anwendungshinweise der Aufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke", September 2014, abrufbar unter: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Anwendungshinweise_Werbung.pdf; a.A. Gierschmann, in: Gierschmann/Säugling, BDSG, § 28, Rn. 114.

[115] Vgl. Gola/Schomerus, BDSG., § 28 Rn. 55.

[116] Burnham, wiedergegeben in Porter, Designing for the Social Web, S. 48.

Hiervon geht ebenfalls ein Werbeeffekt gegenüber Dritten aus. Zudem wird mit dem Benutzernamen des (als bestimmbar unterstellten) Betroffenen geworben. Eine Einwilligung ist somit erforderlich.[117]

- Dasselbe dürfte gelten, wenn ein bestehender Nachbesserungsanspruch übererfüllt wird, etwa durch die Draufgabe eines Gutscheins, und dies in ähnlicher Weise publiziert wird.
- Schließlich kann nach der ständigen, zutreffenden Rechtsprechung des OLG Köln auch eine Umfrage nach einem Servicefall Werbecharakter besitzen.[118] Dies ist der Fall, wenn nicht nur nach der ordnungsgemäßen Vertragsabwicklung Erkundungen eingeholt werden, sondern zusätzlich, in Form der Fragen oder neben der eigentlichen Befragung, der Service des Unternehmens bzw. dessen Streben nach Verbesserungen hervorgehoben werden. Daneben kann eine Verschleierung einer Werbeansprache durch Wahl der äußeren Form einer Umfrage nach § 4 Nr. 3 UWG wettbewerbswidrig und damit abmahnfähig sein. Dies kann nach § 16 Abs. 1 TMG ein Bußgeld nach sich ziehen.
- Selbstverständlich gibt es auch Arten von Werbung im Rahmen des Support, die noch eindeutiger sind, z.B. wenn in dem oben genannten Beispiel zum Blogeintrag der Betroffene namentlich genannt wurde, was als nicht erforderliche Speicherung eigens rechtfertigungsbedürftig wäre oder eine Dankes-E-Mail des Betroffenen im Wortlaut als „Testimonial" veröffentlicht werden sollte.

2.3.2.3 Besondere Arten personenbezogener Daten

Eine Einwilligung ist in jedem Fall notwendig bei der Verwendung besonderer Arten von personenbezogenen Daten (§ 3 Abs. 9 BDSG). Gemäß §§ 28 Abs. 6, 4a Abs. 3 BDSG dürfen solche Daten nur mit Einwilligung, die sich ausdrücklich auf sie bezieht, erhoben werden, es sei denn, der Betroffene hätte sie offenkundig öffentlich gemacht.[119] Der Begriff der offenkundigen Öffentlichmachung wird im Schrifttum so verstanden, dass sich ein positiv festzustellender Veröffentlichungswille manifestieren muss.[120] In Bezug auf soziale Medien wird dies insbesondere dann der Fall sein, wenn ein Profil für sozialpolitische Arbeit zur Unterstützung der entsprechenden Gruppe benutzt wird, da dann eine Verbreitung der Kenntnis des Umstands, dass der Betroffene einer geschützten Gruppe zugehört, offensichtlich positiv gewollt ist. Die tatsächliche Verfügbarkeit für sich allein genommen ist hingegen in keinem Fall hinreichend, um eine Einwilligung anzunehmen.

2.3.2.4 Einwilligung nach den Richtlinien von Facebook

Dass Dritte vor einer Datenerhebung in sozialen Netzwerken die Einwilligung des Betroffenen einholen müssen, findet sich in Nr. 5.7 der Nutzungsbedingungen von Facebook vom Stand 12.05.2015 wieder. Dort heißt es „Wenn du Informationen von Nutzern erfasst, dann wirst du Folgendes tun: Ihre Zustim-

[117] Je nach Ausgestaltung des Netzwerks und des vorangegangenen Kontakts zwischen Betroffenem und Unternehmen kann jedoch ggfs. eine konkludende Einwilligung angenommen werden.

[118] OLG Köln, NJOZ 2013, S. 692.

[119] Scheja/Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 5, Rn. 85.

[120] Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 171.

mung einholen, klarstellen, dass du (und nicht Facebook) ihre Informationen sammelst, und Datenschutzrichtlinien bereitstellen, in denen du erklärst, welche Informationen du sammelst und wie du diese verwenden wirst". Danach hat die verantwortliche Stelle von allen Nutzern, deren Daten sie erfasst, gleichviel ob dies „Freunde" oder Dritte sind, eine Einwilligung („consent", im Deutschen mit „Zustimmung" übersetzt) einzuholen. „Erfassung" (engl. „collection") dürfte dem Begriff der Erhebung entsprechen. Für die Eindeutigkeit (Opt-In oder Opt-Out) gelten die allgemeinen Voraussetzungen nach dem UWG. Weiter hat die verantwortliche Stelle dafür zu sorgen, den Betroffenen vor Beginn etwaiger Erhebungen sofort zu unterrichten, welche Daten über ihn zu welchem Zweck erhoben werden sollen. Durch diese Nutzungsbedingungen wird der CRM-Betreiber unmittelbar verpflichtet. Sie stellt eine Regel auf, auf deren Geltung die Betroffenen vertrauen dürfen. Mit Blick auf die Interessenabwägung im Sinne der §§ 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG folgt daraus, dass sich das Interesse der Betroffenen, von Erhebungen freizubleiben, regelmäßig durchsetzt.

2.3.2.5 Einwilligungserfordernisse nach dem TMG

Schließlich ist das Einholen einer Einwilligung erforderlich, wenn die verantwortliche Stelle Telemedien im Sinne des § 1 Abs. 1 TMG zur Verfügung stellt und außerhalb der Grenzen des TMG verarbeiten möchte. Grundsätzlich legitimiert das TMG die Verarbeitung von Bestandsdaten zu Zwecken der Begründung, inhaltlichen Ausgestaltung oder Änderung des zugrundeliegenden Vertragsverhältnisses sowie des Anbietens des Telemediums im erforderlichen Umfang, § 14 TMG. Die bei der Nutzung des Dienstes anfallenden Daten dürfen ausschließlich zu den in § 15 TMG genannten Zwecken verarbeitet werden, unter anderem soweit sie erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Eine anderweitige Verwendung der Daten, etwa zu Erstellung personenbezogener Nutzer- und Interessenprofile auf Basis des Klick- und Surfverhaltens und der darauf basierenden werblichen Ansprache bedarf der Einwilligung. Die entsprechende Verarbeitung zu Werbezwecken ist auf Basis von pseudonymen Nutzungsprofilen zulässig, sofern dem Nutzer eine Widerspruchsmöglichkeit eingeräumt wird, § 15 Abs. 3 TMG.

Der Begriff der Informations- und Telekommunikationsdienste ist im Online-Bereich weit zu fassen. So gehören hierzu zuvörderst die Einrichtung von eigenen Webseiten inkl. Foren und Chats, aber auch alle „nicht-sozialen" Formen regelmäßiger Online-Ansprache (insb. E-Mail-Newsletter). Die Unterscheidung hat insbesondere Bedeutung für die Form, in der die Einwilligung abgegeben muss, um Wirksamkeit zu entfalten. Bei der Einwilligung nach Maßgabe des BDSG ist die Abweichung von der Schriftform gesondert zu begründen (§ 4a Abs. 1 Satz 3 BDSG). Für die Einwilligung nach Maßgabe des TMG sieht das Gesetz dagegen die elektronische Einwilligung als gleichwertig an (§ 13 Abs. 2 TMG).

2.3.3 Voraussetzungen der Einwilligung

2.3.3.1 Rückwirkungsverbot

Die Einwilligung ist im Vorfeld der Verarbeitung einzuholen. Ziel ist es, eine mögliche Verweigerung durch den Betroffenen bereits bei Beginn der Datenverarbeitung zu berücksichtigen. Bei Verstößen hier-

gegen ist eine nachträgliche Heilung durch Genehmigung/Einverständnis ausgeschlossen.[121] Es wäre mit der freiwilligen Natur der Einwilligung unvereinbar, wenn es der verantwortlichen Stelle freistünde, den Betroffenen zunächst vor vollendete Tatsachen zu stellen und aus dieser Position der Stärke heraus um eine Genehmigung nachzusuchen. Dies gilt umso mehr, wenn die Daten bereits Dritten übermittelt wurden, da eine Verweigerung der Genehmigung in einem solchen Fall den Betroffenen faktisch nicht mehr schützen kann.

Relevant ist in diesem Zusammenhang eine Entscheidung des Verwaltungsgerichts Berlin[122], welche Fragen der Form und Rückwirkung von Einwilligungen aufgreift: Hiernach kann auch der Einholung einer Einwilligung selbst ein Werbeeffekt zukommen und nach § 28 Abs. 3 BDSG verboten sein. Dies gilt nach Ansicht des Gerichts für alle Fälle, in denen die verantwortliche Stelle von sich aus, etwa durch Anrufe bei Bestandskunden unter Nutzung der Stammdaten, um die Erteilung einer Einwilligung nachsucht. Das Urteil verdient im Ergebnis Zustimmung. Zum einen ist das Nachsuchen um Einwilligungserteilung der Werbeansprache unmittelbar vorgelagert, zum anderen ist es in vielen Fällen auch inhaltlich mit der Datennutzung zur Werbung gleichzusetzen. Der Betroffene wird insoweit bereits mit der scheinbaren oder tatsächlichen Attraktivität der Produkte vertraut gemacht.

Diesem Ergebnis steht auch nicht § 28 Abs. 3a BDSG entgegen. Insbesondere würde die Norm nicht ihre Bedeutung verlieren, wenn Werbung mit der Einwilligungseinholung gleichgesetzt würde. So wird nur die initiative Einholung von Einwilligungen unterbunden, nicht aber die, auch nach dem sonstigen Datenschutzrecht weitgehend unproblematischen Fälle, in denen der Betroffene von sich aus oder in Reaktion auf nicht personenbezogene Werbung tätig wird.

Weiterhin sieht § 28 Abs. 3 BDSG keine Privilegierung von Vertragsbeziehungen vor, weil der Betroffene bereits einen Kommunikationskanal eröffnet hat. Hierfür ergeben sich aus dem Gesetz keine Anhaltspunkte. Dagegen spricht zudem die Zweckbindung, welcher die erhobenen Daten unterliegen. Ein Vorrang besteht insoweit nur für die zulässig festgelegten Zwecke. Soll Werbung an den Betroffenen gehen, sollte dieser daher bereits bei Vertragsschluss eine ordnungsgemäße Einwilligung unterbreiten.

2.3.3.2 Freiwilligkeit

Die Einwilligung muss freiwillig abgegeben werden. Dies bedeutet, dass für die Einwilligung weder übermäßige Vorteile versprochen, noch Nachteile angedroht werden dürfen.[123] Für die Einwilligung in die werbliche Nutzung personenbezogener Daten beinhaltet § 28 Abs. 3b BDSG eine abgestufte Regelung.[124] Durch § 28 Abs. 3b BDSG wird ein sog. Kopplungsverbot[125] begründet, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne Einwilligung nicht oder nicht in zumutbarer

[121] OLG Köln, MDR 1992, S. 447; NJW 1993, S. 793.

[122] VG Berlin, ZD 2014, S. 540.

[123] Schapper/Dauer, RDV 1987, S. 170.

[124] Gola/Schomerus, BDSG, § 4a, Rn. 21; § 28, Rn. 46; § 28 Abs. 3a BDSG ist als Konkretisierung der wegen besonderer Umstände angemessenen Form nach § 4a Abs. 1 Satz 3 BDSG zu verstehen: vgl. BT-Drs. 16/12011, S. 31; Grentzenberg/Schreibauer/Schuppert, K&R 2009, S. 535; Spindler/Nink, in: Spindler/Schuster, § 28, Rn. 10.

[125] Zu allgemeinen Geltung vgl. Simitis, in: Simitis, BDSG, § 4a, Rn. 63; Gola/Schomerus, BDSG, § 4a, Rn. 21; Spindler/Nink, in: Spindler/Schuster, § 28, Rn. 9.

Weise möglich ist. Entsprechend darf die Hauptleistung nicht von der Abgabe der Einwilligung in die Datenverarbeitung abhängig gemacht werden. Zwar existieren auf dem Markt zahlreiche soziale Netzwerke, sodass in der Theorie gleichwertige Leistungen durch konkurrierende Dienste erbracht werden können. Die vollumfängliche Nutzung der Plattformen setzt in der Praxis jedoch voraus, dass dort viele persönlich bekannte Kontaktpersonen ebenfalls registriert sind, mit denen eine Vernetzung möglich ist. Dies ist abgesehen von einzelnen regional aktiven Diensten nur bei großen, marktmächtigen Diensten der Fall. Aus diesem Grund verfügen einige international tätige Unternehmen wie beispielsweise Facebook[126] und Google[127] über eine Monopolstellung. Eine solche ausschließliche Marktmacht schränkt die Freiwilligkeit der Nutzereinwilligungen deutlich ein.[128]

Ein Mangel an Freiwilligkeit kann im Einzelfall auch aus der eindeutigen wirtschaftlichen Überlegenheit der verantwortlichen Stelle ergeben. So mag eine Verweigerung der Einwilligung in eine umfassende Profilbildung der Online-Aktivität suggerieren, es werde in Zukunft ein schlechterer Service geboten. Daher ist die Kopplung der Hauptleistung an die datenschutzrechtliche Einwilligung nicht schon deswegen zulässig, weil es sich bei dem verfolgten Erhebungszweck nicht um Werbung handelt. Schließlich kann die Freiwilligkeit noch bei Vorliegen eines übermäßigen wirtschaftlichen Anreizes ausgeschlossen sein, welcher manipulativ auf die Entscheidungsfreiheit des Betroffenen einwirken kann.[129]

Zur Freiwilligkeit gehört auch die grundsätzliche Widerruflichkeit der Einwilligung. Dieses Gestaltungsrecht wird im BDSG nicht explizit genannt,[130] sein Bestehen wird aber allgemein angenommen. Die Widerruflichkeit wirkt ex nunc, d.h. Datenverarbeitungsmaßnahmen, die vor Zugang des Widerrufs von der Einwilligung gedeckt waren, bleiben zulässig. Der Widerruf bewirkt ein Nutzungsverbot der erhobenen Daten für die Zukunft.

2.3.3.3 Form

Die Form, in welcher die Einwilligung des Betroffenen erteilt werden muss, ist maßgeblich von der rechtlichen Grundlage abhängig, auf welcher die Datenverarbeitung erfolgt.[131] Da sich die formalen Anforderungen der Einwilligung auf Basis des BDSG maßgeblich von jenen des TMG unterscheiden, ist eine Abgrenzung dieser Gesetze zwingend erforderlich.

Das Telemedienrecht ist durch zweierlei Charakteristika geprägt: Sachlich beschäftigt es sich mit Telemedien (§ 1 Abs. 1 Satz 1 TMG). Zweitens handelt es sich um ein Anbieter-Nutzer-Verhältnis (§ 12 TMG), d.h. der Nutzer tritt selbst in ein Verhältnis mit dem Betreiber des Angebots und „nutzt" dieses bewusst. Telemedien mit Werbecharakter sind neben Webseiten insbesondere der bestellte wiederkehrende E-

[126] Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. und 9. Oktober 2014 in Hamburg, abrufbar unter https://www.datenschutz-hamburg.de/uploads/media/Entschliessung_88.DSK_Marktmacht_und_informationelle_Selbstbestimmung.pdf.

[127] Danckert/Mayer, MMR 2010, S. 219.

[128] Schaar, MMR 2001, S. 648; Thüsing/Traut, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 5, Rn. 16.

[129] Thüsing/Traut, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 5, Rn. 5/15 f.

[130] In § 13 Abs. 2 Nr. 4 TMG findet es hingegen Erwähnung.

[131] Instruktiv zu den Formerfordernissen der Einwilligung im Rahmen von Online-Geschäften vgl. Schaar, MMR 2001, S. 644 ff.

Mail-Newsletter sowie Online-Broschüren aller Art. Keine Telemedien sind unter anderem die nicht wiederkehrende Serviceleistung sowie alle Formen von Kommunikation mit dem CRM-Betreiber die nur ad hoc stattfinden, darunter auch einmalige Werbeansprachen.

Gemäß § 4a Abs. 1 Satz 3 BDSG bedarf die Einwilligung grundsätzlich der Schriftform, wobei damit die in § 126a BGB geregelte elektronische Form nicht ausgeschlossen ist (§ 126 Abs. 3 BGB)[132]. Regelmäßig bedarf sie der Unterschrift. Fax oder E-Mail genügen nicht. Nach § 126 BGB ist für die Schriftform die eigenhändige Unterschrift entscheidend, welche auf der Originalurkunde vermerkt ist[133]. Eine E-Mail oder ein Telefax erfüllen die Schriftform damit nicht. Über die bloße Schriftform im Sinne des BGB hinaus bestehen zudem besondere datenschutzrechtliche Anforderungen. So muss die Einwilligungserklärung, falls sie mit anderen Erklärungen schriftlich erteilt werden soll, drucktechnisch hervorgehoben werden (§ 28 Abs. 3a Satz 2 BDSG).

Ein Formverstoß würde in entsprechender Anwendung der §§ 125, 126 BGB die Einwilligung unwirksam machen und zur Unzulässigkeit der darauf basierenden Datenverarbeitungen führen.[134] Nur unter besonderen Umständen kann eine andere Form angemessen sein.[135] Von der Schriftform und den ihr äquivalenten Formen erlaubt § 4a Abs. 1 Satz 2 BDSG Abweichungen, soweit wegen besonderer Umstände eine andere Form angemessen ist. Weil Abweichungen von der Schriftform fast notwendigerweise mit einer erhöhten Gefährdung ihrer Schutzzwecke einhergehen, ist die Anwendbarkeit dieser Alternativen restriktiv auszulegen. Die Angemessenheit der Formabweichung ist nach den der Einhaltung der Schriftform entgegenstehenden tatsächlichen Schwierigkeiten und anhand der Erwartungen des Betroffenen im Vergleich zum Grad der Beeinträchtigung der Warn- und Beweisfunktion zu beurteilen. Im Online-Bereich, in dem die Geschäftsbeziehung zwischen dem Betroffenen und der verantwortlichen Stelle nicht auf einen schriftlich geschlossenen Vertrag über die Erbringung einer anderen Leistung zurückgeht, ist das Bedürfnis nach Alternativen zur Schriftform stark, sodass insbesondere auf die Rahmenbedingungen der Zulässigkeit von Online-Einwilligungen einzugehen ist.

Im Rahmen der Kommunikation innerhalb sozialer Netzwerke scheint es angezeigt, eine Einwilligung durch Online-Kommunikationsmittel, die nicht der Schriftform genügen, als zulässig zu bewerten. Hierunter fallen E-Mails, allerdings auch Nachrichten auf Plattformen, Messenger-Programmen und Chats soweit diese gespeichert und gegebenenfalls ausgedruckt werden können.

Die wichtigsten allgemein anerkannten „besonderen Umstände" im Sinne des § 4a Abs. 1 Satz 3 BDSG, bei denen eine Abweichung von der Schriftform möglich ist, sind der Kundenwunsch[136] und die Eilbedürftigkeit[137]. Beide sind restriktiv auszulegen: So darf eine Abweichung nicht daraus resultieren, dass etwa Druck auf den Betroffenen ausgeübt wird oder eine besonders lange Bearbeitungszeit droht. Beide Fälle sind keine Rechtfertigung dafür, die Warnfunktion der Schriftform nicht aufrechtzuerhalten.

---

[132] Roßnagel, NJW 2001, S. 1871; Simitis, in: Simitis, § 4a, Rn. 36.

[133] Simitis, in: Simitis, § 4a, Rn. 33.

[134] Gola/Schomerus, BDSG, § 4a, Rn. 29.

[135] Simitis in: Simitis, BDSG, § 4a, Rn. 43 ff. m.w.N.

[136] Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 4a, Rn. 15.

[137] Gola/Schomerus, BDSG, § 4a, Rn. 29; Simitis, in: Simitis, BDSG, § 4a, Rn. 45.

Der Grund für die Abweichung von der Schriftform ist zu belegen. Hierzu ist nicht ausreichend, dass etwa das zugrundeliegende Rechtsgeschäft (z.B. Kauf eines Buches) online stattfindet. Es gibt keine datenschutzrechtliche Regel, die besagt, dass die Einwilligung der Form eines Hauptgeschäfts folgt.

Wegen der im Vergleich zur Schriftform stark erweiterten Möglichkeit, etwa durch unrichtiges Ausfüllen des E-Mail-Headers und durch Auftreten unter einem falschen Namen seine Identität zu verschleiern oder diejenige eines Dritten anzunehmen, ist bei Rückgriff auf solche Formen die Beweisfunktion weitgehend entwertet. Der Name des Betroffenen kann außerdem auf Plattformen, die gemäß § 13 Abs. 6 TMG eine anonyme oder pseudonyme Benutzung erlauben, fehlen. Bei der Beantwortung der Frage, unter welchen Bedingungen eine solche Form dennoch zulässig ist, ist zu differenzieren: Bei Anonymität ist eine Einwilligung mangels Zuordenbarkeit des Betroffenen zu seinen Daten nicht möglich, aber auch nicht erforderlich. Die (mögliche) Verwendung eines Pseudonyms durch einen Betroffenen stellt keinen grundsätzlichen Hinderungsgrund für die Einholung einer datenschutzrechtlichen Einwilligung dar. Dennoch muss in diesem Fall in besonderem Maße sichergestellt sein, dass der Inhaber des Pseudonyms mit der Person übereinstimmt, welche die Einwilligung einholt und dass erhobene Daten tatsächlich dem Betroffenen, der die Einwilligung abgegeben hat, zuzuordnen sind. Eine Möglichkeit der Vergewisserung über die Identität des Einwilligungsgebers bietet die Abwicklung über die Funktion des sog. dienste- und kartenspezifische Kennzeichens (§ 2 Abs. 5 PAuswG), welche über den neuen Personalausweis bereitgestellt wird..

Ist die verantwortliche Stelle Diensteanbieter im Sinne des § 2 Nr. 1 TMG, etwa weil sie die Zusendung werblicher E-Mails anstrebt, gilt regelmäßig das Telemediengesetz. Im Rahmen seines Geltungsbereichs gelten Ausnahmen vom Schriftformerfordernis des BDSG:[138] Nach § 13 Abs. 2 TMG ist die Wahl der Einwilligung auf elektronischem Wege unabhängig vom Vorliegen besonderer Umstände möglich. Voraussetzung ist neben einer bewussten und eindeutigen Erklärung durch den Nutzer und dessen Aufklärung über die Freiwilligkeit der Datenverarbeitung die Protokollierung mit jederzeitiger Abrufbarkeit des Protokolls. Die Vorschrift bezieht sich nach allgemeiner Meinung[139] nicht auf die elektronische Form nach § 126a BGB mit qualifizierter Signatur, sondern nur auf die Tatsache, dass der Einwilligung keine Urkunde, sondern ein elektronisches Dokument zugrunde liegt. Diese Abweichung zu den Formvorschriften der Einwilligung nach BDSG ist aus der Natur der angebotenen Dienstleistung zu rechtfertigen. Es handelt sich also entgegen dem Wortlaut daher um eine Öffnung für die Textform.[140]

Soll eine solche Einwilligung in Werbezusendungen erteilt werden, sollte die verantwortliche Stelle das Prinzip des Double-Opt-In zur Bestätigung der Zuordnung des Betroffenen und seiner Kontaktdaten zu der Erklärung beachten. Es ist zunächst darauf zu achten, dass das Opt-In etwa auf einer Website ähnliches aktives Tun erfordert, wie es das Ankreuzen eines Feldes nebst Unterschrift auf einer Urkunde täte. Außerdem ist wie bei Schriftlichkeit darauf zu achten, dass sich die datenschutzrechtliche Einwilligung eindeutig von anderen abhebt. Sodann bestätigt die verantwortliche Stelle, wie in § 28 Abs. 3a BDSG

[138] Einzelheiten bei Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 13 TMG, Rn. 6.

[139] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 13 TMG, Rn. 6.

[140] Die Textform nach § 126b BGB erfordert eine Erklärung auf zur dauerhaften Wiederhaben in Schriftzeichen geeignete Weise. Auch der Name des Erklärenden muss enthalten sein. Im Gegensatz zur Schriftform nach § 126 BGB ist jedoch nicht die eigenhändige Unterschrift erforderlich, sodass permanente elektronische Dokumente ausreichend sind.

vorgesehen, die Einwilligung eines Kunden in schriftlicher Form. Diese Bestätigungs-E-Mail sollte eine Aufforderung an den Betroffenen enthalten, einen in der E-Mail enthaltenen Link anzuklicken, falls die Ansprache gewünscht wird. Erst mit dem Anklicken des Bestätigungslinks gilt die Einwilligung als erteilt. Der Vorgang ist durch Protokollierung von E-Mail, Datum und Uhrzeit sowie des Namens des Betroffenen zu dokumentieren. Bestreitet der Betroffene, eine Einwilligung gegeben zu haben, so trifft ihn diesbezüglich die Darlegungs- und Beweispflicht. Das Double-Opt-In-Verfahren ist jedoch ungeeignet, wenn eine Einwilligung in Zusendung von Werbung über Telefon nachgesucht wird, da hier die vorliegende E-Mail-Adresse keinen Nachweis über den (angeblichen) Inhaber des Telefonanschlusses zu geben vermag. Hier muss sich die verantwortliche Stelle in der Regel durch Wahl der Schriftform davon überzeugen, dass der Anschlussinhaber mit der Person übereinstimmt, die die Einwilligung erteilt hat.[141]

2.3.3.4 Eindeutigkeit und Bestimmtheit

Dicht verknüpft mit der Frage, in welcher Form eine Einwilligung abzugeben ist, ist insbesondere im Servicebereich des SCRM die Frage, welche Anforderungen an die Eindeutigkeit und Bestimmtheit der Einwilligung des Betroffenen zu stellen sind. Genügt bereits eine bloße Äußerung eines Kundenwunsches in einem sozialen Medium? Ist es grundsätzlich möglich, einem solchen Handeln einen Erklärungswert im Sinne einer Einwilligungserklärung beizumessen?

Das Erfordernis der Eindeutigkeit und Bestimmtheit für die Wirksamkeit von Einwilligungserklärungen ergibt sich nicht direkt aus dem Wortlaut des BDSG, wohl aber aus Art. 7 lit. a) der Richtlinie 95/46/EG und allgemein aus der Natur der Einwilligung als Rechtsgrundlage für einen Eingriff in das Persönlichkeitsrecht. Demnach ist eine Einwilligungserklärung nur dann wirksam, wenn diese zweifelsfrei eine Bereitschaft zur Verarbeitung eigener Daten enthält (Eindeutigkeit) und die Reichweite bzw. der Umfang der Erklärung konkret feststellbar ist (Bestimmtheit). Angewandt auf den Bereich der innerhalb sozialer Netzwerke getätigten Äußerungen durch Kunden bedeutet dies Folgendes:

Das Erfordernis einer vorherigen ausdrücklichen Einwilligungserklärung gilt gemäß § 7 Abs. 2 Nr. 3 UWG für Werbung unter Verwendung einer automatischen Anrufmaschine, eines Faxgeräts oder elektronischer Post. Für Werbesendungen per Post bleibt die Frage offen, ob konkludente Einwilligungserklärungen ausreichend wären.

Zwar kommt Schweigen als solchem kein Erklärungswert zu. Nach allgemeinen zivilrechtlichen Wertungen (z.B. § 133 BGB) kann eine Erklärung (auch eine solche in Textform) neben ihrem Wortlaut aber auch auf einen nicht ausdrücklich ausgesprochenen Willen schließen lassen. Die Frage, ob solche sog. konkludenten Erklärungen als Einwilligungserklärung tauglich sind, ist im Schrifttum umstritten, wird für das BDSG von der herrschenden Meinung jedoch grundsätzlich bejaht[142]. Der herrschenden Ansicht ist zuzustimmen. Weder Bundesrecht (§ 4a BDSG) noch die Richtlinie (Art. 7 a)) verlangen, dass eine Einwilligung ausdrücklich erfolgt. Vielmehr bestimmt die Richtlinie a.a.O. nur, dass eine Einwilligung „ohne jeden Zweifel" (englisch „unambiguously", französisch „indubitablement") erteilt worden sein muss. Das Tele-

[141] So: BGH, NJW 2011, S. 2657.

[142] Däubler, in Däubler/Klebe/Wedde/Weichert, § 4a, Rn. 16; Drewes/Siegert, RDV 2006, S. 139; a.A. Simitis, in: Simitis, § 4a, Rn. 44.

mediengesetz spricht in § 13 Abs. 2 Nr. 1 von Bewusstsein und Eindeutigkeit, für das Vorliegen beider Tatbestandsmerkmale ist die verantwortliche Stelle dokumentationspflichtig.

Neben der Feststellung, dass Einwilligungserklärungen im Rahmen von § 7 Abs. 2 Nr. 3 UWG stets ausdrücklich und entsprechende Erklärungen nach § 4a Abs. 1 BDSG auch konkludent erfolgen können, bleibt fraglich, ob allgemeine Regeln dafür aufgestellt werden können, wann Einwilligungen bestimmt genug sind. Wegen der unvermeidlichen semantischen Unbestimmtheit von Rechtsbegriffen wie „ohne jeden Zweifel" und „ausdrücklich" ist eine Abgrenzung für jeden Fall nicht möglich. Dennoch lassen sich Fallgruppen bilden, und Wertungshinweise für weitere, im Social CRM häufig vorkommende Fallkonstellationen geben.

Die Frage nach der Eindeutigkeit bzw. Bestimmtheit von Einwilligungserklärungen stellt sich besonders häufig im Service-Segment des Social Media Managements. Die Grundkonstellation besteht darin, dass ein Kunde in einem sozialen Netzwerk eine Leistung oder einen Rat wünscht, das Herstellerunternehmen im Rahmen des Social Media Monitorings das Posting abfängt und dem Kunden gerne abhelfen möchte. Hierbei stellt sich regelmäßig die Frage, ob in der Beschwerde des Kunden eine Einwilligung zur Weiterverarbeitung der Kundendaten auch im Falle eines Werbeeffekts liegt.

Dabei ist der grundsätzliche Vorrang der gesetzlichen Erlaubnistatbestände zu beachten. Bei einer Serviceleistung, von der kein Werbeeffekt ausgeht, bei welcher der Betroffene eine werbefreie Serviceantwort des Unternehmens erwartet und auch erhält, wird er bezüglich einer Erhebung, Verarbeitung und Nutzung seiner Anfrage und Kontaktdaten keine Einwände haben. Als Legitimationsgrundlage kommt § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Es ist daher in solchen Fällen unnötig, eine Einwilligung zu konstruieren.

Serviceleistungen mit Werbeeffekt sind anders zu beurteilen. Ausdrücklich ist eine Einwilligungserklärung, wenn der Betroffene die verantwortliche Stelle direkt zu einer Handlung auffordert, die eine Datenverarbeitung erfordert und sichergestellt ist, dass dem Betroffenen die Notwendigkeit und Natur dieses Datenverarbeitungsvorgangs bewusst ist[143]. Eine direkte Ansprache in dieser Form liegt dann vor, wenn der Betroffene die spezifische Funktion des sozialen Mediums, die für direkte Ansprachen unter Nutzern üblich ist, wählt. Bei Twitter ist das z.B. der Benutzername der verantwortlichen Stelle mit vorgeschaltetem @-Zeichen und Ansprache-Floskel oder Doppelpunkt. Für die Eindeutigkeit dürfte es genügen, wenn eine Auslegung aus Sicht eines vernünftigen Empfängers ergibt, dass eine bestimmte Maßnahme erwünscht ist. Dies soll durch folgende Beispiele illustriert werden:

Beispiel 1: Ein mit seinem Klarnamen bei Twitter registrierter User schreibt Folgendes:

„Hallo @unternehmen, (bzw. „@unternehmen:") bitte mailt mir mal eure Broschüre „Unternehmen X – Einzigartige Vorteile zu kleinem Preis" zu!

Diese Aufforderung löst den Tatbestand von § 7 Abs. 2 Nr. 3 UWG aus. Es ist demnach eine ausdrückliche Einwilligung erforderlich. Aus ihr würde sich, das Vorhandensein der weiteren Voraussetzungen unterstellt, für das Unternehmens die Erlaubnis ergeben, den angegebenen Namen mit der Kundendatenbank

[143] Vgl. Simitis, in: Simitis, § 4a, Rn. 77 ff.

abzugleichen und die gewünschte Broschüre, auch wenn sie offensichtlich werbenden Inhalt hat, per E-Mail zu übersenden.

Vergleichbares gilt, wenn eine solche Äußerung in einem Serviceforum des Unternehmens erfolgen würde. Das Posting eines Problems auf einer solchen Seite mit der Bitte um Lösung kann im Regelfall als Einwilligung in die zur Zusendung der Broschüre erforderliche Datenverarbeitung zu verstehen sein.

Anders zu behandeln sind „in den Raum gerufene" Probleme auf sozialen Medien. Es handelt sich hierbei um ein für Twitter und Twitter ähnliche Plattformen typisches Phänomen. Beispiel: Ein Twitter-Nutzer postet Folgendes:

„Mist, meine Kamera von #Unternehmen spiegelt immer das Bild um 180°!"

Hier ist das Unternehmen ausdrücklich genannt, begleitet von der Auszeichnungs-Raute (Hashtag), die andeutet, dass das Posting gefunden werden sollte. Allerdings enthält es keinerlei Handlungsanweisung, eine Einwilligung ist hier schon mangels Eindeutigkeit nicht gegeben. Es handelt sich daher nicht einmal um eine eindeutige Erklärung. Ein anderer Nutzer mag Folgendes gepostet haben:

„Mein Kochgeschirr von #Unternehmen zerspringt bei über 220°C! Kann mir jemand hitzebeständigeres Geschirr leihen?"

Dies ist zwar eine Handlungsanweisung, aber sie bezieht sich nicht notwendig auf einen datenschutzrechtlich rechtfertigungsbedürftigen Vorgang. Schreibt der Nutzer aber etwa

„Ich hätte ja gerne gewusst, warum mein Flug gestrichen wurde, aber #Fluglinie kümmert sich ja nicht um mich."

kann trotz der negativen Formulierung hierin nach den Umständen durchaus mit hinreichender Bestimmtheit die Zustimmung zur Eruierung des vom Nutzer gebuchten Fluges liegen. Sie ist jedoch nicht ausdrücklich, so dass eine Serviceleistung mit Werbeeffekt auf der Plattform selbst nicht zulässig wäre. Das Recht der Fluggesellschaft am eingerichteten und ausgeübten Gewerbebetrieb erlaubt ihr jedoch, sich gegen die Unterstellung zu wehren.[144]

Eine weitere Fallgruppe findet sich meist auf freundschaftsbasierten Plattformen wie Facebook. Es handelt sich um diejenigen Fälle, in denen das Unternehmen (etwa weil die User „Fans" des Unternehmens sind) Postings auf Seiten von Kunden einsehen kann, die das Unternehmen benennen, die aber ersichtlich an Freunde gerichtet sind. Beispiel:

„Rolf Bauer, hast du nicht auch die Kamera 438X von der Firma U? Meine ist schon wieder zur Reparatur, das dauert jetzt schon einen Monat, wo die wohl bleibt?"

Selbst wenn sich hieraus ein Wunsch nach Aufklärung ergibt, ist es klar, dass der Betroffene nicht damit rechnet, dass das Unternehmen ungefragt die Verarbeitungsschritte unternimmt, die für die Aufklärung der Frage notwendig sind, vielmehr ist ausschließliches Ziel der Frage, die Meinung von Herrn Bauer einzuholen. Bei Zweifeln ist es in der Kundenbeziehung daher ratsam, für potentiell (auch) werbende Nachrichten eine ausdrückliche Einwilligung einzuholen.

---

[144] Allg. Spindler, in: Bamberger/Roth, § 823 BGB, Rn. 105, 120 ff., 129 ff.; Spindler/Volkmann, in: Spindler/Schuster, Recht der elektronischen Medien, § 1004 BGB, Rn. 7.

2.3.3.5 Vorherige Aufklärung

Europarecht und Bundesrecht gehen von dem Prinzip des allseitig informierten Betroffenen aus. Deswegen ist die Aufklärung vor Beginn des Datenverarbeitungsvorgangs ein entscheidendes Mittel zur Durchsetzung des datenschutzrechtlichen Transparenzgebotes. Der Betroffene ist auf sämtliche Daten, auf die sich seine Einwilligung bezieht, den Zweck der Datenverarbeitung sowie gegebenenfalls auf den Zweck und die Empfänger einer vorgesehenen Datenübermittlung hinzuweisen.[145] Unklarheiten gehen zu Lasten der verantwortlichen Stelle.[146] Eine Blankoeinwilligung ist unwirksam.[147]

Weiterhin muss, unabhängig davon, ob die Daten unter Mitwirkung des Betroffenen (§ 4 Abs. 2 BDSG) oder ohne seine Mitwirkung erhoben werden, über die Identität der verantwortlichen Stelle und überraschende Empfängerkategorien aufgeklärt werden (§§ 4 Abs. 3, 33 Abs. 1 S. 1 BDSG). Nur mit deren vollständiger Nennung ist es dem Betroffenen möglich, seine Rechte wirksam auszuüben. Wird ein Telemedium angeboten, so gelten die extensiveren Aufklärungspflichten nach § 13 TMG[148], die durch einen deutlichen Hinweis dem Betroffenen bekannt gegeben und während der Nutzung des Telemediums jederzeit unmittelbar abrufbar bleiben müssen.

Sämtliche Aufklärungspflichten mit Ausnahme der Belehrung über die Betroffenenrechte müssen bei Beginn der Datenverarbeitung erfüllt werden (§ 13 TMG), damit der Betroffene die Entscheidung über die Preisgabe seiner Daten in Kenntnis aller möglichen Risiken treffen kann. Die Pflicht kann insbesondere nicht durch die Vermutung ersetzt werden, die entsprechenden Informationen lägen beim Betroffenen schon vor.[149]

Solange die Einwilligung bei Unterzeichnung eines schriftlichen Vertrages erteilt wird, ist der Nachweis der Erfüllung der Informationspflichten unproblematisch möglich. Schwieriger wird die rechtliche Bewertung dann, wenn durch den Betroffenen eine ausreichend bestimmte Serviceanfrage gestellt wird, die, wie die Broschürenzusendung, notwendig eine Datenverarbeitung mit Werbecharakter voraussetzt. Bereits das gezielte Auffinden des betreffenden Postings stellt als Beschaffung von personenbezogenen Daten eine Erhebung dar. Vor dieser Erhebung wird regelmäßig keine Möglichkeit der Erfüllung der Transparenzpflichten bestehen. In der Folge ist die Einwilligungserklärung in derartigen Fällen regelmäßig unwirksam. Mangels Sichtbarkeit genügt es nicht, die Aufklärungspflichten etwa in das Profil der verantwortlichen Stelle einzubinden.

Um eine hinreichende Sichtbarkeit zu erzielen und den Anforderungen an die Erfüllung der Hinweispflichten zu genügen, bietet sich daher folgendes praktisches Vorgehen an. Zunächst sollten, wie bereits erklärt, die Fälle der Online-Einwilligung möglichst begrenzt werden. Alle Fälle, die nicht notwendig eine Einwilligung zur Datenverarbeitung erfordern, müssen basierend auf anderen Erlaubnistatbeständen gelöst werden. Dies betrifft die meisten Verarbeitungsvorgänge, die zu nichtwerblichen Zwecken durch-

---

[145] Frantzen, in: Müller-Glöge/Preis/Schmidt, Erfurter Kommentar zum Arbeitsrecht, § 4a BDSG, Rn. 2.

[146] Gola/Schomerus, BDSG, § 4a, Rn. 26

[147] Simitis, in: Simitis, BDSG, § 4a, Rn. 77; Wohlgemuth/Gerloff, Datenschutzrecht, Rn. 192.

[148] Für Telemedien s.a. § 13 Abs. 7 TMG.

[149] Däubler, in: Däubler/Klebe/Wedde/Weichert, § 33 Rn. 25; a.A. Gola/Schomerus, § 33, Rn. 29.

geführt werden. Ferner sollte nach Möglichkeit der Werbeeffekt der Servicemaßnahmen auf ein Minimum reduziert werden, z.B. sollte zunächst kein Cross-Selling-Versuch unternommen werden.

Ist die geplante Ansprache ohne Werbeeffekt nicht möglich (etwa im Broschüren-Fall), dann dürfte es rechtlich jedoch zulässig sein, dass die verantwortliche Stelle die Nachricht zunächst mit dem Speicherungszweck der Einwilligungseinholung speichert, dem Betroffenen allerdings durch einen freigegebenen Kommunikationskanal die notwendige Aufklärung zuteilwird, und ihm gleichzeitig anheimgestellt wird, die Einwilligung zu bestätigen oder zurückzuweisen. Bis zu diesem Zeitpunkt wäre die ursprüngliche Einwilligung unwirksam. Eine schwebende Unwirksamkeit käme nach dem oben zur Nachgenehmigung Ausgeführten ebenfalls nicht in Betracht. An der Datennutzung durch Rückfrage an den Betroffenen hätte die verantwortliche Stelle im Rahmen des geäußerten Wunsches jedoch ein berechtigtes Interesse gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Diesem stünden zudem auch zumeist keine überwiegenden Gegeninteressen des Betroffenen gegenüber, weil (außer in Fällen des, nicht zu vermutenden, Identitätsdiebstahls) die Initiative von dem Betroffenen selbst ausgegangen wäre.

Einer solchen Wertung steht auch die Rechtsprechung des VG Berlin[150] nicht entgegen: Zwar hat dieses entschieden, dass die Bitte um Einwilligung in Werbezusendungen selbst unter den Werbebegriff fallen kann. Diese Wertung kann jedoch nicht auf jene Fälle übertragen werden, in denen die ursprüngliche Initiative von dem Betroffenen ausgegangen ist.

Demnach wäre die Abänderung des Nutzungszweckes auf die Zusendung von Werbung gemäß § 28 Abs. 2 Nr. 1 i.V.m. Abs. 1 Satz 1 Nr. 2 BDSG zulässig, soweit tatsächlich eine eindeutige und bestimmte Ansprache stattgefunden hat.

2.3.3.6 Einbindung in AGB

Fraglich ist schließlich, welche Voraussetzungen erfüllt sein müssen, damit die Einwilligung in Datenerhebungen im Rahmen des Social CRM wirksam Teil von Allgemeinen Geschäftsbedingungen in Verbraucherverträgen werden kann. Prüfungsmaßstab bilden hierbei die allgemeinen Regelungen der §§ 305 ff BGB.

Zunächst ist wegen ihrer Beschränkung auf Fälle der Abweichung von gesetzlichen Vorschriften durch AGB (§ 307 Abs. 3 BGB) und ihres damit gegenüber § 305c BGB engeren Anwendungsbereichs zu prüfen, ob tatsächlich AGB vorliegen (§§ 305 ff. BGB). Bei einem Großteil der datenschutzrechtlichen Vorschriften handelt es sich um zwingendes Recht. Dies gilt insbesondere für Vorschriften, die Gegenstand expliziter Verbotsnormen sind, wie das Verbot auf vertragliche Abbedingung der gesetzlichen Betroffenenrechte in § 6 Abs. 1 BDSG. Nach Ansicht der Literatur ist jede von der gesetzlich zwingenden Norm abweichende Regelung im Rahmen von Allgemeinen Geschäftsbedingungen unwirksam (arg. § 134 BGB).[151] Dementsprechend käme es auf eine Inhaltskontrolle nach § 307 BGB schon gar nicht mehr an. Nach Ansicht der

[150] VG Berlin, AfP 2014, 476 ff.

[151] Die Abweichung von zwingendem Recht ist bereits ohne den Umweg über § 134 BGB oder § 307 BGB nichtig, weil den Parteien im Bereich zwingenden Rechts von vornherein die Dispositionsbefugnis fehlt, vgl. Hinrichs, in: Palandt, BGB, § 134 BGB, Rn. 5.

Rechtsprechung[152] hingegen ist der Rechtsgedanke der §§ 307 ff BGB und die hieran geknüpfte Inhalts- und Klauselkontrolle auch im Falle der AGB-rechtlichen Regelung zwingender Normen anzuwenden. Konsequenz der Rechtsprechung ist, dass auch im Falle der zwingenden Normen des BDSG eine Inhalts- und Klauselkontrolle gem. der §§ 307 ff BGB durchzuführen ist, sofern Allgemeine Geschäftsbedingungen z.B. von der zwingenden Norm der Einwilligung abweichende Regelungen enthalten. Diese Wertung überzeugt. Schutzzweck der AGB-Regelungen ist es, die Position des Verbrauchers gegenüber dem Verwender zu stärken und einen Machtausgleich zwischen Unternehmer und Privatperson zu sichern. Werden Einwilligungserklärungen einseitig durch ein Social CRM-Unternehmen gestellt, so erwächst für den Betroffenen, dessen Daten verarbeitet werden, ein solches Schutzbedürfnis.

Weiterhin erfüllt die Anwendung des Kataloges der §§ 305 ff BGB auf gesetzlich zwingende Normen zudem auch rechtswegwahrende Funktionen: Nach § 1 UKlG kann derjenige, welcher in Allgemeinen Geschäftsbedingungen Bestimmungen, die nach den §§ 307 bis 309 des Bürgerlichen Gesetzbuchs unwirksam sind, verwendet oder für den rechtsgeschäftlichen Verkehr empfiehlt, auf Unterlassung und im Fall des Empfehlens auch auf Widerruf in Anspruch genommen werden. Klageberechtigt sind nach § 3 UKlaG „qualifizierten Einrichtungen", insbesondere Verbraucherschutzverbände. Um ein Leerlaufen dieser passivlegitimierenden Norm zu verhindern, ist es praktikabel auch gesetzlich zwingende Normen dem AGB-rechtlichen Klauselprüfungsverfahren zu unterstellen.

Wendet man – der Rechtsprechend folgend – den Katalog der §§ 305 ff BGB auf Einwilligungen an, welche im Rahmen von Social CRM-Vorgänge erteilt werden sollen, gilt es folgende Problempunkte zu beachten:

2.3.3.6.1 Klauselverbote

Es wird zunächst auf die konkreten Klauselverbote (§§ 308 ff. BGB) eingegangen. Relevant sind insbesondere Verstöße gegen § 308 Nr. 5 BGB, der die Fingierung von Erklärungen, d.h. deren Ersetzung durch die Ausführung einer gewissen, mit der Erklärung unzusammenhängenden Handlung verbietet.

So wäre die folgende Klausel unwirksam:

„App-Hersteller A-GmbH erhält das Recht, Profile und Freundeslisten des Facebook-Nutzers zum Zwecke der Werbung zu erheben. Die Einwilligung hierzu gilt mit der erstmaligen Inbetriebnahme der App als erteilt."

§ 309 Nr. 12 a) BGB verbietet die Überwälzung der Beweislast für das Bestehen oder Nichtbestehen eines Rechtsverhältnisses auf den Betroffenen. So darf ihm insbesondere die Darlegung und der Beweis für das Nichtbestehen einer Einwilligung nicht auferlegt werden. Dies gilt für Einwilligungen aller Art, also für Erhebung, Verarbeitung, Nutzung und Übermittlung einschließlich der stillschweigenden Einschaltung von Auftragsdatenverarbeitern und der Übermittlung ins Ausland.

Schließlich ist gegebenenfalls noch § 309 Nr. 13 BGB einschlägig. Danach darf eine Erklärung des Betroffenen nicht an strengere Formerfordernisse als die Schriftform gebunden werden. Es wäre beispiels-

[152] St. Rspr., vgl. BGH, NJW 2008, S. 3055; NJW 2010, S. 864.

weise unzulässig, für einen späteren Widerspruch gegen die Verarbeitung zu Werbezwecken (§ 28 Abs. 4 BDSG) zu fordern, dass dieser ausschließlich per Post oder per Fax erfolgen könne.

2.3.3.6.2 Unangemessene Benachteiligung

§ 307 Abs. 1 S. 1 BGB erklärt Klauseln in Allgemeinen Geschäftsbedingungen für unwirksam, wenn durch deren Inhalt von Rechtsvorschriften abgewichen wird und der Betroffene hierdurch unangemessen benachteiligt wird.

Der Gesetzgeber erwähnt in § 307 Abs. 2 BGB zwei Hauptfälle, bei denen eine solche Benachteiligung vermutet wird. Von erhöhter Relevanz für den Bereich des E-Commerce ist § 307 Abs. 2 Nr. 1 BGB. Danach ist eine Benachteiligung im Zweifel dann anzunehmen, wenn eine Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist. Es entspricht allgemeiner Praxis, dass in Fällen zwingenden Rechts die bloße Abweichung vom Gesetzeswortlaut bei inhaltlicher Übereinstimmung (sog. „deklaratorische Klausel") in AGB für die Wirksamkeit unschädlich ist. Gleiches gilt, wenn sich die verantwortliche Stelle freiwillig einem höheren, als dem gesetzlich geforderten Datenschutzniveau unterwirft. Ein solches „Mehr" an Datenschutz ist AGB-rechtlich stets wirksam, da die AGB-Kontrolle lediglich Benachteiligungssituationen des Betroffenen verhindern will. Im Umkehrschluss sind solche Klauseln gem. § 307 BGB unwirksam, welche eine Absenkung des gesetzlich vorgesehenen Datenschutzniveaus bezwecken. Wird eine Einwilligung im Social CRM erteilt, so sind zahlreiche Konstellationen denkbar, aus denen sich deren Unwirksamkeit aufgrund unangemessener Benachteiligung des Betroffenen ergeben kann: Wie bereits dargestellt enthält eine AGB-Klausel im Zweifel eine „unangemessene Benachteiligung" des Kunden, wenn sie von einer gesetzlichen Regelung abweicht und gleichzeitig „mit wesentlichen Grundgedanken" dieser gesetzlichen Regelung nicht zu vereinbaren ist (§ 307 Abs. 2 Nr. 1 BGB). Der Wortlaut dieser Formulierung lässt sich auf den in der BGH-Rspr. anerkannten Grundsatz anknüpfen, nach dem AGB-Klauseln unwirksam sind, wenn durch ihren Inhalt das Leitbild abgeändert wird, das für den gewählten Vertragstyp in dispositiven Vorschriften niedergelegt ist.[153]

Eine wirksame Einwilligung muss eindeutig, bestimmbar, freiwillig abgegeben worden sein, durch Schriftform ihrer Warn- und Beweisfunktion gerecht werden und durch eine transparente Gestaltung eine effektive Sicherung der Betroffenenrechte ermöglichen. Wesentliche Datenschutzprinzipien wie beispielsweise das Prinzip des Verbots mit Erlaubnisvorbehalt, die Erhebung beim Betroffenen, der Zweckbindungs- sowie der Erforderlichkeitsgrundsatz werden durch die Einwilligungsvorschriften des BDSG aufgegriffen und bestimmen somit das Leitbild, welches der Wertung des § 307 BGB zugrunde zu legen ist.

Abweichungen vom Wortlaut der Datenschutzgesetze sind daher danach zu beurteilen, ob sie diese Grundsätze verwirklichen. Unzulässig wäre in vielen Fällen etwa eine Klausel, mit der sich eine verantwortliche Stelle pauschal das Recht einräumen lässt, für spätere Zeiten und unbemerkt Erhebungen aller Art vornehmen zu dürfen. Beispiel:

„Die U-AG wird ermächtigt, regelmäßig die Kundendaten durch Abgleich mit Online-Daten aus öffentlichen Quellen zu überprüfen, um Änderungen rechtzeitig festzustellen."

[153] Wurmnest, in: Münchener Kommentar, BGB, § 307 BGB, Rn. 65 m.w.N.

Eine solche Klausel verstößt jedenfalls dann gegen den Direkterhebungsgrundsatz (§ 4 Abs. 2 BDSG), wenn durch sie auch solche Daten erhoben werden, die ohne unverhältnismäßigen Aufwand auch beim Betroffenen selbst (d.h. mit dessen Kenntnis von einzelnen Erhebungsvorgängen und seiner Mitwirkung) zu erheben wären. Es empfiehlt sich stets eine Eingrenzung nach der Art der zu erhebenden Daten vorzunehmen.

Ebenfalls unzulässig sind Fiktionen von Erklärungen, zu deren Abgabe die verantwortliche Stelle verpflichtet ist. So ist es mit § 4 Abs. 1 S. 2 BDSG nicht vereinbar, die zwingend vor der Einwilligung durchzuführende Belehrung zu fingieren. Dasselbe gilt für die Fiktion einer rechtlich gebotenen Aufklärung des Betroffenen (§ 4 Abs. 3, 33 BDSG). Auch die Einräumung eines Rechts zur Einholung einer nachträglichen Genehmigung ist mit § 4 Abs. 1 2. Hs. BDSG nicht vereinbar.

Zwar ist ein rechtsgeschäftlicher Verzicht auf Betroffenenrechte nach § 6 Abs. 1 BDSG bereits durch explizite Verbotsnorm ausgeschlossen und daher ohne weiteres nach § 134 BGB unwirksam, allerdings kann eine solche Unwirksamkeit subsidiär auch aus § 307 Abs. 2 S. 1 BGB folgen. Dasselbe gilt für einen Verzicht auf Schadensersatz (§ 7 BDSG), dessen Unabdingbarkeit zwar nicht aus dem Gesetz hervorgeht, der aber ebenfalls zum zwingenden Recht gehört.

Auch eine Vereinbarung, dass Daten für beliebige Zwecke erhoben werden können, kann wegen Verstoßes gegen den in § 28 Abs. 1 S. 2 BDSG niedergelegten Zweckbindungsgrundsatz kein wirksamer Bestandteil von Allgemeinen Geschäftsbedingungen sein. Beispiel:

„Die U-AG wertet die auf unserem Forum von Ihnen geposteten Beiträge zu eigenen Geschäftszwecken aus."

Die o.g. Klausel wiederholt zwar den Gesetzeswortlaut, da „Geschäftszwecke" aber bereits nach § 28 BDSG sowohl interne als auch Werbezwecke umfassen können, ist der Zweck unzureichend festgelegt.

2.3.3.6.3 Überraschende Klauseln

Schließlich ist zu prüfen, ob es sich bei der Bedingung um eine überraschende Klausel handelt. Gemäß § 1 UKlaG kann diese Vorschrift jedoch nicht von Verbänden, sondern ausschließlich vom Betroffenen selbst geltend gemacht werden. Nach § 305c BGB ist eine überraschende Klausel von zwei Elementen gekennzeichnet, die kumulativ vorliegen müssen: Die Klausel muss objektiv ungewöhnlich**,** d.h. für den Vertragstypen unüblich, und sie muss im konkreten Einzelfall auch für den Betroffenen unvorhersehbar sein, d.h. dass ungewöhnliche Klauseln dann zulässig sind, wenn etwa nach dem Gang der Vertragsverhandlungen oder der herausgehobenen drucktechnischen Gestaltung der Klausel der Durchschnittsverbraucher ihre Einbindung trotzdem erwarten musste, wobei die Beweislast die verarbeitende Stelle trifft. Unter § 305c BGB fallen insbesondere solche Klauseln, deren Regelungsgehalt nicht gegen Datenschutzrecht verstößt und deren Einbindung (nur) wegen ihres Überrumpelungscharakters unzulässig ist. Überschneidungen mit den Fällen von §§ 307 ff. BGB sind selbstverständlich denkbar.

Objektiv ungewöhnlich dürfte zunächst jede Klausel sein, die einem Betroffenen die Zustimmung zu Datenverarbeitungsmaßnahmen abverlangt, die, auch wenn sie vom geltenden Datenschutzrecht nicht abweichen, für die Erfüllung der Pflichten des Hauptvertrags nicht erforderlich sind. Einen besonders

schweren Fall der objektiv überraschenden Klausel stellen solche Einwilligungen dar, die keinerlei inhaltliche Bindung an den Vertragszweck aufweisen.

Dementsprechend wäre eine Klausel ungewöhnlich, welche der verantwortlichen Stelle das Recht einräumt, generell und für jeden Fall die Profile eines Betroffenen auf allgemein zugänglichen sozialen Medien aufzusuchen und die dort hinterlegten Daten zu erheben und nutzen. Gleiches würde etwa für eine Klausel gelten, die bestimmt, dass eine Leistung nur so lange gewährt wird, wie der Betroffene „Freund" des Unternehmens auf einem sozialen Netzwerk ist und dem Unternehmen somit Zugriff auf dessen Profil gewährt, soweit dies nicht bereits gegen § 28 Abs. 3b BDSG verstößt. Schließlich ist auch die Einholung einer Einwilligung zur Nutzung von kommerziell wenig gebräuchlichen Kommunikationswegen auf sozialen Netzwerken (z.B. das Postfach auf Facebook anstelle der Nutzung des Post- oder E-Mail-Verkehrs) objektiv ungewöhnlich. Ebenso ist jedoch auch jede Weitergabe von Daten an Dritte, selbst, wenn sie einwilligungsfähig ist, nach den Wertungen des Datenschutzrechts (§ 4 Abs. 3 Nr. 3 BDSG) stets überraschend.

Die Einbeziehung muss auch subjektiv unvorhersehbar sein. Wird eine Einwilligung ordnungsgemäß eingeholt, so ist die Klausel nur im Ausnahmefall subjektiv unvorhersehbar, da das Datenschutzrecht selbst die Aufklärung des Betroffenen über Verarbeitungszweck und Empfänger hinsichtlich seiner Daten anordnet. Hier ist erneut auf die Bedeutung der jeweils abgesetzten drucktechnischen Gestaltung der Einwilligungserklärungen hinzuweisen (§ 4a Abs. 1 S. 4 BDSG). Die Erklärung darf auf keinen Fall im Kleingedruckten untergeschoben wirken, indem eine besonders kleine Schriftart oder ein besonders langer Text gewählt wird.[154] In Frage kommt ein leicht lesbarer Text in einem farbig umrahmten oder abgesetzten Feld. Die Wahrscheinlichkeit der Wirksamkeit wird erhöht, wenn auch dann ein Opt-In-Kästchen zur Bestätigung der Kenntnisnahme benutzt wird, wenn eine rechtliche Verpflichtung hierzu nach der Rechtsprechung nicht besteht. Sind Werbeansprachen geplant, ist darüber hinaus § 7 UWG und das dortige Erfordernis aktiver Einwilligungen zu beachten.

2.3.3.6.4 Wirksame Einbeziehung in den Vertrag

Für die Einbeziehung nicht überraschender Klauseln gilt § 305 Abs. 2 BGB. Danach muss der Betroffene grundsätzlich ausdrücklich auf die Einbeziehung datenschutzrechtlicher Einwilligungen hingewiesen und der Zugang auch tatsächlich gewährt werden. Auch hier sehen die §§ 4, 4a BDSG strengere Voraussetzungen vor als die zivilrechtlichen Normen. Es ist darauf zu achten, dass sich datenschutzrechtliche Einwilligungen deutlich vom Rest der AGB absetzen.

2.3.4 Fehlerfolgen

Ist eine unwirksame Einwilligung abgegeben worden, ist der verantwortlichen Stelle für die betreffenden Daten ein Rückgriff auf gesetzliche Erlaubnisnormen verwehrt. Gleiches gilt, wenn der Betroffene eine Einwilligung verweigert hat.[155] Die Datenverarbeitung ist nach § 4 Abs. 1 BDSG dann zwingend rechtswidrig. Die verantwortliche Stelle ist verpflichtet, für die beabsichtigte Datenerhebung, -verarbeitung

[154] Ähnlich BGH, Urt. v. 16.07.2008, VIII ZR 348/06, Rn. 31 – Payback.

[155] Vgl. Simitis, in: Simitis, BDSG, § 28, Rn. 20.

und -nutzung vorab das Bestehen einer gesetzlichen Erlaubnisgrundlage zu prüfen. Für Social CRM-Betreiber bedeutet dies, dass auf die Abfassung als AGB eingebundener Einwilligungserklärungen besondere Sorgfalt zu verwenden ist..

Die Einholung einer Einwilligung zur Verarbeitung von Social-Media-Daten begegnet dem Problem, dass das Einverständnis mit der Datenerhebung in der Regel mit einer Gegenleistung gekoppelt wird, die in keinem Zusammenhang mit der Datenerhebung steht. Es ergeben sich dadurch Mängel hinsichtlich einer in Kenntnis der Verarbeitungszwecke freiwillig abgegebenen Einwilligung[156] und bezüglich der AGB-rechtlichen Zulässigkeit einer formularmäßigen Erklärung. Eine Einwilligung kann unfreiwillig sein, wenn die versprochene Gegenleistung so dominant und attraktiv ist, dass der Betroffene die Vereinbarung als einseitig begünstigend empfindet und sich typischerweise über die Folgen der Einwilligung keine Gedanken macht.[157] Umgekehrt kann auch ein grobes Missverhältnis zwischen dem Umfang der Datenverarbeitung, in welche eingewilligt wird und der Gegenleistung Zweifel an der Freiwilligkeit der Erklärung begründen. In solchen Fallkonstellationen kann die Wirksamkeit einer Einwilligungserklärung auch deshalb scheitern, weil eine Verletzung von § 138 BGB vorliegt.

Ist die genannte fehlende inhaltliche Konnexität zwischen Datenerhebung und Gegenleistung Gegenstand von AGB, kann dies nach Maßgabe von § 305c BGB zusätzlich zur Annahme einer überraschenden und damit unwirksamen Klausel führen.

Im Übrigen ist für Einwilligungserklärungen grundsätzlich die Schriftform zu wählen. Abweichungen vom Schriftformerfordernis müssen begründbar sein, um eine der Schriftform gleichwertige Beweisgeeignetheit zu gewährleisten. [158] Eine Einwilligungserklärung muss drucktechnisch abgesetzt und getrennt von anderen Erklärungen unterschrieben werden. Zwar ist ein Opt-In nicht für alle Werbeformen notwendig (siehe § 7 UWG), allerdings muss auch bei einem Opt-Out eindeutig sein, dass der Betroffene überhaupt eine Entscheidung getroffen hat.

2.4 Die Datenerhebung aus sozialen Netzwerken

Im Rahmen der Verarbeitung von Daten aus sozialen Netzwerken (Social Media Monitoring) werden von Unternehmensseite gezielt soziale Medien überwacht. Dabei wird in der Regel entweder der gesamte Datenstrom oder nur eine bestimmte Anzahl von Accounts (z.B. bekannte Kunden) nach der Nennung von Keywords durchsucht. Als Keywords bieten sich zumeist Schlagworte an, welche mit dem Unternehmen in keinem Zusammenhang stehen, etwa die Nennung unternehmenseigener Produkte. Das Monitoring kann in Echtzeit oder durch periodische Suchabfragen erfolgen. Die Suchergebnisse werden dann, soweit sie gespeichert werden, verschiedenen internen Geschäftszwecken zugeführt. Neben dem Ziel der Markbeobachtung ermöglicht es Social Media Monitoring CRM-Betreibern ebenso, gezielt einzelne Datensätze aus sozialen Medien zu erheben und hierdurch beispielsweise das Verhalten einzelner Personen gezielt zu überwachen.

---

[156] Rogosch, Die Einwilligung im Datenschutzrecht, S. 82 ff.; Zscherpe, MMR 2004, S. 727.

[157] Taeger, in: Taeger/Gabel, BDSG, § 4a, Rn. 51.

[158] Scheja/Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 5, Rn. 86, 97.

Eine weitere Methode der Datenakquise aus sozialen Netzwerken ist schließlich der Datenkauf von auf Monitoring und Auswertung von Big Data spezialisierten Unternehmen (sog. Data-Brokern). Auch dieser Vorgang stellt aus Sicht des CRM-Betreibers eine Datenerhebung dar (§ 3 Abs. 3 BDSG). Die von Datenbrokern angebotenen Produkte reichen von anhand von Stichworten erhobenen Rohdaten über Profilinhalte bis zu individuell erstellten, auf der Verknüpfung von Daten aus verschiedenen Quellen basierenden, umfassenden Profilen.

Einer Datenerhebung durch Social CRM können zahlreiche Probleme entgegenstehen: Teilweise kann die Einholung einer Einwilligung aus faktischen Gründen bereits nicht durchführbar sein, weil es sich bei den von einer Datenerhebung Betroffenen zum Beispiel um einen Nichtkunden handelt. Doch auch im Falle einer existierenden Kundenbeziehung können der Einholung einer Einwilligung die oben bezeichneten Risiken entgegenstehen. Um jene Hindernisse der Datenerhebung zu vermeiden, ist zu klären, ob und vor allem wie es CRM-Betreibern ermöglicht werden kann, die für das Social Media Monitoring erforderlichen Daten zu erhalten ohne dass hierfür eine Einwilligung des Betroffenen erforderlich ist. Die dafür nötige Grundlage kann sich nach § 4 Abs. 1 BDSG nur aus dem Gesetz selbst ergeben.

Die datenschutzrechtliche Zulässigkeit solcher Erhebungen bestimmt sich nach dem Zweck, den die verantwortliche Stelle mit der Datenerhebung verfolgt, das bedeutet, dass die reine Begutachtung der Erhebung keine abschließende Bewertung der Maßnahme erlaubt. Die folgende Darstellung beschränkt sich daher auf die Frage, in welchen Fällen bereits die Erhebung rechtswidrig ist, und in welchen Fällen zusätzlich die weiteren Verarbeitungs- und Nutzungsvorgänge betrachtet werden müssen. Da jedes erhobene Datum grundsätzlich nur zu bestimmten Verarbeitungs- und Nutzungszwecken erhoben werden darf, bietet es sich an, die Social Media Monitoring-Maßnahmen nach solchen Zwecken zu untergliedern.

Die für die Datenerhebung in sozialen Netzwerken in Frage kommenden Erlaubnisnormen sind folgendermaßen strukturiert: Die grundlegende Erlaubnisnorm bildet § 28 Abs. 1 Satz 1 BDSG mit drei Unterfällen (Nrn. 1-3), in welchen unter bestimmten Voraussetzungen die Datenerhebung und -speicherung für (allgemeine) eigene Geschäftszwecke erlaubt wird. Auch § 29 BDSG, der sich mit der geschäftsmäßigen Übermittlung als Erhebungszweck beschäftigt, und bei dem im Gegensatz zu § 28 BDSG die Daten und ihre Weitergabe selbst den Geschäftszweck darstellen, mag im Einzelfall Anwendung finden, obwohl für das CRM gerade die Datenerhebung zur geschäftsabhängigen, eigenen Nutzung charakteristisch ist. Daneben gilt es, spezialgesetzliche Normen zu beachten, die unter Umständen vorrangig anzuwenden sind.

Einen Sondertatbestand für das Social Media Monitoring stellt § 30a BDSG dar, welcher die Erhebung von Daten zum Zwecke der geschäftsmäßigen Markt- und Meinungsforschung unter besondere Voraussetzungen stellt. Die Vorschrift sieht gegenüber den §§ 28, 29 BDSG Lockerungen insbesondere hinsichtlich der Verarbeitbarkeit besonderer Arten von personenbezogenen Daten vor.[159] Fraglich ist, in welchem Umfang Social Media Monitoring-Ergebnisse in dieser Form privilegiert werden können.

Die Vorschrift ist § 29 Abs. 1 BDSG nachgebildet. So wie § 29 BDSG von einer Übermittlung an einen Dritten zur Weiterverarbeitung ausgeht, hat § 30a BDSG nach der gesetzgeberischen Vorstellung primär die Durchführung von Studien durch externe Sozialforschungseinrichtungen im Auge. Es besteht dennoch

[159] Ambs, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 30a, S. 141; Gola/Schomerus, BDSG, § 30a, Rn. 1 f.; vgl. auch die Gesetzesbegründung, BT-Drs. 16/13657, S. 33.

Konsens im Schrifttum, dass auch In-House-Marktforschung unter § 30a BDSG fällt, weil die Norm weder dem Wortlaut nach, noch zur Verwirklichung der Normziele zwingend die Weitergabe an eine externe Stelle voraussetzt.[160]

Leitbild der Markt- und Meinungsforschung ist traditionell die Umfrage. Die Umfrage hat gegenüber der Erhebung von Daten aus sozialen Netzen den Vorzug, dass sie im Einklang mit dem Direkterhebungsgrundsatz gemäß § 4 Abs. 2 BDSG steht. Werden Daten aus sozialen Netzwerken ohne Einwilligung des Betroffenen erhoben, gestaltet sich der Direkterhebungsgrundsatz als ein nur schwerlich zu überwindendes rechtliches Hindernis. Ausnahmsweise darf auf die Direkterhebung beim Betroffenen nach § 4 Abs. 2 Nr. 2b BDSG verzichtet werden, wenn sie einen unverhältnismäßigen Aufwand erfordern würde. Um diesem gesteigerten Rechtfertigungsaufwand vorzubeugen, sollte das Unternehmen daher vor einem Einsatz des Social Media Monitoring zu Marktanalysezwecken stets prüfen, ob nicht in zumutbarer Weise dieselben Daten etwa im Rahmen einer Online-Umfrage abgefragt werden könnten. Ist dies der Fall, verbietet sich eine Erhebung personenbezogener Daten zur Marktanalyse ohne weiteres. Dies gilt unabhängig davon, ob sie Markt- und Meinungsforschung im Rechtssinne darstellt oder nicht. Es verbliebe die anonyme oder pseudonyme Erhebung.

Es ist fraglich, inwieweit die Berechnungen, welche das Social Media Monitoring durch die Erhebung vorbereitet und die Business-Intelligence-Engine durchführt, überhaupt als Markt- und Meinungsforschung im Sinne der Norm gelten können. Denn es ist von § 30a BDSG zwar nicht zwingend ein Outsourcing an Sozialforschungsunternehmen gefordert, wohl aber eine wissenschaftliche Methodik. Hieran scheitern die Analysen von aus Social Media Monitoring gewonnenen Daten regelmäßig. Das Erfordernis bei der Erhebung wissenschaftliche Methoden zu verwenden, folgt zum einen aus der eindeutigen Gesetzesbegründung[161], zum anderen kann sie auch aus dem Wortlaut der Norm („Forschung“) entnommen werden. [162] Social Media Monitoring kann zwar nicht per se[163], aber bei einem entsprechenden methodengeleiteten wissenschaftlichen Vorgehen unter § 30a BDSG gefasst werden.[164]

Dies geschieht überwiegend bereits beim ersten Schritt, der korrekten Stichprobenauswahl.[165] Hier wird üblicherweise nicht, wie in der soziologischen Statistik üblich, randomisiert ausgewählt, sondern die Stichprobe computergeneriert so weit wie möglich gefasst, was ohne Rechtfertigung bereits mit dem Grundsatz der Datenvermeidung nach § 3a BDSG kollidiert und daher wegen Verfehlung des Normzwecks an der Privilegierung durch die Norm nicht teilhaben kann. Auch findet in aller Regel keine Vali-

---

[160] Vgl. Pflüger, RDV 2010, S. 103 f.

[161] BT-Drs. 16/13657, 19 f., mit Verweis auf die Prüfbitte des BR in BR-Drucks. 4/09, 15 und BT-Drs. 16/12011, 43 f. Beispiele für methodisch unzureichendes Vorgehen bei Schäfer-Newiger, WRP 2001, S. 784f.

[162] Eine a.A. will zur Bestimmung der Wissenschaftlichkeit allein das Ziel der Umfrage als entscheidend betrachten; so z.B. Ehmann, in: Simitis, BDSG, § 30a, Rn. 98.

[163] A.A. Solmecke/Wahlers, ZD 2012, S. 552.

[164] Dies bejaht auch Forgó, in: BeckOK BDSG, § 30a, Rn. 3; zu weitgehend demgegenüber Solmecke/Wahlers, ZD 2012, S. 552.

[165] Vgl. Ehmann, in: Simitis, BDSG, § 30a, Rn. 98; Forgó, in: BeckOK BDSG, § 30a, Rn. 3; abwegig insofern Iraschko-Luscher/Kiekenbeck, ZD 2012, S. 263, die selbst nicht davon ausgehen, dass Daten aus Bewertungsportalen repräsentativ sind.

dierung der Daten aus sozialen Netzwerken statt, so dass die Stichproben einen Grad an Unzuverlässigkeit aufweisen können, der mit dem wissenschaftlichen Anspruch der Sozialforschung nicht vereinbar ist.

Weiterhin ist keine Markt- und Meinungsforschung als empirisch-stochastisches Verfahren zur Bestimmung von Gruppenverhalten gegeben, wenn nicht, wie in § 30a Abs. 3 Satz 1 BDSG gefordert, frühestmöglich anonymisiert wird, bzw. nicht gemäß S. 2 der Vorschrift eine getrennte Speicherung der Zuordnungsfunktion erfolgt. Dann bleibt nämlich die Kontrolle des Verhaltens Einzelner möglich, was gerade nicht Ziel eines abstrakten Forschungsvorhabens sein kann. Der Zwang zur Anonymisierung bzw. Pseudonymisierung schließt es neben der rechtlichen Unzulässigkeit nach § 30a Abs. 2 Satz 1 BDSG auch tatsächlich aus, die erhobenen Daten neben der Markt- und Meinungsforschung noch einem weiteren datenschutzrechtlich relevanten Zweck zuzuführen. Bleibt die Bestimmbarkeit von Betroffenen in den Stichproben aufrechterhalten, ist eine Zweckänderung zumindest tatsächlich denkbar, was dem Normzweck widerspräche.

Ob die Methodik der Auswertung der Daten wissenschaftlichen Standards genügt, hängt von der eingesetzten Software und deren Algorithmen ab. Ziel muss eine abstrakte Darstellung des Marktes sein, wobei statistische Grundsätze insbesondere zur Gruppierung der Ergebnisse einzuhalten sind. Im Übrigen kann eine unwissenschaftliche Stichprobengenerierung durch eine mathematisch anerkannte Form der Auswertung auch nicht geheilt werden.

Schließlich ist noch auf die Abgrenzung zwischen wissenschaftlicher Marktforschung und Erhebungen zur Vorbereitung von Werbung zu achten. Zwar steht die Verfolgung eigener Geschäftsinteressen der Wissenschaftlichkeit der Markt- und Meinungsforschung nicht entgegen. Dass die Ergebnisse der Studie die eigenen Absatzchancen mittelbar fördern, indiziert daher noch nicht ihren Werbecharakter. Allerdings wird die Privilegierung des § 30a BDSG gerade um den Preis gewährt, dass die Markt- und Meinungsforschung sich von unmittelbarer werblicher Verwertbarkeit fernhält. Das bedeutet, dass das Ergebnis nur einen abstrakten, nicht personenbezogenen oder –beziehbaren Überblick über den Markt darstellen darf, was mit ausreichender Gruppengröße bei den einzelnen Datenpunkten sichergestellt werden kann.

Insoweit fallen nur wenige Verfahren der Business Intelligence unter § 30a BDSG. Soweit keine Einwilligung vorliegt, muss also auch bei einer Verarbeitung mit dem Zweck „Datenanalyse“ in der Regel § 28 BDSG geprüft werden.

Auch ohne Einwilligung wäre eine Erhebung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig, wenn sie zur Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen (§ 311 BGB) Schuldverhältnisses erforderlich ist. Das Gesetz meint insoweit nicht die Herstellung von Gelegenheiten zum Vertragsschluss im Sinne der Werbung, vielmehr muss bereits auf andere Weise mindestens ein vorvertragliches Schuldverhältnis im Sinne des § 311 Abs. 2 BGB mit beiderseitigen Interessen am Vertragsschluss entstanden sein.[166] „Erforderlich“ bedeutet in diesem Fall, dass zur Erfüllung des Vertragszwecks auf die Erhebung nicht in zumutbarer Weise verzichtet werden kann.[167] Das dürfte in Bezug auf Social Media-Daten selbst dann nicht der Fall sein, wenn z.B. unvollständige, aber zur Vertragser-

[166] Gola/Schomerus, BDSG, § 28, Rn. 13.

[167] Simitis, in: Simitis, BDSG, § 28 Rn. 57; Gola/Schomerus, BDSG, § 28, Rn. 15.

füllung notwendige Angaben, etwa Adressdaten in der Kundendatenbank der verantwortlichen Stelle online recherchiert und eingefügt würden. Eine solche Recherche verstieße gegen den Direkterhebungsgrundsatz nach § 4 Abs. 2 BDSG. Bei einem bekannten Kunden, zu dem wenigstens eine Kontaktmöglichkeit vorhanden ist, ist diese auszuschöpfen und der Betroffene um eigenhändige Vervollständigung seiner Angaben zu bitten.

2.4.1 Der Erlaubnistatbestand des § 28 Abs. 1 S. 1 Nr. 3 BDSG

Große Relevanz für das Social CRM entfaltet § 28 Abs. 1 Satz 1 Nr. 3 BDSG, der die Erhebung, Verarbeitung und Nutzung von allgemein zugänglichen Daten unter vereinfachte Bedingungen stellt. Danach ist die Datenverarbeitung nur dann unzulässig, wenn das schutzwürdige Interesse des Betroffenen an deren Ausschluss das berechtigte Interesse der verantwortlichen Stelle an der Datenverarbeitung offensichtlich überwiegt.

Teilweise wird vertreten,[168] dass § 28 Abs. 1 Satz 1 Nr. 3 BDSG unanwendbar sei, soweit mit dem Betroffenen ein Vertragsverhältnis besteht. Die Grenze der zulässigen Datenerhebung bilde hierbei entweder eine eingeholte Einwilligung oder Nr. 1 der Vorschrift, der die verarbeitende Stelle ausschließlich dazu berechtigt, diejenigen Daten zu erheben, die für die Begründung, Durchführung und Beendigung des Vertrages erforderlich sind. Eine Ausweitung der zulässigen Datenbasis der verantwortlichen Stelle könne hieraus nicht erwachsen.

Es trifft zu, dass jedenfalls der erklärte Wille des Betroffenen die Grenze von § 28 Abs. 1 Satz 1 Nr. 3 BDSG darstellt. Damit besteht ein Vertrauensschutz darauf, nicht weiter von Erhebungsmaßnahmen betroffen zu werden, als dieser erklärte Wille reicht. Dieser ist einschließlich abgegebener Einwilligungen auch im Rahmen der Vorschrift selbst zu prüfen, einmal auf tatbestandlicher Ebene bei der Frage der Zugänglichkeitskontrolle und einmal im Rahmen der Interessenabwägung. Es ist damit die Stellung von § 28 Abs. 1 Satz 1 Nr. 3 BDSG im Gefüge der Erlaubnisnormen darzustellen. Die Vorschrift trägt dem Jedermannsgrundrecht, „sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten" (Art. 5 Abs. 1 Satz 1 2. Hs. GG), der sog. Rezipientenfreiheit, Rechnung. Dieses Recht steht nach allgemeiner Meinung auch juristischen Personen im Rahmen ihrer Geschäftstätigkeit zu (Art. 19 Abs. 3 GG).[169]

Die Entwicklung dahin, dass nunmehr jedermann die Gelegenheit hat, mit eigenen Aussagen die Öffentlichkeit zu erreichen, aber auch die Gefahren, dass solche Daten versehentlich veröffentlicht werden oder zu einem unbeabsichtigten Zweck wie dem Erstellen von Persönlichkeitsprofilen potentieller Kunden weiterverwendet werden könnten, konnte der Gesetzgeber nicht vorhersehen. Der Gesetzgeber hat eine Klarstellung, was in Zeiten von Big Data als allgemein zugängliches Datum zu betrachten sei, anlässlich der BDSG-Novelle 2009 versäumt, obwohl seinerzeit die Gefahren der Datensammlung in sozialen Netzwerken absehbar waren. Auch wenn das Bundesdatenschutzgesetz technikneutral gestaltet werden sollte, kann aus dieser legislativen Untätigkeit jedoch nicht geschlossen werden, dass es der Wille des Gesetzgebers war, Daten aus der Tageszeitung und solche aus sozialen Netzwerken rechtlich gleich zu behandeln. Bei der Bestimmung der Reichweite der Informationsfreiheit im Rahmen von § 28 Abs. 1 Satz 1

[168] BAG, DB 1987, S. 1048; Simitis, in: Simitis, BDSG, § 28, Rn. 55; Gola/Schomerus, BDSG, § 28, Rn. 9.

[169] Grabenwarter, in: Maunz/Dürig, GG, Art. 5 GG, Rn. 19; Herzog, in: Maunz/Dürig, GG, Art. 5, Rn. 87, 90f.

Nr. 3 BDSG ist daher weiterhin zu berücksichtigen, dass die Rezipientenfreiheit maßgeblich auf „allgemein zugängliche Quellen" aufbaut.

Trotz dieser verfassungsrechtlichen Grundlage spricht der derzeitige Wortlaut des § 28 Abs. 1 Satz 1 Nr. 3 BDSG von allgemein zugänglichen Daten, nicht hingegen von „Quellen." Im Folgenden ist deshalb zu klären, was im Rahmen von Social CRM unter dem Begriff „allgemein zugängliche" Daten zu verstehen ist. Sodann ist die Struktur der Abwägung darzustellen und, soweit ohne Rücksicht auf den Erhebungszweck möglich, sind Hinweise zur Abwägung zu geben.

2.4.2 Allgemein zugängliches Datum

Die vom Bundesverfassungsgericht entwickelte Definition zur Rezipientenfreiheit,[170] setzt die Begriffe „allgemein zugängliches Datum" und das in Art. 5 Abs. 1 Satz 1 2. Hs. genannte „Datum aus einer allgemein zugänglichen Quelle" gleich. Nach diesem verfassungsrechtlichen Begriff ist ein Datum immer dann allgemein zugänglich, wenn es aus einer Quelle entnommen ist, die technisch geeignet und bestimmt ist, der Allgemeinheit, d.h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen.[171] Dagegen setzt die Definition im Bundesdatenschutzgesetz seit der Reform des § 28 BDSG im Jahre 2009 jedenfalls sprachlich nicht mehr am Quellenbegriff, sondern an der allgemeinen Zugänglichkeit der Daten selbst an. Zwar soll hieraus nach der Literatur keine Bedeutungsänderung erfolgen.[172] Gleichzeitig wird nach der ganz herrschenden Meinung[173] in der Literatur auch ein Datum, das aus einer nicht allgemein zugänglichen Quelle entnommen wurde, in die Privilegierung von § 28 Abs. 1 Satz 1 Nr. 3 BDSG aufgenommen, sofern die Entnahme möglich gewesen wäre. Insoweit wird nur zwischen Daten, die bereits einer unbestimmten Anzahl Personen mitgeteilt waren, und solchen, bei denen dies nicht der Fall war, unterschieden. Diese Unterscheidung scheint im Datenschutzrecht fragwürdig. Wenn § 28 Abs. 1 Satz 1 Nr. 3 BDSG Ausfluss der Rezipientenfreiheit ist, kann auch die Regelung des BDSG nur für die grundrechtlich geschützten Rechtsgüter gelten. Art. 5 Abs. 1 Satz 1 2. Hs. GG ist gerade nicht primär ein Grundrecht auf Datensammlung, sondern ein Grundrecht auf Information aus einer Vielfalt von öffentlichen Quellen, die eine selbstbestimmte Meinungsbildung zur Teilnahme am öffentlichen Leben ermöglichen soll. Nur insoweit ist angesichts der entgegenstehenden Grundrechte des Betroffenen die verarbeitungsfreundliche Regelung zu rechtfertigen. In praktischer Hinsicht führt dies dazu, dass stets doppelt geprüft werden muss: Erstens, ob es sich um allgemein zugängliche Daten handelt und zweitens, ob das betreffende Datum aus allgemein zugänglichen Quellen erhoben wurde. Daraus resultiert eine praktische Beschränkung auf allgemein zugängliche Quellen. Es ist nach alledem daran festzuhalten, dass grundsätzlicher Anknüpfungspunkt die allgemeine Zugänglichkeit der Quelle bleibt.

Die Tatsache, dass es nach der grundrechtlichen Definition zuvörderst auf die Geeignetheit und Bestimmtheit der Quelle und nicht des Datums ankommt, bedeutet für die Bestimmung des berechtigten

---

[170] BVerfGE 27, 71.

[171] BVerfGE 23, 73; Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 28 BDSG, Rn. 7; Gola/Schomerus, BDSG, § 28, Rn. 32.

[172] Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 56.

[173] Simitis, in: Simitis, BDSG, § 28, Rn. 159; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 59.

Interesses der verantwortlichen Stelle, dass die Motive des Betroffenen (etwa, ob die Offenbarung gegenüber Dritten absichtlich oder versehentlich geschehen ist) bei der Beurteilung der allgemeinen Zugänglichkeit außer Betracht bleiben müssen. Entscheidend ist vielmehr, ob die Quelle ihrer technischen Einrichtung nach für jedermann von außen zugänglich ist.[174] Subjektive Elemente können gegebenenfalls in der folgenden Abwägung berücksichtigt werden.[175]

Schließlich ist daran zu erinnern, dass besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) nur dann an der Privilegierung des § 28 Abs. 6 Nr. 2 BDSG teilhaben, wenn sie offenkundig öffentlich gemacht worden sind. Dies kann in Nutzerprofilen der Fall sein.

Allerdings wird auch in einzelnen Postings, Tweets und Beiträgen regelmäßig eine Zugehörigkeit eines Dritten zu einer der in § 3 Abs. 9 BDSG genannten Gruppen erwähnt werden. Ein solches Posting wäre von der Erlaubnis zur Verarbeitung ohne Einwilligung nicht gedeckt. Es empfiehlt sich in der Praxis wegen der hiermit verbundenen Unwägbarkeiten, auf die Erhebung besonderer Arten personenbezogener Daten in Textkörpern so weit wie möglich zu verzichten und, gegebenenfalls in Form einer stichwortbasierten Ausschlussliste, die Erhebung von Postings, die besondere Arten personenbezogener Daten enthalten, zu verhindern. Selbst eine Pseudonymisierung kann hierbei keinerlei Abhilfe schaffen: Zumindest bis zur endgültigen Löschung des den Zuordnungsschlüssel beinhaltenden Datensatzes bleibt dieser personenbeziehbar im Sinne des § 3 Abs. 1 BDSG und seine Erhebung rechtfertigungsbedürftig. Zudem erlaubt das in §§ 3 Abs. 9, 28 Abs. 6 Nr. 2 BDSG aufgestellte absolute Verbot bei besonderen Arten personenbezogener Daten mangels Wertungsmöglichkeit innerhalb der betroffenen Normen keine Differenzierung.

2.4.2.1 Übersicht über die allgemeine Zugänglichkeit bei typischen sozialen Netzwerken

Interne und externe Suchmaschinen ermöglichen es jedermann, die in sozialen Netzwerken befindlichen Daten auffindbar und ihre Inhalte zugänglich bzw. weiterverwendbar zu machen. Lediglich die Menge der auf diesem Wege verfügbargemachten Daten variiert je nach Zugriffsbeschränkung. Die Gründe für die Zugänglichkeit der Daten sind vielfältig und im Rahmen der Abwägung stets zu würdigen.

Auf Plattformen wie Twitter, auf denen häufig die Ansprache einer unbestimmten Anzahl von Lesern und der Beitrag zu öffentlichen Diskussionen vom Nutzer erwünscht sind, stellt die öffentliche Einsehbarkeit den Regelfall dar.

Facebook macht hingegen die „Erfassung" von Nutzerdaten von deren „Zustimmung" abhängig.[176] Außerdem wird der verantwortlichen Stelle vorgeschrieben, klarzustellen, dass Informationen durch sie und nicht durch Facebook erhoben werden, sowie eine Datenschutzrichtlinie bereitzustellen, in der die gesammelten Datenarten und Nutzungszwecke kenntlich sind.

Die Diskussion , ob Inhalte von Facebook-Profilen allgemein zugänglich sind, erübrigt sich somit; § 28 Abs. 1 Satz 1 Nr. 3 BDSG kann wegen des Einwilligungserfordernisses keine Anwendung finden.

---

[174] Ambs, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 28 BDSG, Rn. 10.

[175] H.M.; a.A. offenbar Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 59.

[176] Siehe Abschnitt 5.7 der „Erklärung der Rechte und Pflichten" von facebook; die im englischen Original verwendeten Begriffe „collection" und „consent" entsprechen den im Europarecht verwendeten Begriffen für Erhebung und Einwilligung.

Blogs und ähnliche Dienste (z.B. YouTube), bei denen ebenfalls ein Wirken nach außen im Vordergrund steht, sind in aller Regel allgemein zugänglich. Foren sind weitgehend allgemein zugänglich, sofern für das Lesen der Beiträge keine individuellen Hürden gestellt werden. Dasselbe gilt für Diskussionen auf Wikis.

Foren können gelegentlich im Lesezugriff beschränkt sein, stehen dann aber oft gegen Anmeldung jedermann zur Verfügung. Newsgroups und Mailinglisten arbeiten auf einer ähnlichen Subskriptionsbasis. Ob bei der Anmeldung zu diesen Formen sozialer Medien eine Prüfung des zukünftigen Abonnenten stattfindet, ist plattform- und betreiberabhängig.

2.4.2.2 Einzelfälle der allgemeinen Zugänglichkeit

Fraglich ist, inwieweit die allgemeine Zugänglichkeit auch durch Algorithmen zusammengefasste Inhalte abdeckt, welche ad-hoc gemäß einer Suchanfrage zusammengestellt werden. Problematisch ist hierbei insbesondere die Verkettung von Datensätzen**.** Durch Suchanfragen werden Beiträge verschiedenster Art zu einem bestimmten Thema gebündelt dargestellt. Die Verkettung von Daten ist ein Verarbeitungsvorgang, der neue, den Einzelergebnissen nicht zu entnehmende personenbezogene Daten entstehen lässt. Diese Verkettung ist als selbstständiger Verarbeitungsvorgang durch eine eigenständige Rechtsgrundlage zu legitimeren. Beispiel:

Die U-AG, ein Pkw-Hersteller, sucht auf Twitter nach Nennungen eines Modells der Konkurrenz, welches in einem Marktsegment mit einem ihrer Modelle konkurriert. Die ersten beiden Suchergebnisse ergeben folgende Daten:

Suchergebnis 1: Kommentar eines Freundes: A hat als Holstein-Fan natürlich das Autokennzeichen KI-EL 1900!

Suchergebnis 2: Bild eines Autos mit dem Kennzeichen KI-EL 1900, das in einen Unfall verwickelt ist

Die sich aus diesen beiden Suchergebnissen ergebende personenbezogene Einzelangabe „A hatte einen Unfall“ ist den einzelnen Quellen ohne Rückgriff auf nicht-öffentliche Register oder zufällige Kenntnis nicht zu entnehmen. Sie ergibt sich aber ohne weiteres aus der Gesamtschau der beiden Tweets. Wie der EuGH in seiner Entscheidung zu den Sperrpflichten von Suchmaschinenbetreibern im Mai 2014 festgestellt hat,[177] kann eine Seite von Suchergebnissen bereits ein umfassendes Profil eines Betroffenen ergeben und daher das Persönlichkeitsrecht in besonders qualifizierter Weise bedrohen. Ein solches Profil enthält typischerweise zahlreiche, nur in der Verkettung sichtbar gemachte, neue Daten. Allerdings sind diese, zumindest zum Zeitpunkt der Erhebung, grundsätzlich für jedermann einsehbar gewesen. Weder für die Daten selbst noch für die Quelle gab es eine personelle Beschränkung der Einsehbarkeit. Nach der derzeitigen Rechtslage muss der genannte Datensatz daher als allgemein zugänglich angesehen werden. Dass die einzelnen Tweets nicht verkettet werden sollten, hebt ihre technische Geeignetheit zur Außenwirkung nicht auf. Auch das Datum „A hatte einen Unfall“ ist daher grundsätzlich als allgemein zugänglich zu bewerten.

[177] EuGH, NJW 2014, S. 2257.

Ein weiteres Problem stellen sog. Reposts bzw. Retweets dar. Es handelt sich um eine von den sozialen Medien mit ihrem Fokus auf das Teilen von Inhalten beförderte Praxis, sich Postings von Dritten zu eigen zu machen oder sich mit ihnen auseinanderzusetzen, indem sie kopiert, kommentiert oder als eigenes Posting weiterverbreitet werden. Dieser Vorgang ist durch den ursprünglichen Verfasser kaum zu verhindern oder zu kontrollieren, zumal der Re-Poster nicht auf eine Weiterleitungsfunktion angewiesen ist, die der ursprüngliche Verfasser gegebenenfalls abschalten könnte, sondern die Nachricht einfach kopieren oder bei entsprechendem Schutz abschreiben kann. Das Zugänglichkeitsproblem entsteht dann, wenn der ursprüngliche Poster sein Profil geschützt hatte und Inhalte von Nutzern geteilt werden, die ihr Profil allgemein zugänglich gemacht haben. Dadurch können personenbezogene Daten eingesehen werden, ohne dass dies vom ursprünglichen Ersteller beabsichtigt war. Gründe für ein solches Vorgehen können im Whistleblowing oder dem Wunsch nach Herstellung einer Prangerwirkung bestehen, allerdings auch schlicht Zustimmung zu der ursprünglichen Aussage ausdrücken. Es handelt sich traditionell gesprochen um das Äquivalent der Veröffentlichung privater Notizen.

Fraglich ist, ob das neue Posting als neue Quelle anzusehen ist, und wenn dies der Fall ist, ob aus dieser eine Erhebung privilegiert zulässig ist, ohne dass auf Tatbestandsebene bereits auf den entgegenstehenden Willen des ursprünglichen Autors abzustellen ist.

Erstere Frage muss bejaht werden, weil die Rechtmäßigkeit jeder Erhebung nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG danach zu beurteilen ist, ob zum Zeitpunkt der Erhebung tatsächlich eine unbestimmte Vielzahl von Personen die Quelle zur Kenntnis nehmen konnten. Das kopierte Datum erbt also nicht die Unzugänglichkeit seiner „Urschrift".

Ob die Zugänglichkeit der Kopie auch zur erleichterten Verarbeitung nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG führt, ist nach den aufgezeigten Grundsätzen zu beurteilen. Die verantwortliche Stelle findet die betreffende Nachricht vor, ohne dass sie eine Sperre umgangen hätte oder irgendjemanden getäuscht hätte. Es kann also vorkommen, dass die verantwortliche Stelle von einer unbefugten Handlung des Re-Posters profitiert, obwohl dieser sich in Widerspruch zum Veröffentlichungswillen des ursprünglichen Inhaltsverantwortlichen stellt. Teilweise wird hier verlangt,[178] in Fällen des offenkundig fehlenden Verbreitungswillens das Zugänglichkeitskriterium entgegen dem Obenstehenden mit einem subjektiven Element auszustatten, wodurch die allgemeine Zugänglichkeit in solchen Fällen wegfiele. Die herrschende Meinung sieht zu Recht von einer subjektivierenden Behandlung des Begriffs ab, was den Schwerpunkt der Prüfung auf die Interessenabwägung des § 28 Abs. 1 Satz 1 Nr. 3 BDSG legt.

2.4.3 Zweckfestlegung

Wie bereits anhand der Einwilligung dargestellt, bedarf jegliche Datenerhebung, auch wenn sie sich auf allgemein zugängliche Daten bezieht, der Festlegung eines legitimen Zwecks. Dies bedeutet, dass die verarbeitende Stelle darlegen muss, welche Schritte der Verarbeitung oder Nutzung für die betreffenden Daten vorgesehen sind, und zwar gedacht bis zum Endzweck (§ 28 Abs. 1 Satz 2 BDSG). Nach der Speicherung kann der Nutzungszweck zwar gemäß § 28 Abs. 2 Nr. 1 BDSG geändert werden. Diese Zweckän-

[178] Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 58.

derung ist als neue, selbstständige Datenverarbeitung aber im selben Maß rechtfertigungsbedürftig. Die engen Erlaubnistatbestände führt § 28 Abs. 2 BDSG auf.

Im Rahmen von § 28 Abs. 1 Satz 1 Nr. 3 BDSG kommt der Zweckfestlegung eine Doppelfunktion zu. Zum einen ist sie ein separates Tatbestandsmerkmal, dessen Fehlen die geplante Maßnahme schon rechtswidrig macht, ohne dass es noch einer Interessenabwägung bedarf. Ist zwar ein Zweck in Form einer geplanten Verarbeitung oder Nutzung festgelegt, dieser aber nicht legitim (z.B. unberechtigte Weitergabe an Auskunfteien, § 28a BDSG), strahlt dies auf die Erhebung selbst aus, mit der Folge, dass diese genauso unzulässig ist, als sei überhaupt kein Zweck festgelegt worden.

Zwar wäre es mit Blick auf das BDSG denkbar, dass zunächst Daten zu einem unzulässigen Zweck erhoben werden, dann aber im Rahmen der Zweckänderung gemäß § 28 Abs. 2 Nr. 1 BDSG nach ihrer Speicherung einen nach § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG zulässigen neuen Zweck erhalten und hierzu genutzt werden. Diese Praxis wäre wegen Verstoßes gegen Art. 6 b) der Datenschutzrichtlinie allerdings europarechtswidrig. Nach deren unzweideutigem Wortlaut dürfen Daten nur für rechtmäßige Zwecke erhoben werden. Die anderslautende Lösung würde zudem dem Sinn der Zwecksetzung zuwiderlaufen, der in den Transparenzpflichten nach §§ 4, 33 BDSG zum Ausdruck kommt, nämlich zumindest vorläufig eine für alle Beteiligten verbindliche Nutzung festzulegen. Es hätte die absurde Folge, dass die verantwortliche Stelle Daten grundsätzlich auf unbestimmte Zeit zu rechtswidrigen Zwecken speichern dürfte, wenn sie diese nur nach Zweckänderung einer rechtmäßigen Nutzung zuführt. Eine Zweckänderung kann daher nur zwischen zwei rechtmäßigen Zwecken erfolgen und einen rechtswidrigen Zweck nicht nachträglich rechtfertigen.

Schließlich kann der Erhebungszweck bei einer möglichen Abwägung als Anhaltspunkt dafür dienen, ob das von der verantwortlichen Stelle verfolgte Interesse sich gegenüber dem des Betroffenen durchsetzt.

Das von Art. 6 Abs. 1 lit. b) der Richtlinie 95/46/EG vorgegebene Erfordernis der Zwecksetzung ist zudem ein entscheidender Unterschied zwischen dem Monitoring nach amerikanischem Vorbild und der in der Europäischen Union zulässigen Praxis. Beim klassischen Monitoring mit Speicherung in einem Data-Warehouse wurden Daten für etwaige spätere Geschäftszwecke auf Vorrat und ohne konkrete Nutzungszwecke gesammelt. Nach dem Verständnis der Richtlinie 95/46/EG muss ein Verarbeitungszweck aber im Vorfeld so konkret festgelegt werden, dass eine Weiterbenutzung der Daten zu einem anderen Zweck eindeutig als solche erkennbar ist. Eine insofern oft anzutreffende Zweckfestlegung „zu eigenen Geschäftszwecken" ist ebenso wie die Festlegung „zur Verbesserung des Service" nur eine Wiederholung des Gesetzes und daher unzureichend. In beiden Fällen bliebe etwa eine Profilbildung noch von dem weiten Zweck erfasst, ohne dass dies für den Betroffenen transparent wäre. Ein Werbecharakter der geplanten Maßnahme ist besonders zu kennzeichnen, da ein Handeln ohne Einwilligung im Rahmen des Social CRM stets zur Rechtswidrigkeit der Maßnahme führen würde. Auch bei einer Erhebung zu anderen Zwecken muss an dieser Stelle bereits eine vorgezogene Rechtmäßigkeitsprüfung hinsichtlich des jeweils geplanten Zwecks stattfinden. Die Änderung des ursprünglichen Verarbeitungszwecks ist nur in Ausnahmefällen auf Grundlage einer konkreten, diese Zweckänderung rechtfertigenden, Rechtsgrundlage zulässig. Ein Beispiel für die nachträgliche Zweckänderung ist etwa § 28 Abs. 3 Satz 2 Nr. 1 BDSG, der die nachträgliche Nutzung von Kundendaten zu Werbezwecken rechtfertigt, obwohl diese ursprünglich nur zur Abwicklung des Vertrages erhoben wurden.

2.4.4 Interessenabwägung

Die allgemeine Zugänglichkeit von Daten kann zwar Grundlage der Datenerhebung sein und ist aufgrund der Struktur der Norm ein verhältnismäßig starker Indikator für deren Zulässigkeit. Sie allein erlaubt die Datenerhebung jedoch noch nicht. Gemäß § 28 Abs. 1 Satz 1 Nr. 3 BDSG ist die Erhebung vielmehr ausgeschlossen, wenn das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Es ist demnach eine Abwägung vorzunehmen, wobei die Datenerhebung dann unterbleiben muss, wenn das überwiegende Interesse für einen verständigen, neutralen Beobachter auf der Hand liegt. Eine Abwägung findet deswegen nur dort statt, wo solche Anhaltspunkte unmittelbar ins Auge springen. Das bedeutet unter der Prämisse der automatisierten Datenverarbeitung, dass die Fälle, in denen die Abwägung stattfinden muss, eine Ausnahme darstellen, gleichzeitig muss die technische Möglichkeit bestehen, solche offensichtlichen Anhaltspunkte für ein gegenläufiges Interesse des Betroffenen zu erkennen und danach zu handeln.

2.4.4.1 Interesse der verantwortlichen Stelle

Für das Interesse der verantwortlichen Stelle ist jedes mit den eigenen Geschäftszwecken (§ 28 Abs. 1 Satz 1 BDSG) verbundene Interesse ausreichend. Berechtigt ist jedes Interesse, welches von der Rechtsordnung gebilligt wird,[179] d.h. insbesondere ein solches, das mit den für die Geschäftstätigkeit der verantwortlichen Stelle geltenden Gesetzen konform ist. Hier ist einerseits auf die Umstände der Erhebung, andererseits auf den festgelegten Verarbeitungszweck abzustellen. Der Zweck bildet die Grundlage der Abwägung. Besondere Bedeutung kommt hier der internen Dokumentation zu, bei wiederkehrenden Verarbeitungen dem Verfahrensverzeichnis.

Ein berechtigtes Interesse hat die verantwortliche Stelle regelmäßig nur an solchen Daten, die sachlich zutreffend sind. Es ist jedenfalls ein generelles Bemühen um richtige und vollständige Daten notwendig.[180] Dies entspricht Art. 6 d) der Richtlinie 95/46/EG, nach der die verantwortliche Stelle „alle angemessenen Maßnahmen" treffen muss, damit unrichtige Daten gelöscht oder berichtigt werden. Die zu treffende Einzelfallentscheidung stellt die verantwortliche Stelle vor Schwierigkeiten und ist im Rahmen von § 28 Abs. 1 Satz 1 Nr. 3 BDSG nur in Ausnahmefällen geboten. Die grundsätzliche Erlaubnis zur Datenerhebung aus allgemein zugänglichen Quellen generiert regelmäßig auch eine rechtliche Vermutung der Zuverlässigkeit der Quelle. Auf eine Unrichtigkeit der Daten kann z.B. deren Herkunft deuten: Stammt das Datum etwa erkennbar von einem Satire-Account, so wird der Informationsgehalt regelmäßig von dem wertenden Element überzeichnet sein. Eine Prüfpflicht besteht im Sinne von § 4 Abs. 2 BDSG darüber hinaus regelmäßig, wenn Aussagen über Betroffene durch Dritte gemacht werden. Insofern muss § 4 Abs. 2 Nr. 2b BDSG so gelesen werden, dass bei Erhebungen aus allgemein zugänglichen Quellen eine Prüfpflicht in jedem Fall dann eintritt, wenn die erhobenem Daten erkennbar nicht von dem Betroffenen selbst zugänglich gemacht wurden.

---

[179] BGH, NJW 1984, S. 1887; VGH Mannheim, NJW 1984, S. 1912; Hoeren, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.6, Rn. 3 f.; Gola/Schomerus, BDSG, § 28, Rn. 33; Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 28, Rn. 6.

[180] Simitis in Simitis, BDSG, § 28, Rn. 33.

Die verantwortliche Stelle darf Daten von Dritten also in aller Regel nicht ohne Prüfung erheben. Soll eine Prüfpflicht vermieden werden, ist sicherzustellen, dass nur Äußerungen im eigenen Namen zur Speicherung ausgewählt werden.

Der Gesetzgeber hat, anders als bei § 28 Abs. 1 Satz 1 Nrn. 1 und 2 BDSG, bei § 28 Abs. 1 Satz 1 Nr. 3 BDSG bewusst darauf verzichtet, den Umfang der möglichen Erhebung danach zu begrenzen, ob die erhobenen Daten zur Erreichung des Erhebungszwecks erforderlich, d.h. unumgänglich notwendig, sind. Zu berücksichtigen ist aber, dass die Vorschriften für allgemein zugängliche Daten nur für die Ersterhebung gelten. Ursächlich hierfür ist, dass die Daten, im Fall ihrer Speicherung wegen der Verkettung mit anderen Daten regelmäßig nicht mehr allgemein zugänglich sind. Folglich muss eine gesonderte Rechtsgrundlage zur Weiterverarbeitung herangezogen werden.

Die Prüfung der Rechtmäßigkeit dieser „Fernziele" erfolgt im Rahmen der Prüfung des Erhebungszwecks (s.o.) und hat deswegen auch Auswirkungen auf die Rechtmäßigkeit der Erhebung selbst. Daher wird die verantwortliche Stelle in der Praxis häufig gezwungen sein, sich auf das Erforderliche zu beschränken. Ein solches Fernziel wird nicht selten die Anbahnung und spätere Erfüllung von Schuldverhältnissen sein. Die dort gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG geforderte Erforderlichkeitprüfung, wirkt sich auf die Erhebung allgemein zugänglicher Quellen aus, als dass die Erhebung von Daten, die für die Zwecke nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG nicht erforderlich sind, unter Umständen keinen legitimen Zweck für das Unternehmen darstellt. Eine Vorratsspeicherung ohne vorherige Zweckbindung ist dem § 28 Abs. 1 Satz 1 Nr. 1 BDSG fremd.

Zwar muss der verantwortlichen Stelle ein gewisser Einschätzungsspielraum bei der Auswahl der für die Zweckerreichung notwendigen allgemein zugänglichen Daten zugestanden werden. Im Umkehrschluss gilt indes, dass jedenfalls an der Erhebung von Daten, die ihrer Natur nach nicht zur Erreichung des Zwecks beitragen können, kein berechtigtes Interesse bestehen kann. Ferner ist darauf hinzuweisen, dass § 3a S. 1 BDSG auf allgemein-technischer Ebene die verantwortliche Stelle dazu anhält, so wenige Daten wie möglich zu verarbeiten.

Anhand dieser Kriterien wird eine klarere Konturierung des berechtigten Interesses der verantwortlichen Stelle möglich. So dürften für den Erhebungszweck nicht erforderliche Daten der Erhebung bereits dann entzogen sein, wenn tatsächliche Anhaltspunkte dafür bestehen, dass ein (offenkundig) überwiegendes Ausschlussinteresse des Betroffenen besteht. Für den legitimen Zweck erforderliche Daten dagegen müssen nur dann aus der Erhebung ausscheiden, wenn die tatsächlichen Grundlagen für ein entgegenstehendes Interesse am Ausschluss der Erhebung ohne vernünftigen Zweifel feststehen.

Ein besonderes Problem des Social Media Monitorings ist die intensive und extensive Überwachung von Einzelpersonen. Dabei wird über einen nicht unerheblichen Zeitraum der von einem Account ausgehende Datenstrom mitgeschnitten, indem alle oder doch die meisten Beiträge eines bestimmten Nutzers erhoben werden. Dem Unternehmen kommt es in solchen Fällen neben der Kenntnisnahme von den Inhalten der Kommunikation auch darauf an, abzuklären, welche Personen konkret (Benennung in der Message) oder potentiell (Freundesliste) von den Äußerungen angesprochen werden. Die Daten der Kontakte werden daher in der Regel miterhoben.

Eine solche Überwachung ist zwar nicht grundsätzlich unzulässig, allerdings stellt sie in vielen Fällen einen so tiefen Einschnitt in Persönlichkeitsrechte und Meinungsfreiheit der Betroffenen dar, dass sie sich

selbst unter den verarbeitungsfreundlichen Regeln von § 28 Abs. 1 Satz 1 Nr. 3 BDSG nicht rechtfertigen lässt. Die Prüfung der Zulässigkeit von Überwachungsmaßnahmen tangiert abermals Aspekte der Zwecksetzung, nämlich der Nutzung der gesammelten Äußerungen für weitere Maßnahmen. Insofern kann ihre Zulässigkeit nicht ohne Beurteilung der geplanten Datennutzung geprüft werden. Die Überwachung stellt gleichzeitig eine Modalität (extensiv, intensiv) der Erhebung selbst dar, so dass bestimmte Formen gemessen an den entgegenstehenden Rechten der Betroffenen bereits ihrer Eingriffsintensität nach ohne Rücksicht auf den Erhebungszweck unzulässig sind. Es ist insbesondere Folgendes denkbar:

Der Betroffene könnte ein Kritiker des Unternehmens sein. In diesem Fall ist neben dem Persönlichkeitsrecht die Meinungsfreiheit (Art. 5 Abs. 1 Satz 1, 1. Alt. GG) zu beachten. Es ergibt sich die Situation, dass sich auf beiden Seiten der Abwägung von Art. 5 GG geschützte Rechtsgüter gegenüberstehen, nämlich die (passive) Rezipientenfreiheit bei der verantwortlichen Stelle und, neben dem regelmäßig mitbetroffenen Recht auf informationelle Selbstbestimmung, die Meinungsäußerungsfreiheit auf Seiten des Betroffenen. Beide Grundrechtspositionen unterliegen derselben Schranke: Sie finden ihre Grenzen in den allgemeinen Gesetzen (Art. 5 Abs. 2 GG), grundsätzlich also ineinander. Eine Rangfolge der Grundrechte ist den einzelnen Modalitäten von Art. 5 GG nicht zu entnehmen. Dies ist vorliegend unproblematisch, da die Schutzbereiche der in Rede stehenden Einzelgrundrechte jeweils abweichen und eine gestufte Abwägung unter Berücksichtigung der tendenziell verarbeitungsfreundlichen Vorgaben von § 28 Abs. 1 Satz 1 Nr. 3 BDSG je nach der Schwere der jeweiligen Betroffenheit möglich ist.

Nach Ansicht des Bundesverfassungsgerichts beinhaltet jede Erhebung zur Profilbildung eine latente Gefahr für die Freiheit des offenen gesellschaftlichen Diskurses.[181] Auf die Bedeutung der Anonymität für die Äußerung von Kritik ohne Furcht vor Repressionen wird insbesondere im Zusammenhang mit der grundsätzlichen Verpflichtung von Telediensteanbietern zum Angebot ihrer Dienste in anonymisierter Form (§ 13 Abs. 6 TMG) immer wieder hingewiesen.[182] Diese grundsätzliche Nichtbestimmbarkeit im Online-Bereich soll nach der Vorstellung des Datenschutzrechts auch nicht durch Profilbildung umgangen werden. Dies gilt insbesondere, wenn die Erhebung durch die Namhaftmachung und Charakterisierung von Kritikern die Bekämpfung von Kritik vorbereiten soll. Nach alledem unterliegt die systematische „Verfolgung" des Social-Media-Streams von Kritikern eines Unternehmens erhöhten Rechtfertigungsanforderungen, wobei sich je nach Vorverhalten des Kritikers eine abgestufte Abwägung ergibt. Es sind Wertungen des Äußerungsrechts mit in die Abwägung einzubeziehen.

Unzulässig dürfte eine solche gezielte Überwachung trotz allgemeiner Zugänglichkeit der Quelle und ungeachtet des verfolgten Zwecks regelmäßig sein, wenn die folgenden Voraussetzungen erfüllt sind: Die Äußerungen des Betroffenen richten sich erkennbar an spezifisch benannte Dritte, bzw. einen Freundeskreis, die Äußerungen des Betroffenen haben sich in der Vergangenheit im Rahmen der Meinungsfreiheit gehalten (Insbesondere wurde keine auf bloße Diffamierung ausgerichtete Schmähkritik geübt.) und enthalten keine falschen Tatsachenbehauptungen, wobei im Fall der Vermischung von Meinung und Tatsache grundsätzlich eine Meinungsäußerung zu unterstellen ist.

[181] BVerfGE 65, 42f.

[182] Zuletzt BGH, NJW 2014, S. 2276.

Umgekehrt gilt, dass ein Betroffener, der die verantwortliche Stelle gezielt mit äußerungsrechtlich unzulässigen Beiträgen angreift und sich dadurch absichtlich exponiert, auch bei intensiveren Eingriffen in sein Persönlichkeitsrecht wie dem in Rede stehenden, hinsichtlich dieses Persönlichkeitsrechts nicht schutzwürdig ist.

Für den Fall der Beleidigung (§ 185 StGB), also der Äußerung, die dem CRM-Betreiber den persönlichen Geltungsanspruch (die Ehre) absprechen, liegt die Hürde zur Eingriffsbefugnis hoch. Personengemeinschaften (OHG, KG, GbR) sind nur dann unter einer Kollektivbezeichnung beleidigungsfähig, soweit sie eine anerkannte, gesellschaftliche oder wirtschaftliche Aufgabe oder soziale Funktion erfüllen und einen einheitlichen Willen bilden können, gleichgültig in welcher Rechtsform sie existieren.[183] Auch inhaltlich müssen an die Feststellung einer Beleidigung hohe Anforderungen gestellt werden. Diese Hürden sind höher anzusetzen als bei einer natürlichen Person, da ein Unternehmen erstens durch die Teilnahme am Wirtschaftsleben nicht in der Intimsphäre getroffen werden kann, und ihm zweitens keine Menschenwürde zukommt, welche traditionell den Kern des strafrechtlichen Ehrschutzes darstellt.

Praktisch relevanter ist die Reaktion auf die Gesellschaft schädigende und nicht erweislich wahre, bzw. erweislich falsche, Tatsachen (§§ 186, 187 StGB). Tatsachen sind Aussagen über die physikalische Welt, konkrete Geschehnisse oder Zustände der Vergangenheit oder Gegenwart, die dem Beweis zugänglich sind.[184] Meinungen sind hingegen nach Auffassung des Bundesverfassungsgerichts (auch tatsachenhaltige) Äußerungen, welche durch die „Elemente der Stellungnahme, des Dafürhaltens oder Meinens geprägt sind".[185] Falsche Tatsachenbehauptungen sind nicht von der Meinungsfreiheit gedeckt.

Die Interpretation von Tatsachen zu Ungunsten des CRM-Betreibers kann nicht ohne weiteres als unzulässige Tatsachenbehauptung interpretiert werden. Es gilt, dass im Zweifelsfall eine (zulässige) Meinungsäußerung vorliegt, wobei die Aussage stets im Kontext zu betrachten ist. Verbreitet der Betroffene hingegen erweislich unwahre Tatsachen, sind diese durch seine Meinungsfreiheit auch dann nicht gedeckt, wenn er sie für wahr hält.

2.4.4.2 Interesse des Betroffenen

Das Interesse des Betroffenen, von der Erhebung seiner Daten freizubleiben, muss nach außen treten, denn die verantwortliche Stelle kann ohne deren Erkennbarkeit die gegen die Erhebung sprechenden Gesichtspunkte nicht in die Abwägung miteinbeziehen. Wegen der Ausgestaltung von § 28 Abs. 1 Satz 1 Nr. 3 BDSG als Evidenzkontrolle gilt das Offenkundigkeitskriterium sowohl für die Erkennbarkeit des Schutzbedürfnisses als auch für dessen Überwiegen gegenüber dem Informationsinteresse des CRM-Betreibers.[186] Daher ist die verantwortliche Stelle lediglich zu einer summarischen Prüfung verpflichtet

[183] BGH NJW 1971, S. 1655; OLG Karlsruhe AfP 1998, S. 72; OLG Nürnberg NJW-RR 2003, S. 40 ff.; Damm/Rehbock, Widerruf, Unterlassung und Schadenersatz in den Medien, Rn. 401.

[184] BVerfG, NJW 2003, S. 661; BGHSt 12, S. 291; BGH, JR 1977, S. 29; BGH, NJW 1994, S. 2615; BGH, NJW 2010, S. 761; RGSt 55, S. 131; Lackner, in: Lackner, StGB, § 186 StGB, Rn. 3; Eisele/Lencke, in: Schönke/Schröder, StGB, § 186, Rn. 3.

[185] Vgl. BVerfGE 42, 163; 60, 234; 93, 294; s. auch EGMR NJW 1987, S. 2143.

[186] Gola/Schomerus, BDSG, § 28, Rn. 31.

und muss nur solche entgegenstehenden Interessen berücksichtigen, die sich jedem vernünftigen Beobachter unmittelbar aufdrängen.[187]

Der Form nach muss sich das Interesse des Betroffenen nicht notwendigerweise in einem ausdrücklichen Widerspruch manifestieren, vielmehr genügt ein offenkundiges Schutzbedürfnis, welches sich unmittelbar aus der Gestaltung „seiner" Inhalte aus einem sozialen Medium ergibt. Die folgenden Fallgruppen sollen eine erste Einordnung ermöglichen. Es dürften sich allerdings wegen der verarbeitungsfreundlichen Vermutungsregel in § 28 Abs. 1 Satz 1 Nr. 3 BDSG nur in Einzelfällen weitere *fallgruppenartige* Ausschlussgründe finden lassen.

Der stärkste Indikator, dass ein der Verarbeitung entgegenstehendes Interesse besteht, ist der Widerspruch des Betroffenen. Dieser würde im Falle seines Zugangs gemäß § 28 Abs. 4 BDSG sogar die Folgen einer Einwilligung beseitigen und so mittelbar die Anwendung gesetzlicher Tatbestände sperren. Er muss daher erst recht im Rahmen von Interessenabwägungen Platz greifen, durch die unmittelbar die Anwendung von Erlaubnisnormen gesperrt wird.

Ein solcher Widerspruch ist nicht schon wegen etwaigen widersprüchlichen Verhaltens des Betroffenen unbeachtlich, insbesondere nicht deswegen, weil der Betroffene zwar sein Profil für natürliche Personen zugänglich macht, aber einer technisch möglichen Datenerhebung widerspricht. Die Freiheit des Betroffenen, grundsätzlich selbst über seine persönlichen Daten zu bestimmen, umfasst die Freiheit, diese zwar zu veröffentlichen, sie aber trotzdem gegen alle oder bestimmte Formen der automatisierten Datenverarbeitung, die Gegenstand des Bundesdatenschutzgesetzes ist, zu schützen. Gegenüber einem solchen, nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG unübersehbar hervortretenden Wunsch hat das Informationsinteresse der verantwortlichen Stelle zurückzustehen. Fraglich ist, welche Formen des Widerspruchs bei einer summarischen Prüfung durch den CRM-Verantwortlichen beachtlich sind.

Zunächst wird vorausgesetzt, dass ein etwa verwendeter Crawler den freiwilligen Robots Exclusion Standard respektiert, dass er also Vorhandensein und Inhalt der sogenannten robots.txt-Datei im Stammverzeichnis einer Plattform prüft und sich an die dort gegebenenfalls angegebenen Beschränkungen zur automatischen Indexierung einzelner Profile hält.[188] Dasselbe gilt für das HTML-Metaelement „noindex", das ebenfalls eine Aufforderung an einen Crawler darstellt, die betreffende Website nicht zu indexieren. Der Kreis der verbleibenden Profile wird damit wesentlich enger sein.

Viele sozialen Netzwerke bieten benutzerseitig die Einstellung an, die Indexierung durch Suchmaschinen für das eigene Profil auszuschließen. Dies ist eine klare und eindeutige Willensbekundung im Sinne der Datenschutzrichtlinie, von Erhebungen durch Dritte auf automatisiertem Wege freizubleiben. [189] Ein Crawler, der, was technisch unproblematisch ist, diese Standards ignoriert, gilt als *rogue* und daher als unseriös. Dasselbe gilt für etwaige Benutzereinstellungen zum Ausschluss sonstiger Clients, mit denen sich ein Datenstrom verfolgen und auswerten lässt. Solche Software muss in der Lage sein, serverseitige Hinweise auf einen Widerspruch des Benutzers zu erkennen und sich nach ihnen zu richten. Der CRM-Betreiber muss sich daher mit den jeweiligen Beschränkungen der API der Plattform und deren sonstiger

[187] Ambs, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 28 BDSG, Rn. 9.

[188] Zu den Hintergründen siehe Sieber, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 1, Rn. 103.

[189] Vgl. im Umkehrschluss OLG Köln, MMR 2011, S. 323.

Architektur beschäftigen, damit die verwendete Software auch hinter der vollständigen Sperrung des Profils zurückbleibende Privacy-Einstellungen erkennt und respektiert.

Eine Aussage in Profilen und Postings selbst, die ausdrückt, dass trotz der allgemeinen Zugänglichkeit eine Verarbeitung der Daten nicht erwünscht ist, ist dagegen nur dann erheblich, wenn sie besonders „ins Auge springt". Das kann, muss aber nicht der Fall sein, wenn durch die Verwendung von plattforminternen Zeichen ausdrücklich ein Dritter angesprochen wird. Bei Twitter entspricht eine solche direkte Ansprache etwa dem @-Zeichen, gefolgt von dem Benutzernamen des Angesprochenen.

Es dürfte in solchen Fällen auf die Öffentlichkeit der Diskussion ankommen, für die sich etwa bei Twitter Hinweise in den Metadaten des jeweiligen Datensatzes finden. Handelt es sich beispielsweise um eine von vielen Antworten auf eine Aussage eines Multiplikators auf dem sozialen Netzwerk, so handelt es sich regelmäßig um einen Beitrag zu einer öffentlichen Diskussion, bei der keine überwiegenden Interessen des Betroffenen festzustellen sind. Ähnlich liegt es etwa in einem Forum, in dem über ein Produkt des CRM-Betreibers gesprochen wird. Zwar beziehen sich Postings normalerweise direkt auf einzelne Beiträge im Thread, dies impliziert jedoch keine vertrauliche Ansprache. Handelt es sich bei der direkten Ansprache von Freunden dagegen erkennbar nicht um eine größere Diskussion, so spricht einiges dafür, dass an eine Außenwirkung nicht gedacht war und gegebenenfalls das Risiko einer rechtswidrigen Datenerhebung im Raum steht. Im Zweifel ist eine öffentliche Diskussion anzunehmen. Die etwaige vertrauliche Natur muss ohne besondere Schwierigkeit zu identifizieren sein.

Weiterhin kommt ein überwiegendes Interesse des Betroffenen in Betracht, wenn er einer Personengruppe angehört, die wegen ihrer Unerfahrenheit oder einer aus anderen Gründen mangelnden Einsichtsfähigkeit schützenswert ist. Die praktisch wichtigste Gruppe dieser Art stellen Kinder und Jugendliche dar. Grundsätzlich gilt, dass wer mangels Einsichtsfähigkeit nicht in der Lage ist, eine datenschutzrechtliche Einwilligung abzugeben, ohne Einschaltung der Erziehungsberechtigten erst recht nicht Betroffener einer einwilligungsfreien Datenverarbeitungsmaßnahme sein kann.[190] Da die Einsichtsfähigkeit allerdings nicht mit der Geschäftsfähigkeit deckungsgleich ist, und insbesondere nicht an ein bestimmtes Alter geknüpft ist, kann die Abgrenzung im Einzelnen schwierig sein.[191]

Grundsätzlich gilt, dass ein CRM-Betreiber, welcher die Inhalte von Profilen von sozialen Netzwerken erheben will, sicherstellen muss, dass in dem Fall, in dem ein Profilinhaber ein Geburtsjahr zur Verfügung stellt, dieses ausgelesen wird, und zwar derart, dass das Datum unverzüglich gelöscht wird, falls die Einsichtsfähigkeit verneint werden muss. Ein Problem liegt in der Zuverlässigkeit der erhobenen Angaben. Oft werden Geburtsjahre auf sozialen Medien, sei es zum Selbstschutz, aus Eitelkeit oder zur Erlangung gewisser Privilegien und Zugangsrechte, falsch angegeben, und zwar sowohl in Form der Erhöhung als auch der Verringerung des tatsächlichen Alters. Eine solche Falschangabe kann jedoch nach der Abwägungsstruktur der Norm nicht ohne weitere Anhaltspunkte angenommen werden, die Richtigkeit des Datums darf daher in der Regel angenommen werden. Betroffene Nutzer sind nach § 33 BDSG ohnehin zu benachrichtigen, auf diesem Wege kann, gegebenenfalls durch die Erziehungsberechtigten, interveniert werden.

---

[190] Ausf. Jandt/Roßnagel, MMR 2011, S. 638 ff.

[191] Jandt/Roßnagel, MMR 2011, S. 639 f.

Es empfiehlt sich trotz der o.g. Schwierigkeiten die geschäftsinterne Festlegung eines bestimmten Alters, bei dessen Unterschreitung Profile nicht ausgewertet werden dürfen. Wenn der CRM-Betreiber sichergehen will, dass die Datenerhebung nicht an der Schutzwürdigkeit des Betroffenen aus Altersgründen scheitert, muss er prüfen, ob der Profilinhaber nach eigenen Angaben das achtzehnte Lebensjahr vollendet hat. Die Festlegung einer niedrigeren Altersgrenze wird im Einzelfall zulässig sein, wenn mit der Erhebung kein Zweck verfolgt wird, vor dem das Gesetz besonders schützen will, so etwa die automatische Entscheidung nach Profilbildung (§ 6a BDSG) oder das Scoring (§ 28b BDSG).

Bei geistig behinderten oder ansonsten in ihrer intellektuellen Entwicklung eingeschränkten Betroffenen ist eine Erhebung von Angaben ihres entsprechenden Gesundheitszustands regelmäßig nach §§ 28 Abs. 6-8, 3 Abs. 9 BDSG unzulässig.[192] Es muss daher besonders darauf geachtet werden, dass etwaige Erkenntnisse dieser Art aus den CRM-Datenbanken gelöscht werden, sobald sie zur Erkennung des Ausschlussgrundes verarbeitet wurden. Da solche Einschränkungen auf sozialen Webseiten jedoch üblicherweise nicht offenbart werden, wird der Umstand einer geistigen Behinderung in der Praxis nur selten in einer Deutlichkeit erkennbar sein. Es ist regelmäßig nicht geboten, die Profile etwa mit einer Liste von in Frage kommenden Gesundheitsproblemen zu vergleichen.

Es mögen noch weitere Fallgruppen existieren, in denen im Rahmen der summarischen Prüfung eine Schutzwürdigkeit festgestellt werden muss. Darüber hinaus gilt, dass, im Interesse der Compliance im Zweifel eine Erhebung zu unterlassen ist, wenn ein verwendetes Werkzeug bei der Vorprüfung weitere unternehmensintern festgelegte Faktoren auffindet, die für eine Schutzwürdigkeit sprechen.

2.4.5 Das nicht allgemein zugängliche Datum (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG)

Ist das zu erhebende Datum nicht allgemein zugänglich, so ist der Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 3 BDSG unanwendbar. Ein Monitoring kann daher nur nach dem strengeren § 28 Abs. 1 Satz 1 Nr. 2 gerechtfertigt werden. Danach ist das Erheben personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Auch die Anwendbarkeit von § 28 Abs. 1 Satz 1 Nr. 2 BDSG wird von der Literatur für den Fall, dass ein Vertragsverhältnis besteht, bezweifelt. Mit Hinblick auf den Normzweck von § 28 BDSG, der in der Beschränkung der Handlungsalternativen der verantwortlichen Stelle läge, wird gelegentlich eine Sperrwirkung des § 28 Abs. 1 Satz 1 Nr. 1 BDSG angenommen. Bei § 28 Abs. 1 Satz 1 Nr. 2 BDSG kommt hinzu, dass der strenge Begriff der Erforderlichkeit dafür spricht, dass Nr. 2 als Auffangnorm bereits nach der gesetzlichen Vorstellung ergänzend zu § 28 Abs. 1 Satz 1 Nr. 1 BDSG für nicht berücksichtigte, atypische und zwingende Interessenlagen auch innerhalb von Vertragsverhältnissen heranzuziehen ist.

Der Begriff der „berechtigten Interessen" entspricht demjenigen in § 28 Abs. 1 Satz 1 Nr. 3 BDSG. Es sind auch hier sowohl wirtschaftliche als auch rechtliche und ideelle Interessen denkbar. Im Gegensatz zu § 28 Abs. 1 Satz 1 Nr. 3 BDSG findet sich hier als Rechtmäßigkeitsvoraussetzung das Kriterium der Erforderlichkeit. Die datenschutzrechtliche Literatur verlangt im nichtöffentlichen Bereich keine absolute Alternativ-

[192] Gola/Schomerus, BDSG, § 3, Rn. 56a.

losigkeit der Erhebung zur Verwirklichung des berechtigten Interesses, sondern nur, dass Alternativen zu der konkreten Erhebung der verantwortlichen Stelle nicht zumutbar sein dürfen.[193] Dies bedeutet, dass die Erhebung jedes Datums rechtfertigungsbedürftig ist und die Erhebung zu vieler Datenkategorien, oder von Daten über einen für die Erreichung des Zwecks nicht strikt relevanten Zeitraum, rechtswidrig ist.

Die Abwägung ist derart ausgestaltet, dass sich das Ausschlussinteresse des Betroffenen bereits dann durchsetzt, wenn ein Grund zur Annahme besteht, dass sein schutzwürdiges Interesse am Ausschluss der Verarbeitung oder Nutzung dasjenige der verantwortlichen Stelle überwiegt. Dies ist darin begründet, dass der verantwortlichen Stelle anders als in § 28 Abs. 1 Satz 1 Nr. 3 BDSG hier keine generell grundrechtlich geschützte Position zukommt, da wegen der fehlenden allgemeinen Zugänglichkeit das Grundrecht der Rezipientenfreiheit (Art. 5 Abs. 1 Satz 1, 2. Alt. GG iVm Art. 19 Abs. 3 GG) nicht greift. Dies schließt nicht aus, dass die verantwortliche Stelle nicht im Einzelfall andere Grundrechtspositionen (insbesondere die Berufsausübungsfreiheit nach Art. 12 GG und das von Art. 14 GG geschützte Recht auf den eingerichteten und ausgeübten Gewerbebetrieb) geltend machen kann.

Abzustellen ist also auf den Erhebungszweck. Eine Schwierigkeit ergibt sich für den Betroffenen daraus, dass er den ohne seine Kenntnis festgesetzten Erhebungszweck in der Regel nicht erkennen kann und sich daher sein entgegengesetztes Interesse häufig nicht manifestieren kann.

Es macht jedoch gerade den Unterschied zwischen der Abwägung nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG und derjenigen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG aus, dass eine solche Manifestation in der Regel nicht erforderlich ist. Es handelt sich bei § 28 Abs. 1 Satz 1 Nr. 2 BDSG nämlich im Gegensatz zu § 28 Abs. 1 Satz 1 Nr. 3 BDSG nicht um ein summarisches, sondern um ein umfassendes Abwägungserfordernis. Das bedeutet, dass im Falle einer Erhebung auf Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 BDSG die verantwortliche Stelle die für sie erkennbaren möglichen Interessen des Betroffenen selbständig in die Abwägung einbringen muss. Dabei ist nach dem Wortlaut („Grund zur Annahme“) ausreichend, dass überwiegend wahrscheinlich ist, dass das zu unterstellende Interesse tatsächlich von dem Betroffenen geteilt wird.

Im Rahmen des Social CRM ist zunächst danach zu unterscheiden, ob eine durch den Nutzer selbst erteilte Berechtigung der verantwortlichen Stelle zur Kenntnisnahme der betreffenden Daten vorliegt. Es macht einen Unterschied in der Abwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, ob die verantwortliche Stelle Daten unmittelbar aus für sie rechtlich oder tatsächlich gesperrten Quellen erlangt, oder ob sie sich aus Quellen informiert, die zwar für sie zugänglich sind, aber ansonsten einer personenbezogenen Zugangskontrolle unterliegen (z.B. geschützte Twitter-Profile individueller Nutzer, die „Follower“ des CRM-Betreibers sind). Solche Sperren können tatsächlicher (z.B. Passwort) oder rechtlicher Natur sein. Im ersteren Fall müsste die verantwortliche Stelle den Zugang zu den Daten widerrechtlich erlangen, wobei sie zur Überwindung technischer Sperren regelmäßig gemäß § 202a StGB strafbar handeln müsste. Ein solches Vorgehen kann datenschutzrechtlich nicht gerechtfertigt werden. Der Bundesgerichtshof hatte im Rahmen einer Strafsache zu entscheiden, in welchem Fall aus einer für die verantwortliche Stelle rechtlich unzugängliche Quelle (hier: unzulässig erhobene Bewegungsdaten) strafrechtlich rechtmäßig erhoben

[193] BGH, NJW 1986, S. 2505; Scheja/Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 5, Rn. 132.

werden darf.[194] Dabei griff er auf die Rechtsprechung des Bundesverfassungsgerichts zum Mitschnitt des gesprochenen Worts[195] zurück. Die in den hier in Rede stehenden Fällen zu erhebenden Daten dienen in der Regel erst der Bestimmung des Betroffenen und sind daher häufig nicht so einschneidend wie ein zur Beweisführung gesammeltes Bewegungsprofil oder der Mitschnitt von Telefongesprächen bereits bestimmter Personen. Wegen des gleichermaßen vorhandenen Rechtsbruchs durch die verantwortliche Stelle kann die Entscheidung allerdings entsprechend herangezogen werden:

Danach muss der Erhebung der nicht zugänglichen Daten ein existenzbedrohender Angriff des Betroffenen auf die Rechtsposition der verantwortlichen Stelle vorausgegangen sein, so dass der verantwortlichen Stelle in ihrer „notwehrähnlichen Situation" kein anderes Mittel als die rechtswidrige Handlung zur Verfügung stand. Folge ist zwar nicht die datenschutzrechtliche Rechtmäßigkeit der Erhebung, wohl aber eine strafrechtliche Rechtfertigung mit der Folge, dass die verantwortliche Stelle gegebenenfalls Sanktionen entgehen kann. Diese wiederum kann sich maßgeblich auf die Abwägung im Rahmen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG auswirken.

Am Kriterium der Erforderlichkeit wird eine solche Form der Notwehr aber regelmäßig scheitern. Handelt es sich bei dem Betroffenen nämlich um den Nutzer eines sozialen Netzwerks, bei welchem konkrete Anhaltspunkte den Verdacht begründen, dass er durch ein geschlossenes Profil strafrechtlich unzulässige Äußerungen gegen die verantwortliche Stelle tätigt, wäre Strafanzeige zu stellen. Die Staatsanwaltschaft ist nach Maßgabe von § 14 Abs. 2 TMG in der Lage, die personenbezogenen Daten des Betroffenen zwecks Identifizierung zu erheben. Da § 14 Abs. 2 TMG hinsichtlich Auskunftsbegehren an den Telemedienanbieter über die Bestandsdaten einzelner Nutzer abschließend ist, hat die verantwortliche Stelle keinen eigenen Anspruch gegen den Telemedienanbieter auf Auskunft über die Identität des Täters.[196] Umso weniger ergibt sich, etwa unter dem Aspekt eines rechtfertigenden Notstands (§ 34 StGB) die Befugnis der verantwortlichen Stelle, sich unbefugt Zugang zu den betreffenden Daten zu verschaffen.

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG rechtfertigt im Social CRM insoweit insbesondere die Erhebung in Fällen, in denen zumindest die verantwortliche Stelle, ohne dass sie hierfür wie bei Facebook eine gesonderte Einwilligung benötigt, autorisiert ist, die betreffenden Daten zu erheben. Die Differenzierung nach der Autorisierung der verantwortlichen Stelle bringt es zudem mit sich, dass die Erhebung für gewisse kommerzielle Zwecke auch von „halbzugänglichen" Daten nicht grundsätzlich ausgeschlossen ist, wobei der legitime Verarbeitungszweck zusammen mit der den Betroffenen schützenden Abwägungsdogmatik von § 28 Abs. 1 Satz 1 Nr. 2 BDSG den Maßstab darstellt. Dies entspricht der vom EuGH vertretenen Ansicht, nach der es europarechtswidrig wäre, die allgemeine Interessenabwägung auf Fälle allgemeiner Zugänglichkeit zu beschränken.[197] Fehlt diese, ist in der Abwägung der Vermutung Rechnung zu tragen, dass die vertrauliche Behandlung seiner Daten dem manifestierten Willen des Betroffenen entspricht. Gleichzeitig liegt in der Tatsache, dass die verantwortliche Stelle etwa auf der Freundesliste eines Nutzers steht, nicht etwa das (gegenüber der allgemeinen Zugänglichkeit) konkretisierte Wohlwollen des Betroffenen ge-

194 BGH, Urt. v. 04.06.2013, 1 StR 32/12.

195 BVerfG, Beschl. v. 09.10.2002, BVerfGE 106, 28.

196 Gegen einige Instanzgerichte so nun auch BGH, Urt. v. 1.7.2014, VI ZR 345/13.

197 EuGH, Urt. v. 24.11.2011, verb. Rs. C-468/10 und C-469/10.

genüber einer Erhebung seiner Daten. Vielmehr ist der „Fan" eines Unternehmens in der Regel zunächst ausschließlich an den auf der Unternehmensseite geposteten Inhalten interessiert. Dies ist bei der Interessenabwägung zu berücksichtigen.

Die Differenzierung zwischen allgemein zugänglichen und nicht allgemein zugänglichen Daten erfordert, in jedem Fall die zu erhebenden Daten zu überprüfen, ob sie von einem geschützten Profil stammen oder nicht. Die folgenden Ausführungen beziehen sich nur auf geschützte Profile, wobei eine Beurteilung der Rechtmäßigkeit der Erhebung in der Regel nur mit Blick auf den Verarbeitungszweck im Einzelfall geschehen kann.

Da jeder Grund zur Annahme, das schutzwürdige Interesse des Betroffenen überwiege, ausreicht, um die Datenerhebung rechtswidrig zu machen, sind auch andere Formen der Auswertung von Persönlichkeitsmerkmalen aus nicht allgemein zugänglichen Daten als eine Form von Zweckentfremdung grundsätzlich unzulässig. So ist eine Datenerhebung, die auch nur nebenbei ein personenbezogenes Profil entstehen lässt, nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG rechtswidrig, soweit diese nicht schon an der Zweckbindung und der damit zusammenhängenden Erforderlichkeit scheitert.

Ein weiterer Ausschlussgrund ergibt sich unmittelbar aus der Nichtöffentlichkeit des Accounts des Betroffenen. Wenn der „Fan" oder „Follower" eines Unternehmens seine Beiträge gegenüber Dritten unsichtbar sind, spricht dies regelmäßig dafür, dass diese Beiträge auf den von ihm gewählten Kreis beschränkt bleiben soll. Dieses Interesse steht einer Übermittlung des CRM-Verantwortlichen an Drittunternehmen genauso entgegen wie der Mitteilung von Inhalten an Dritte etwa in Form eines ungeschützten „Retweets".

Denkbar ist hingegen, dass ein überwiegendes schutzwürdiges Interesse nicht vorliegt, wenn der betreffende Datensatz frühestmöglich anonymisiert wird (§ 3a Satz 2 BDSG). Die Festlegung eines Verwendungszwecks ausschließlich zur anonymen Verarbeitung bietet der verantwortlichen Stelle die größte Gewähr, dass eine Verarbeitung der Daten nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG nicht die Rechte des Betroffenen verletzt, und daher kein entgegenstehendes überwiegendes Interesse die Erhebung rechtswidrig macht.

Zwar liegt in solchen Fällen für den Zeitraum vor der erfolgten Anonymisierung ein Personenbezug vor. Wenn durch eine geeignete Form der Anonymisierung die Bestimmbarkeit aufgehoben wird, ist es aber bei Verfolgung eines nichtwerblichen Erhebungszwecks denkbar, dass die Erhebung zulässig ist. In solchen Fällen wird der Erhebung nämlich in der Regel nachträglich die Eignung entzogen, überhaupt einen Grundrechtseingriff auszulösen. Das Bundesverfassungsgericht[198] hat entschieden, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung durch Erhebung personenbezogener Daten nachträglich (ex tunc) beseitigt werden kann, wenn die bei der Erhebung erlangten Daten sofort und spurenlos gelöscht werden. Die hier begutachtete Herstellung von Anonymität ist nicht unmittelbar mit der in o.g. Entscheidung behandelten Löschung von Daten vergleichbar, da gerade eine Weiternutzung stattfindet. Vorliegend bewirkt die Anonymisierung eine Unanwendbarkeit des BDSG auf den aggregierten Datensatz jedenfalls ex nunc, sobald die Merkmale, die einen Personenbezug herstellen können, nach dem sich

[198] BVerfGE 120, 378.

sofort an die Erhebung anschließenden Aggregationsvorgang nicht mehr vorhanden sind.[199] Eine Datenverarbeitung, die eine Bestimmbarkeit des Betroffenen dauerhaft ausschließt, kann mit Blick auf die Interessen der Betroffenen in deutlich größerem Umfang nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein. Weitere Rechtmäßigkeitskriterien werden im Kapitel 2.6 besprochen.

2.4.6 Der Datenkauf

Auch wenn moderne CRM-Systeme das Monitoring zunehmend in die Hände des CRM-Betreibers selbst legen, ist die Branche der Daten-Broker weiterhin von großer, oft gegenüber dem unternehmenseigenen Monitoring dominierender wirtschaftlicher Bedeutung. Die Datenhandel-Industrie bietet zahlreiche Produkte an, die das gesamte Spektrum der Verarbeitung von Daten abdecken. Dieses reicht von reinen, nur nach Suchworten gefilterten Kopien der Posting-Ströme sozialer Medien bis hin zu umfassenden und komplexen Kundenprofilen, die aus unterschiedlichen Quellen aggregiert werden. Zu untersuchen ist, wie sich der Umstand, dass eine andere Instanz die primäre Datenerhebung durchführt, sich auf die Zulässigkeit der Weiterverarbeitung der Daten durch die verantwortliche Stelle auswirkt.

Von primärer Bedeutung ist, ob eine Form der Auftragsdatenverarbeitung vorliegt. Dies wird für den klassischen Adresshändler („Lettershop") allgemein verneint, da dieser über seinen Adressbestand selbständig verfügt und Adressen mehrfach verkauft, so dass keine ausschließliche Verfügungsbefugnis der verantwortlichen Stelle vorliegt[200].

Für den vorliegenden Fall ist zu differenzieren: Liegen die zu erhebenden Daten bereits vor und besteht die einzige verbleibende Tätigkeit des Datenbrokers in der Filterung und der Übergabe an die verantwortliche Stelle, so wird § 11 BDSG unanwendbar sein. Der Databroker handelt in eigener Verantwortung. Werden die Daten dagegen erst nach Erteilung eines (längerfristigen) Auftrages erhoben, so dürfte eine Auftragsdatenverarbeitung vorliegen. Daraus folgt dann die Pflicht zum Abschluss eines Vertrages nach § 11 BDSG, mit der Folge, dass im Falle seiner Wirksamkeit in der Weitergabe an die verantwortliche Stelle keine Übermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG liegt. Da sich § 11 BDSG ausweislich seines Wortlauts ausdrücklich auf das Outsourcing von Erhebungsvorgängen erstreckt, ist es für die Feststellung seiner Anwendbarkeit unschädlich, dass vorliegend keine Daten der verantwortlichen Stelle verarbeitet werden.

Was den Rückgriff auf präexistente Datensammlungen angeht, so ist daran zu erinnern, dass die Erhebung von Daten ohne Festlegung eines konkreten Erhebungszwecks im EWR unzulässig ist (Art. 6 Abs. 1 b) DSRL, § 29 Abs. 1 Satz 2 i.V.m. 28 Abs. 1 Satz 2 BDSG im Bundesrecht). Das Bundesverfassungsgericht hat in diesem Zusammenhang ausgeführt, dass „die Speicherung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" nicht mit dem Grundrecht auf informationelle Selbstbestimmung zu vereinbaren ist.[201] Die Zweckfestlegung „Weitergabe an später zu bestimmende Vertragspartner zu von diesen festzulegenden Zwecken" ist daher nicht ausreichend bestimmt, weil völlig offen ist, wel-

[199] Vgl. Bergmann/Möhrle/Herb, BDSG, § 3, Rn. 128 ff.; Heidrich/Wegener, MMR 2010, S. 806.

[200] Umfassende Ausführungen zur Auftragsdatenverarbeitung in 2.2.2 Auftragsdatenverarbeitung und Auslandsbezug.

[201] BVerfGE 65, 1 (46).

che (Kategorien von) Empfängern zu welchen Zwecken die Daten empfangen werden.[202] Es handelt sich, selbst wenn Profile erhoben werden sollen, auch nicht um Listendaten im Sinne von § 28 Abs. 3 BDSG, deren Weiterverwendung gegebenenfalls zulässig wäre, da soziale Netzwerke keine „vergleichbaren Verzeichnisse" gemäß § 28 Abs. 3 Satz 2 Nr. 1 BDSG sind und die Daten auch nicht im Rahmen der Geschäftsbeziehung gesammelt wurden.

An der Zweiterhebung und Nutzung rechtswidrig erhobener Daten aber kann kein berechtigtes Interesse im Sinne der § 29 Abs. 2 Nr. 1 BDSG (für die Übermittlung) und 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG (für die Erhebung bei der verantwortlichen Stelle) bestehen. Dasselbe gilt, wenn die verantwortliche Stelle zur Umgehung des Verbots auf einen Datenbroker etwa in den USA zurückgreift, wo der Zweckbindungsgrundsatz nicht greift.[203] Auch hier ist ein berechtigtes Interesse nicht gegeben. Ist der Zweck dagegen hinreichend festgelegt, gelten die allgemeinen Vorschriften.

Hinsichtlich der Aufbereitung von Daten im Auftrag gilt die Regel, dass auch bei Einhaltung der Bestimmungen des § 11 BDSG die Datenerhebung durch Beauftragte nur zulässig ist, wenn die verantwortliche Stelle die Daten auch selbst erheben dürfte. Die wichtigste Konsequenz aus dieser Tatsache besteht darin, dass die oben benannten Sorgfaltspflichten[204] operativ der Auftragnehmerin auferlegt werden müssen, während sie rechtlich bei der verantwortlichen Stelle verbleiben. Damit die verantwortliche Stelle effektiv die Kontrolle ausüben kann, muss sie detaillierte Vorgaben zur Einhaltung der Vorschriften machen, etwa was die Erkennung und Aussonderung von Postings angeht, an deren Ausschluss von der Erhebung ein überwiegendes schutzwürdiges Interesse besteht. Dabei darf die verantwortliche Stelle der Auftragnehmerin nicht die Abwägung selbst überlassen, sondern muss klare Regeln aufstellen, welche die unzulässige Verarbeitung zuverlässig vermeiden. Die Konsequenz ist dabei letztlich, dass der Handlungsspielraum der verantwortlichen Stelle in einem solchen Szenario weiter eingeschränkt wird, als dies bei der „eigenhändigen" Datenerhebung der Fall wäre.

2.5 Die Visualisierung von Zusammenhängen zwischen Nutzern - Social Network Analysis

Typisch für Social Network Analysis ist die Darstellung von Beziehungen zwischen Nutzern in Form eines Netzdiagramms, wobei die Knotenpunkte (Nodes) jeweils die Nutzer darstellen. Ziel ist neben der allgemeinen Analyse der Beziehungen insbesondere die Überwachung der Fortpflanzung von (positiven oder negativen) Nennungen eines Unternehmens oder Produkts über Netzwerke und die Identifizierung von besonders aktiven (intensive Besprechung von Produkten des CRM-Betreibers) oder einflussreichen (besonders viele Freunde, denen Meinungen mitgeteilt werden) Nutzern. So kann die verantwortliche Stelle frühzeitig die virale Verbreitung von Gerüchten und Skandalen („Shitstorm") identifizieren und kontrollieren oder den Erfolg einer eigenen Imagekampagne nachprüfen.

Social Network Analysis-Software kann üblicherweise dahingehend konfiguriert werden, ob ausschließlich das „Freundesnetzwerk" der verantwortlichen Stelle, oder ob zusätzlich andere Freundesnetzwerke,

---

[202] So i.E. auch Ehmann, in: Simitis, BDSG, § 29, Rn. 54 ff.

[203] Spies/Schröder, MMR 2008, S. 279.

[204] Siehe unter 2.4.2.

üblicherweise die der Freunde bzw. Follower des CRM-Betreibers, soweit zugänglich, mitüberwacht werden. Ob Namen oder andere identifizierende Merkmale der Visualisierung hinzugefügt werden, ist ebenfalls eine Frage der benutzten Software und deren Konfiguration. Einige Anbieter ordnen den einzeln dargestellten Nutzern zumindest Namen und Fotos zu. Andere Darstellungen nennen nicht den Namen oder Benutzernamen der Betroffenen. Dennoch wird durch die Visualisierung bisweilen eine Bestimmbarkeit derart hergestellt, dass Äußerungen des Betroffenen eingeblendet werden, die sich mit Hilfe der Suchfunktion des jeweiligen sozialen Netzwerks ohne Weiteres einer bestimmten Person zuordnen lassen. Noch häufiger ist die Darstellung ohne Namensnennung nur ein Anzeigemodus, ein Klick auf den betreffenden Node fördert den Benutzernamen sowie gegebenenfalls andere zur Bestimmung geeignete Daten zutage. Insofern ist Anonymität bei vielen Anwendungen nur scheinbar gegeben. Wieder andere Systeme machen die Bestimmbarkeit schwieriger, indem sie lediglich das Netzwerk darstellen, und an den anonymen Knoten jeweils farblich eine Nennung des gewünschten Keywords visualisieren. Hier könnte zwar bei weitergehender Analyse der genauen Anzahl der Freunde eine Bestimmbarkeit hergestellt werden, aber wenn das Keyword allgemein genug gewählt wird, ist in dieser Phase häufig die Bestimmbarkeit zumindest wesentlich erschwert. Verbreitet ist in diesem Zusammenhang die Praxis, dass in einem automatisierten Schritt durch semantische Analyse der Nachricht eine sog. „Tonalität" errechnet wird, also der Grad, zu welchem eine Aussage positiv oder negativ scheint. Hierbei wird ein Score errechnet, welcher der verantwortlichen Stelle flankierend zu dem Umstand der Nennung mitgeteilt wird, während die Nachricht selbst sofort nach der Datennutzung gelöscht wird.

In rechtlicher Hinsicht ist bei alledem festzustellen, dass eine anonyme Erhebung begrifflich ausgeschlossen ist. Selbst wenn ausschließlich nach der Verbreitung häufig erwähnter Keywords gesucht und auf eine Tonalitätsanalyse verzichtet wird, gilt, dass die Betroffenen, deren Daten erhoben werden, Knoten im dargestellten Diagramm zugeordnet werden müssen. Dies bedingt, dass selbst bei fehlender Beschriftung der Knoten eine Wiedererkennbarkeit gewährleistet werden muss. Es wird daher die Regel sein, dass für die Knoten Pseudonyme im Sinne des § 3 Abs. 6a BDSG gebraucht werden. Es handelt sich zudem notwendig um ein von der verantwortlichen Stelle gewähltes Pseudonym, der Betroffene bleibt damit bestimmbar und das Pseudonym unwirksam, solange eine Zuordnungsfunktion vorliegt. Die Personenbeziehbarkeit ist damit unverändert gegeben. Für Datenverarbeitungen im Rahmen der Social Network Analysis ist folglich stets eine Rechtfertigung erforderlich.

Werden ganze Postings erhoben, ist der Datensatz in aller Regel ohne weiteres personenbezogen, so dass der Umstand der Substitution des Namens keine Rolle spielt. Dies gilt selbst dann, wenn Postings ohne Namen, Fotos oder Zeitangaben erhoben werden, weil die Individualität der Texte den Betroffenen regelmäßig bestimmbar macht. Pseudonymität, also die wesentliche Erschwerung der Bestimmbarkeit,[205] wäre nur dann denkbar, wenn außer der Nennung des Keywords oder etwa der Markierung als Repost einer Originalnachricht keinerlei eigene Zusätze in dem Posting auftauchen, und eine ausreichende Anzahl anderer Nutzer dieselbe Nachricht weitergeleitet haben. Zum Beispiel ist es denkbar, dass eine verantwortliche Stelle die Verbreitung eines von ihr geposteten Links verfolgt. Wenn außer der Tatsache der Weiterverbreitung keine personenbeziehbaren Daten erhoben werden, liegt Pseudonymität vor und die Erhebung ist in der Abwägung zu privilegieren.

[205] § 3 Abs. 6a BDSG.

Erste Voraussetzung für die rechtmäßige Erhebung ist nach alledem, dass alle betroffenen Profile zumindest für die verantwortliche Stelle zugänglich gemacht wurden.[206] Dies ist unproblematisch für allgemein zugängliche Profile der Fall, sofern keine besonderen Umstände für überwiegende Interessen der Profilinhaber sprechen. Für eine Erhebung für die verantwortlichen Stelle einsehbarer, aber nicht allgemein zugänglicher Profildaten, fehlt das überwiegende berechtigte Interesse im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Dies gilt jedenfalls bei der Auswertung technisch nicht verbergbarer Teile von Profilen derjenigen Betroffenen, mit denen die verantwortliche Stelle nicht selbst verknüpft ist, sondern die nur „friend-of-a-friend" sind. Bei Facebook betrifft dies insbesondere Name oder Nickname, Foto und andere Header-Informationen, die mit den verfügbaren Privatsphäre-Einstellungen nicht verbergbar sind. Dies gilt auch dann, wenn wegen frühestmöglicher wirksamer Pseudonymisierung der mit der Erhebung einhergehende Grundrechtseingriff für sich gesehen wenig intensiv sein sollte. Selbst bei wirksam pseudonymisierten Daten geht von ihr ein Aspekt der Verhaltensüberwachung aus, der zu Nachteilen führen kann, wenn, wie oft der Fall, sich eine unmittelbar personenbezogene Überwachung der pseudonymen anschließt. Da dieser weitere Nutzungszweck dieselben erhobenen Daten betrifft, ist er in die Abwägung einzustellen.

Fraglich ist weiterhin, ob die Follower-Listen von Followern, auch wenn sie allgemein zugänglich gemacht wurden, Teil solcher Erhebungen werden können. Hieran bestehen erhebliche Zweifel, da die zunächst miterhobenen Namen personenbezogene Daten von Drittbetroffenen darstellen, die in keinerlei Verhältnis zu dem CRM-Betreiber und seinen Produkten stehen. Zwar sind diese Drittbetroffenen auf der Profilseite des Followers in der Regel nur dann kenntlich, wenn sie dies zugelassen haben. Allerdings dürfte die reine Möglichkeit, dass ein einzelner, bisher nicht in Erscheinung getretener Friend-of-a-Friend etwas beizutragen hat, nur geringes Interesse an der Erhebung oder Auswertung seiner Daten erzeugen, so dass jedenfalls für nachfolgende Nutzungszwecke regelmäßig ein überwiegendes Ausschlussinteresse begründet wird und damit bereits die Erhebung unzulässig ist. Es ist daher zu empfehlen, mit der Social Network Analysis grundsätzlich nur den eigenen Follower-Kreis auszuwerten. Hier ist zunächst auch die Erhebung von Klarnamen und/oder Nicknames denkbar.

Die wichtigere Voraussetzung für die Zulässigkeit der Erhebung ist erneut die Festlegung eines rechtmäßigen Erhebungszwecks.[207] Nur durch ihn kann eine abschließende Beurteilung der Zulässigkeit erfolgen. Nach alledem ist zur Bestimmung der Zulässigkeit im Einzelfall auf die denkbaren Verarbeitungsschritte und Nutzungszwecke einzugehen. Dabei ist fraglich, ob es sich bei den durch Erhebung gewonnenen und
(zwischen-) gespeicherten Daten noch um allgemein zugängliche handelt. Dies ist, die allgemeine Zugänglichkeit der Quelle vorausgesetzt,[208] zumindest dann zu bejahen, wenn das Posting noch als unverändertes Rohdatum vorliegt und eine Verknüpfung mit bisher nicht zusammenhängenden Daten nicht erfolgt ist.[209] Ein solches, isoliert oder im ursprünglichen Kontext gespeichertes, Datum konnte auch von jedem beliebigen Dritten zur Kenntnis genommen werden. Daran ändert nichts, dass gegebenenfalls nur

[206] Gola/Schomerus, BDSG, § 28 Rn. 31.

[207] Becker/Ambrock, JA 2011, S. 561 (563); Gola/Schomerus, BDSG, § 14, Rn. 9.

[208] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 28 BDSG, Rn. 7.

[209] Gola/Schomerus, BDSG, § 28, Rn. 31.

einzelne Teile eines Postings erhoben werden. Diese Daten sind unter diesen Umständen daher noch unter den vereinfachten Bedingungen von § 28 Abs. 1 Satz 1 Nr. 3 BDSG weiterzuverarbeiten.[210]

Im Anschluss wird der Datensatz regelmäßig um nicht benötigte Daten bereinigt. Hierbei handelt es sich nicht um eine Löschung im Sinne des § 3 Abs. 4 Nr. 5 BDSG, weil die Daten regelmäßig noch nicht final gespeichert sind[211], insbesondere noch keinem Nutzungszweck zugewiesen worden sind. Das verbleibende Posting ist sodann nicht mehr als allgemein zugänglich anzusehen.

In einem weiteren Schritt werden Postings möglicherweise semantisch in Form eines Scores ausgewertet, um eine automatisierte Warnung an den CRM-Betreiber durch das System zu ermöglichen. Dies stellt, neben einer Verarbeitung in Form einer Veränderung (§ 3 Abs. 4 Nr. 2 BDSG), die Erhebung eines nicht allgemein zugänglichen Datums dar, da der klar personenbezogene Zahlenwert nur bei der verantwortlichen Stelle verfügbar ist. Rechtsgrundlage für die Verarbeitung ist daher § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Die Bildung eines solchen Werts stellt für sich kein Scoring im Sinne des § 28b BDSG dar, da der errechnete Wert nicht den dort genannten Zwecken dient und auch keine Wahrscheinlichkeit eines bestimmten zukünftigen Verhaltens errechnet wird. Soweit pseudonymisiert worden ist, wird die Bestimmbarkeit des Betroffenen gegenüber der Nutzung des gesamten Postings verringert.[212] In solchen Fällen ist die Scorebildung datenschutzrechtlich zulässig, solange dem Betroffenen keine unangemessenen Nachteile oder rechtlichen Folgen aus der automatisierten Beurteilung erwachsen, § 6a BDSG. Daher sollte einziger Zweck einer solchen Erhebung die Verfolgung der Stimmungslage in Bezug auf das eigene Unternehmen sein. Wenn dargelegt werden kann, dass die Scorebildung hierzu geeignet und erforderlich ist, ist das Vorhaben datenschutzkonform.

Voraussetzung für diese Privilegierung ist weiterhin, dass nach der Auswertung das Posting selbst unverzüglich gelöscht wird.[213] Die Beibehaltung des Postings im Wortlaut führt wegen Verstoßes gegen den Zweckbindungsgrundsatz regelmäßig zum Überwiegen der Betroffeneninteressen.

Die Scorebildung in Bezug auf nicht pseudonymisierte Profile steht unter strengeren Voraussetzungen. Hier muss gerade die Beibehaltung des Klarnamens erforderlich sein. Dies kann z.B. in Fällen der Verteidigung gegen Eingriffe in den eingerichteten und ausgeübten Gewerbebetrieb (§ 823 Abs. 1 BGB bzw. Art. 14 GG) der Fall sein. Abgesehen davon darf die Einschätzung, ob aufgrund des Scores gegen den Betroffenen vorgegangen werden soll, wegen der Erheblichkeit des Eingriffs nur von einer natürlichen Person getroffen werden, § 6a BDSG.

Schließlich findet eine Visualisierung statt. Diese kann in einer Momentaufnahme des Zustands eines Netzwerks nach Abschluss einer Analyse, aber auch in einer Darstellung von Entwicklungen in Echtzeit bestehen. Die personenbezogenen Daten, die dem CRM-Betreiber angezeigt werden, sind in der gegebenen Form nicht allgemein zugänglich, da sie üblicherweise nicht nur die für sich allgemein zugänglichen „Freundeslisten“ darstellen. Die Verbreitung von Äußerungen durch das dargestellte Netzwerk sind

---

[210] Forst, NZA 2010, S. 430.

[211] Vgl. Ambs in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 3 BDSG, Rn. 27.

[212] Gola/Schomerus, BDSG, § 3a, Rn. 10; Roßnagel, DuD 1999, S. 255.

[213] Vgl. Gola/Schomerus, BDSG, § 14, Rn. 20.

nicht ohne weiteres öffentlich einsehbar, sondern im Wege der Verkettung von Zusammenhängen aufdeckt worden, die sich aus den Rohdaten nicht gewinnen lassen. Auch errechnete Scores sind Folge derartiger Verket und damit nicht allgemein zugänglich.

Die weitere Beurteilung von Datenverarbeitungen bei der Visualisierung von Zusammenhängen und Social Network Analysis im Allgemein hängt des Weiteren von den folgenden Einzelaspekte ab.

2.5.1 Pseudonymisierung und Klarnamenbenutzung

Die erste Frage, die zu stellen ist, bezieht sich auf die Bestimmbarkeit von Einzelpersonen. Die Verbindung von Klarnamen mit weiteren Daten (wie Meinungsäußerungen) ist immer rechtfertigungsbedürftig, wenn nicht nach den o.g. Kriterien bei der Visualisierung allgemeine Zugänglichkeit vorliegt. Dies ist nur denkbar bei einer reinen Visualisierung, die über die Darstellung der Freundesliste(n) hinaus keine weiteren Informationen bietet. Eine Netzdarstellung, nämlich die Verbindung von Nutzern untereinander, ist zwar für sich allgemein zugänglich, kann allerdings regelmäßig über die jedermann zugänglichen Einzelinformationen hinausgehende Daten generieren und stellt sich damit als nicht allgemein zugänglich dar.

Die Klarnamenbenutzung muss auch für die Visualisierung erforderlich sein.[214] Auch hier wird auf den Zweck der Erhebung der Netzwerkdaten abzustellen sein. Wenn die Nennung erforderlich ist, um den Betroffenen später anzusprechen, sind die Kriterien zur Ansprache[215] heranzuziehen. Das Verbot werbender Ansprache bei Nichtvorliegen einer Einwilligung ist darüber hinaus erneut zu betonen.[216] Der Zweck des Social Media Monitoring muss insbesondere in der empirischen Feststellung der Stimmungslage bestehen und die gewonnenen Erkenntnisse dürfen nicht unmittelbar für Marketing- oder andere kommunikative Zwecke verwendet werden.[217]

2.5.2 Kunden und Nichtkunden/Follower und Friends-of-Friends

Bei der Abwägung, ob die Visualisierung der Zusammenhänge und Äußerungen von (pseudonymisierten) Kunden und Nichtkunden zulässig ist, ist bereits eine weitere Differenzierung vorgenommen worden, nämlich zwischen Gruppen, die mit dem CRM-Betreiber bereits in Berührung gekommen sind und solchen, die bisher keinen Kontakt mit diesem gehabt haben. Letztere sind im Hinblick auf die fehlende allgemeine Zugänglichkeit der Netzwerkdaten schützenswerter. Eine Abwägung zugunsten der verantwortlichen Stelle, ob die Stellung eines Nutzers im Netzwerk des CRM-Betreibers ausgewertet werden darf, ist regelmäßig nur in Fällen denkbar, in denen eine Vorbefassung zwischen dem Betroffenen und der verantwortlichen Stelle stattgefunden hat.

Hier stellt sich die Frage, ob neben dem bereits genannten plattformbezogenen Attribut „Follower“ noch anhand des geschäftsbezogenen Attributs „Kunde“ zu differenzieren ist, wobei „Follower“ wie oben für

---

214 Ambs in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 13 BDSG, Rn. 2.

215 Siehe Kapitel 2.8.1.

216 Gola/Schomerus, BDSG, § 4a Rn. 4 f.

217 Vgl. OLG Köln, RDV 2009, S. 75; OLG Hamburg, RDV 2009, S. 178.

sämtliche Formen der technisch vorgesehenen, auf Willensbekundung basierenden Verbundenheit auf sozialen Plattformen steht, welche einen privilegierten Zugang zu dem Profil des jeweils anderen ermöglicht (auf anderen Plattformen: Freund, Mitglied eines Kreises usw.).

Es ist hier darauf hinzuweisen, dass die verantwortliche Stelle, um ihre Kunden zu identifizieren, zusätzliche Daten erheben müsste, während sie, wenn sie Daten von den Followern erhebt, dies ohne Rücksicht auf deren Identität tun kann, und oben bereits die potentiell privilegierende Rolle einer wirksamen Pseudonymisierung besprochen wurde. Weiterhin ist etwa eine Einwilligung in die Erhebung des Freundesnetzwerks in der Regel nur anlässlich eines Kontakts zwischen Betroffenem und dem Unternehmen auf dem sozialen Netzwerk selbst möglich, da sie ansonsten überraschend und daher nach dem Recht der Allgemeinen Geschäftsbedingungen regelmäßig unzulässig wäre.[218] Im Übrigen existieren viele Anwendungsfälle des Social CRM, in denen die verantwortliche Stelle keine B2C-Kundenliste führt, weil sie Kaufverträge mit unbestimmten Personenkreisen abschließt oder abschließen lässt. Das bedeutet, dass ihr Produkt so beschaffen ist, dass, wie etwa bei Packungen von Tiefkühlerbsen im Supermarkt, der Name der Endverbraucher den Lebensmittelproduzenten weder erreicht noch interessiert.[219] Relevant sind allein die tatsächlich auf sozialen Medien getätigten Äußerungen. Es besteht daher bei einem Betroffenen, der bewusst nicht „Freund" des Unternehmens geworden ist, aus Sicht des Unternehmens bei der Abwägung gegenüber den Nichtkunden, die Follower des Unternehmens sind, ein ebenso hohes Schutzbedürfnis.

2.5.3 Visualisierung und Influencer-Listen

Fraglich ist, in welcher Form die Ergebnisse der Social Network Analysis präsentiert und damit genutzt werden dürfen. Da es hier um die Beobachtung der Propagation von Meinungen geht, kann auch nur dieser Aspekt in diesem Kapitel beleuchtet werden. Fragen der allgemeineren Statistik werden im Kapitel zur Business Intelligence behandelt. Es zeigt sich, dass sich die Frage nach der Zulässigkeit auch an dieser Stelle noch nicht abschließend beantworten lässt. Es kommt vielmehr darauf an, ob sich an die reine Visualisierung noch eine weitere Nutzung anschließt, und welcher Natur diese ist. Dabei ist der Zweckbindungsgrundsatz für den Fall mehrerer hintereinanderliegender Nutzungszwecke besonders zu beachten, um eine unzulässige Zweckänderung zu vermeiden. Allgemein lassen sich an dieser Stelle die Konturen der Zulässigkeit wie folgt darstellen:

a) Grundsätzlich darf nur das eigene Followernetzwerk verfolgt werden, Verbindungen zwischen Personen nur, soweit beide Teil des Kreises sind.

b) Es handelt sich auch in der Visualisierung, zumindest nach einer Verkettung, um nicht allgemein zugängliche Daten, was bedeutet, dass Anhaltspunkte für ein überwiegendes schutzwürdiges Interesse des Betroffenen ausreichen, um die Nutzung in der konkreten Form unzulässig zu machen.

---

[218] Scheja/Haag, in: Leupold/Glosser, Münchener Anwaltshandbuch IT-Recht, Teil 5, Rn. 97; Thüsing/Traut, in: Thüsing, Beschäftigtendatenschutz, § 5, Rn. 26.

[219] Vgl. Müller, JZ 1982, S. 777.

c) Die Namensnennung ist anhand des Erforderlichkeitsgrundsatzes zu rechtfertigen. Dies wird in der Regel nur in Fällen des mutmaßlichen Einverständnisses, d.h. des Fehlens von schutzwürdigen Gegeninteressen, der Fall sein,[220] da eine Ansprache, gleich zu welchem Zweck, nach Auswertung via Social Network Analysis regelmäßig auf einer nicht erforderlichen Erhebung beruht. Die Darlegungslast für dieses Einverständnis liegt bei der verantwortlichen Stelle. Ein Weglassen von Namen führt dabei selten zur Anonymität im Sinne von § 3 Abs. 6 BDSG. Die Einblendung von „Tonalitäten" und ähnlichen Scores kann, wenn die Network Analysis ausschließlich zu informatorischen Zwecken erfolgt, eine Privilegierung gegenüber der Einblendung ganzer Zitate von Teilnehmern zur Folge haben. Dies gilt insbesondere bei durchgeführter, wirksamer Pseudonymisierung. Die Privilegierung erfolgt auch nur, wenn die originalen Postings nach Abschluss der Analysen gelöscht sind und wirkt nur so lange, wie diese Zitate nicht ohne wesentliche Erschwerung wiederhergestellt werden können.

Auszuführen ist noch die in Buchstabe b) genannte Fallgruppe, in welcher ein mutmaßliches Einverständnis zur Namensnennung vorliegt. Dies kann im Fall von sog. Influencern der Fall sein, d.h. Personen, welche besonders intensiv zu einem Thema, Unternehmen oder Produkt posten und es darauf anlegen, mit diesen Beiträgen besonders viele andere Nutzer zu beeinflussen.[221] Dabei kann gegebenenfalls von dem objektiven Merkmal der Aktivität auf das subjektive Merkmal des Wunsches nach Wirkung geschlossen werden. Eine solche Wirkung kann gegebenenfalls vom Hersteller des Produkts ausgehen. Je nach Ausgestaltung des Einzelfalls kann vorbehaltlich des Verwendungszwecks regelmäßig auch bei Verwendung nicht allgemein zugänglicher Daten eine namentliche Kenntlichmachung durch den Hersteller zulässig sein. Der Grundsatz der legitimen Zwecksetzung ist oft deswegen gewahrt, da der Zweck „Identifizierung der aktivsten User" wegen der spontanen, selbstbestimmten Aktivität des Betroffenen, die oft gerade darauf abzielt, das Interesse des Unternehmens zu wecken, rechtlich unbedenklich sein dürfte. Zu beachten ist aber unbedingt der Personenkreis, an den sich die Postings wenden. Eine Möglichkeit hierfür ist, dass gezählt wird, mit wie vielen Postings die verantwortliche Stelle selbst (z.B. unter Verwendung des von der Firma abweichenden Accountnamens bzw. unter Verwendung des @-Zeichens) angeschrieben wurde. Andere Anzeichen, dass der Betroffene gegen eine Erhebung seiner Daten voraussichtlich nichts einzuwenden habe, müssten auf äquivalentem Niveau liegen. Abzustellen ist auch hier auf den weiteren Verwendungszweck solcher Listen. Zu vermeiden ist die Nutzung zu Werbezwecken ohne Einwilligung, unabhängig davon, ob die Einlassungen des betroffenen Nutzers positiv oder negativ waren.

2.6 Die Aufbereitung von Daten zu internen Geschäftszwecken - Business Intelligence

Wie erwähnt[222], handelt es sich bei Business Intelligence um die statistische Auswertung von Kundendaten, wobei im Rahmen dieser Studie speziell auf Daten eingegangen werden soll, die zumindest teilweise durch Social Media Monitoring bzw. Social Search gewonnen wurden.

---

[220] Vgl. Tiedemann, NJW 1981, S. 948.

[221] Eck von Eck, MPR 2013, S. 107.

[222] Siehe dazu 1.5.1.2 Business Intelligence/Business Analytics.

2.6.1 Grundsätzliches

Die Datenbasis dieser Statistiken bilden daher entweder aus sozialen Medien erhobene Rohdaten oder mit Daten aus dem CRM-System im engeren Sinne. Schließlich kommen noch Daten als Quellen in Frage, die von der verantwortlichen Stelle als Telemedienanbieter mit Einwilligung der Betroffenen erhoben wurden. Hierunter fallen etwa selbstbetriebene Foren, aber auch auf Drittplattformen angebotene Apps[223]. Nur die aus sozialen Medien erhobenen Rohdaten können als allgemein zugängliche im Sinne des § 28 Abs. 1 Satz 1 Nr. 3 BDSG behandelt werden, und dies auch nur, soweit allgemeine Zugänglichkeit bei der Quelle vorlag. In allen anderen Fällen unterliegt die Nutzung anderen Rechtfertigungsnormen.

Business Intelligence kann für die Zwecke dieses Abschnitts in verschiedene Konstellationen aufgeteilt werden:

- Es erfolgt eine anonyme oder pseudonyme Datenerhebung (z.B. reine Zählung von Nennungen des eigenen Produkts pro Tag).
- Die Anonymisierung oder Pseudonymisierung wird unmittelbar nach Erhebung und vor der endgültigen Speicherung zur Nutzung (z. B. Tonalitätsanalysen mit nicht personenbezogenen Scores; nach Aggregierung und Segmentierung: Trendanalysen, Reichweitenanalysen) vorgenommen.
- Die Kundendatenbank wird als Quelle genutzt, soweit Daten aus Social Media-bezogen werden. Der statistische Output bleibt jedoch anonym.
- Die Kundendatenbank wird als Quelle genutzt und aus Social Media gewonnene Daten werden bestimmbaren Personen zugeordnet.
- Datenbestände von außerhalb der verantwortlichen Stelle bleiben personenbezogen gespeichert, die Visualisierung als Nutzung erfolgt jedoch anonymisiert (Daten aus beliebiger Quelle außer Kundendatenbank, ausgegebene Statistiken sind nicht personenbezogen).
- Datenbestände werden außerhalb der verantwortlichen Stelle gewonnen. Es werden individuelle Aussagen und Voraussagen über einzelne Personen getroffen (z.B. Werbescoring, Aktivitätslisten, Trends, Leadgenerierung).

2.6.2 Personenbezug des Datenmaterials

2.6.2.1 Anonyme und pseudonyme Daten

Es stellt demnach auch hier ein entscheidendes Kriterium dar, ob Daten anonym oder pseudonym erhoben oder nachträglich anonymisiert und pseudonymisiert werden. Gleichermaßen relevant ist es, ob personenbezogene oder –beziehbare Daten sofort nach der Erhebung gelöscht werden. Eine anonyme oder pseudonyme Erhebung ist bei der Nutzung von bestehenden Kundendaten meist von vorneherein ausgeschlossen, denn die Datensätze liegen bereits in personenbezogener Form vor. Bei Apps ist Pseudo-

[223] Siehe dazu 2.9 Datenschutzgerechte Nutzung von Drittplattformen.

nymität nur denkbar, soweit dies nach plattformspezifischen Datentransfer-Mechanismen vorgesehen ist und auf die Erhebung weiterer Daten verzichtet wurde. Bei den meisten Apps werden allerdings automatisch eine große Anzahl für die Bereitstellung und Abrechnung der App nicht erforderliche (s. § 14 Abs. 1 TMG) Daten des Accounts des Betroffenen an den Diensteanbieter übermittelt. Hiervon sind insbesondere auch solche Daten umfasst, die bis dahin nicht zugänglich waren.[224]

Aber auch bei Gebrauch des zweckgebundenen Social Media Monitoring als Datenbasis gilt: Anonymität ist regelmäßig nur gegeben, wenn der Datensatz entweder nur einen einzigen Datenpunkt umfasst und dieser selbst keinen Rückschluss auf eine bestimmte oder bestimmbare Person zulässt („Mann", nicht aber „Käufer des Bildes mit der Katalognr. 290902"),[225] oder bei der gleichzeitigen Erhebung mehrerer Datenpunkte die Schnittmenge der damit beschriebenen Personen groß genug bleibt, um eine Bestimmung auszuschließen (Käufer des Produkts, Geschlecht).[226] Letztere Variante dominiert in der Praxis, da ein Merkmal, z.B. „Äußerung zu unserem Produkt" bereits den Suchterminus darstellt und für die Marktsegmentierung ein weiteres Merkmal dazukommen soll. Unternehmen sind zum Beispiel daran interessiert, zu erfahren, welche Interessen diejenigen Personen, die ihre Produkte erwähnen, gemeinsam haben.

Dabei ist zu beachten, dass es modernen Big Data-Algorithmen heutzutage möglich ist, durch Betrachtung statistischer Korrelationen auch verkettete Datensätze mit wenigen Datenpunkten, die von sich aus nicht auf eine bestimmbare Person schließen lassen, anderen Datensätzen zuzuordnen, die sich mit einiger statistischer Wahrscheinlichkeit auf denselben Betroffenen beziehen. Auf diese Weise wird trotzdem eine Bestimmbarkeit unter Profilbildung ermöglicht. Gelegentlich wird dies nicht als Grund angesehen, von den betreffenden Ausgangsdaten isoliert als personenbeziehbar zu sprechen und es wird für solche Fälle gar eine Aufgabe des Personenbezugs als Anknüpfungspunkt des Datenschutzrechts gefordert, um solche scheinbaren Schutzlücken zu füllen.[227] Dem ist zu entgegnen, dass Datenschutzrecht in seinem öffentlich-rechtlichen Kern Gefahrenabwehrrecht ist und es daher geboten ist, auch die Re-Identifizierung als nicht fernliegende Gefahr den Regeln des Datenschutzrechts zu unterstellen, indem der Begriff der Anonymität verengt wird. Hierzu ist schlicht eine Definition der Bestimmbarkeit zu wählen, die die technischen Möglichkeiten der Rückrechnung und Verkettung berücksichtigt.[228] Weiterhin muss im Fall von längerfristiger Speicherung regelmäßig geprüft werden, ob nach dem Stand der Technik die gespeicherten Daten noch als anonym gelten können.[229] Die Beschränkung auf personenbezogene Daten und ihre spezifischen Gefahren ist dann für den Schutz der informationellen Selbstbestimmung ausreichend.

---

[224] Thüsing/Pötters, in: Thüsing, Beschäftigtendatenschutz, § 15, Rn. 28; s.a. Sachs/Meder, ZD 2013, S.303.

[225] Gola/Schomerus, BDSG, § 3, Rn. 4, 44.

[226] Gola/Schomerus, BDSG, § 3a, Rn. 10a.

[227] Vgl. Roßnagel, SVR 2014, S. 284.

[228] Dies entspricht dem Ansatz aus dem 26. Erwägungsgrund der Richtlinie 95/46/EG, wonach bei „der Entscheidung, ob eine Person bestimmbar ist, (…) alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen (…) eingesetzt werden könnten."

[229] Tinnefeld/Ehmann/Gerling, Datenschutzrecht, S. 288.

Es ist, wenn die Privilegierung der Anonymität in Anspruch genommen werden soll, nach alledem darauf zu achten, dass zusätzliche Datenpunkte im oben bezeichneten Sinne kumulativ eine ausreichend große Allgemeinheit aufweisen. Nach der Erreichung des legitimen Nutzungszwecks muss eine Zweckänderung ohne neuerliche Prüfung unabhängig von Zusatzwissen tatsächlich oder praktisch unmöglich sein. Bei der Erhebung anonymer Daten, wenn also die Anwendbarkeit des Datenschutzrechts wirksam ausgeschlossen werden soll, ist zudem nicht nur auf die Erhebung des Namens, sondern auch auf zusätzliche Angaben etwa zu Zeit und Umständen der Erhebung zu verzichten.[230] Geschieht eine von Anfang an derart generische Erhebung, ist das Datenschutzrecht häufig nicht anwendbar.[231] Dasselbe gilt, wenn etwa Nennungen des eigenen Produkts ausschließlich gezählt werden, ohne dass Daten der Autoren der Postings erhoben werden, insbesondere die Herstellung sog. Leistungskennzahlen (Key Performance Indicators = KPI). Gleiches gilt grundsätzlich für die Nennungen anderer nicht personenbezogener Stichwörter, solange sich nicht aus deren Verbindung ergibt, dass mittelbar auf bestimmbare Personen abgezielt wird (etwa Filterungen der Suchanfrage nach bestimmten Profilinhalten). Zulässig sind alle Nutzungen dieser anonymen Daten, solange der Personenbezug nicht mit verhältnismäßigen Mitteln wiederhergestellt werden kann. In der Praxis werden insbesondere Statistiken über die Anzahl der Nennungen des Produkts allgemein („Buzz"), die Anzahl der einzelnen Benutzer, die über ein bestimmtes Produkt posten („Reichweite") und die Anzahl der Nennungen pro gewählter Zeiteinheit („Intensität") in unterschiedlichen Abstufungen generiert, die jeweils anonym und daher datenschutzrechtlich nicht problematisch sind.

Für Fälle, in denen unmittelbar der Name des Betroffenen vom Datensatz getrennt wird, gilt grundsätzlich das oben Ausgeführte[232]. Der Personenbezug fällt nicht schon durch das Weglassen des Namens weg, vielmehr bestimmen die verbleibenden Daten in der Gesamtschau, ob der Personenbezug nachhaltig reduziert oder ganz aufgehoben wurde. Eine Reduktion des Personenbezugs ist in diesen Fällen ist jedoch manchmal einfacher zu erreichen als bei der Network Analysis, weil die Verortung des Betroffenen als Knoten in Netzwerken und damit seiner Stellung zur verantwortlichen Stelle als personenbeziehbares Merkmal wegfällt. Eine wirksame Methode, die Bestimmbarkeit zu reduzieren, besteht darin, verkürzte Datensätze ohne weitere Angaben zu speichern und sodann statistischen Segmenten zuzuteilen, die für sich jeweils groß genug sind, um auch einzelne „statistische Ausreißer" mit Zusatzwissen nicht mehr zuordenbar zu machen. Geschieht dies, liegt hierin wegen sofortiger Anonymisierung kein Eingriff.[233] Sind solche „Ausreißer" dagegen nachvollziehbar (klassisches Beispiel: nur ein Element in einem Segment, z.B. „mehr als 50 Postings am Tag zu Produkt X", „Nennung unseres Namens und häufige Reisen nach Papua-Neuguinea") und soll gegebenenfalls sogar eine Re-identifizierung erfolgen, sind die allgemeinen Regeln zum berechtigten Interesse nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG anwendbar, wobei darauf zu achten ist, dass eine solche Re-identifizierung vor Beginn der Erhebung in den Nutzungszweck mit aufgenommen wird, da eine Zweckänderung nach § 28 Abs. 2 BDSG oft nicht zu rechtfertigen sein dürfte. Wären Ausreißer theoretisch re-identifizierbar, besteht hieran aber bei der verantwortlichen Stelle kein Interesse,

---

230 Tinnefeld/Ehmann/Gerling, Datenschutzrecht, S. 287.

231 Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 128; Wohlgemuth/Gerloff, Datenschutzrecht, Kap. 3.3.2.4.

232 Siehe 2.5 Die Visualisierung von Zusammenhängen zwischen Nutzern - Social Network Analysis

233 Gola/Schomerus, BDSG, § 3a, Rn. 10a.

muss darauf geachtet werden, dass das Datum nach Erreichung des Zwecks gemäß § 35 Abs. 2 Nr. 3 BDSG gelöscht wird.

Entsprechend den Ausführungen in 2.5 kann auch die Umrechnung von Beiträgen und Inhalten in Zahlenwerte (Scores) zur Pseudonymisierung beitragen. Die Speicherung einer Vielzahl personenbezogener Profildaten ist als solche oft nicht zu rechtfertigen, die Speicherung ausschließlich des Datums „Einstellung des (pseudonymen) Betroffenen zum Unternehmen ist 67% positiv" ist dagegen (vorbehaltlich des Nutzungszwecks) regelmäßig zulässig, weil sie eine Re-identifizierung nicht zulässt.

2.6.2.2 Scores und Scoring

Soll der Personenbezug der einzelnen Scores dagegen aufrechterhalten werden, etwa im Fall des Werbescorings oder des flexiblen Pricings so sind die Hürden hierfür oft deutlich höher. Neben den allgemeinen Erlaubnistatbeständen (regelmäßig § 28 Abs. 1 Satz 1 Nr. 2 BDSG) können nämlich zusätzlich die Vorschriften über die automatische Einzelentscheidung (§ 6a BDSG) und das Scoring im engeren Sinne (§ 28b BDSG) einschlägig sein.[234] Die Regelung des § 28b BDSG enthält die Voraussetzungen dafür, dass die verantwortliche Stelle Scores bilden und nutzen darf, die ein zukünftiges Verhalten des Betroffenen prognostizieren, und die zur Entscheidung über Begründung und Durchführung eines Vertragsverhältnisses dienen. Diese Vorschrift wurde ursprünglich für das Kreditscoring entwickelt,[235] seine weite Formulierung zwingt jedoch zur Anwendung auf alle Fälle des Abschlusses von Verträgen. Auch die Konditionen eines Vertrages sind jedoch grundsätzlich von § 28b BDSG umfasst.[236] Es reicht insoweit, dass die auf dem Scoring basierende Entscheidung eine rechtliche Folge im Zusammenhang mit einem Vertragsverhältnis für den Betroffenen hat. Dann handelt es sich um eine Entscheidung über die Durchführung eines Vertragsverhältnisses,[237] da ein möglicher Vertragsschluss zu für den Betroffenen günstigeren Konditionen ausscheidet.

Dieser Zusammenhang fehlt hingegen beim Werbe-Scoring.[238] Bei dieser in sozialen Netzwerken verbreiteten Werbeform werden anhand der Interessen der Betroffenen Profile gebildet und ausgewertet. Mittels dieser Daten wird ermittelt, welcher Nutzer sich potentiell für welches Produkt interessieren könnte und zum Kauf bereit und liquide ist. Auf diese Weise wird ihm zielgerichtete, für ihn zusammengestellte Werbung präsentiert. Der Score entscheidet nicht nur darüber, welche Produkte er zu sehen bekommt, sondern auch, auf welche Art und auf welchem Weg.[239] Bei den Werbeeinblendungen handelt es sich noch nicht um den Abschluss eines Vertrages, sondern um bloße Information ohne unmittelbare Rechtsfolge.[240] Auch wenn es denkbar ist, dass der Kunde durch das Werbe-Scoring belastet wird, weil ihm bei-

---

[234] Siehe zum Scoring ausf. ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen.

[235] BT-Drs. 16/10529, S. 1 ff.

[236] Däubler/Klebe/Wedde/Weichert, BDSG, § 28b, Rn. 2a.

[237] BT-Drs. 16/10529, S. 16; ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, S. 21.

[238] Gola/Schomerus, BDSG, § 28b, Rn. 8; Wäßle/Heinemann, CR 2010, S. 412.

[239] Hansen/Meissner, Verkettung digitaler Identitäten, S. 113.

[240] ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, S. 21 f.

spielsweise die Werbeeinblendung stört, interessante Angebote vorenthalten werden oder er sich unzutreffend eingeschätzt sieht, ändert dies an der Unanwendbarkeit des § 28b BDSG nichts.[241]

Anders zu behandeln ist die flexible Anpassung von Preisen. Bei dieser Form dient der Score gerade zur Festlegung der Konditionen, zu denen die verantwortliche Stelle bereit ist, einen Vertrag abzuschließen.[242] In diesem Fall muss die verantwortliche Stelle vor Erhebung und Nutzung des Scores die Vorgaben des § 28b BDSG beachten.

Die Zulässigkeit eines Scorings nach dieser Vorschrift setzt zunächst voraus, dass das Scoring auf der Basis eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens erfolgt. Die verwendeten Daten müssen statistische Relevanz besitzen und korrekt gewichtet sein, die wissenschaftlichen Erkenntnisse plausibel nachvollziehbar sein und es darf kein Nutzungsverbot durch eine unzulässige Diskriminierung bestehen.[243] Oberstes Kriterium ist dabei die Richtigkeit der verwendeten Daten.[244] Gerade dies ist bei Daten, die aus sozialen Netzwerken generiert werden, nicht gewährleistet. Bereits die Identität der Nutzer in sozialen Netzwerken kann nicht sicher nachvollzogen werden.[245] Selbst dann, wenn ein Nutzer unter einem vermeintlichen Klarnamen auftritt, kann dieser entweder willkürlich erdacht worden oder die Folge eines Identitätsdiebstahls sein. Auch die Angaben, die ein Nutzer in derartigen Netzwerken macht, entspricht nicht automatisch der Wahrheit, sondern zeigt lediglich das Bild, das der Nutzer nach außen hin von sich vermitteln möchte. Kann die Richtigkeit der Daten ausnahmsweise dennoch gesichert werden kann, folgt das Problem, dass ein wissenschaftlich anerkanntes Verfahren für die trennscharfe Berechnung solcher Scores nicht existiert. Es ist auch nicht bestimmbar, welche Daten für eine solche Scorebildung überhaupt erheblich sein können. Regelmäßig wird es zudem schon an einer Rechtsgrundlage für die Datenerhebung fehlen. Die Erhebung öffentlich zugänglicher Daten nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG steht nämlich unter dem Vorbehalt des schutzwürdigen Interesses des Betroffenen am Ausschluss der Verarbeitung. In sozialen Netzwerken überwiegend gemachte Angaben zum Freizeitverhalten, Schilderungen zu privaten Beziehungen oder zum Konsum zählen zur privaten Sphäre des Betroffenen. Werden entsprechende Informationen in sozialen Medien verbreitet, so dürfen diese nicht in eine Score-Wertberechnung einfließen.[246]

Zulässig ist ein Scoring gegebenenfalls, wenn aus der verantwortlichen Stelle bereits vorliegenden Daten, etwa die Beziehungshistorie in der Kundendatenbank, über das Zahlungsverhalten Voraussagen getroffen werden. Mit den Offline-Fällen gleich zu behandeln wäre es wohl auch, wenn der Betroffene regelmäßig über ein soziales Netzwerk gegenüber der verantwortlichen Stelle selbstverschuldete Beschädigungen an einem Produkt (z.B. mehreren Mietwagen) meldet und die verantwortliche Stelle einen Score über die Wahrscheinlichkeit weiterer Beschädigungen bildet. Voraussetzung wäre, dass die Identität des

---

241 Ambs in Erbs/Kohlhaas Strafrechtliche Nebengesetze, § 28b BDSG, Rn. 12b.

242 ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, S. 41.

243 Weichert, DuD 2006, S. 401.

244 ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, S. 35; Weichert, DuD 2006, S. 401.

245 Vgl. ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, S. 89.

246 ULD/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, S. 38.

Meldenden, das tatsächliche Bestehen der Schäden und das Verschulden verifiziert worden sind. Dann gibt es keinen Grund, Daten aus dem sozialen Netzwerk anders zu behandeln als im Offline-Geschäftsgang erhobene, der Score bezieht sich gerade nicht auf unzuverlässige Online-Daten.

2.6.2.3 Automatisierte Einzelentscheidung

Eine weitere rechtliche Hürde für die Zulässigkeit des Einsatzes von Scoringsystemen für Entscheidungen gegenüber einzelnen Betroffenen stellt der parallel zu § 28b BDSG anwendbare § 6a BDSG dar. Danach dürfen Entscheidungen, die den Betroffenen erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Beispiele für Persönlichkeitsmerkmale sind nach Art. 15 Abs. 1 der Richtlinie 95/46/EG ihre berufliche Leistungsfähigkeit, ihre Kreditwürdigkeit, ihre Zuverlässigkeit oder ihr Verhalten. Ein solches Persönlichkeitsmerkmal ist z.B. auch die wirtschaftliche Leistungsfähigkeit als solche. Die Vorschrift zielt daher gerade darauf ab, eine automatische, auf Profilbildung durch Kumulation personenbezogener Daten basierende Schlechterstellung zu unterbinden.[247] Wenn einem Kunden ein höherer Preis oder ein ungünstigerer Finanzierungsrahmen angeboten wird, der sich ausschließlich aus der automatisierten Auswertung seiner Aktivitäten auf sozialen Medien ergibt, so handelt es sich um automatisierte Einzelentscheidungen zu seinen Ungunsten. Jedoch ist umstritten, wie der Begriff der erheblichen Beeinträchtigung zu umreißen ist. Er ist auch unter Berücksichtigung der Vertragsfreiheit jedenfalls dann erfüllt, wenn aufgrund der Datenverarbeitung ein Vertragsschluss abgelehnt wird.[248] Dasselbe wird zu gelten haben, wenn dem Betroffenen, der in einem Abhängigkeitsverhältnis zum CRM-Betreiber steht (etwa in Monopolkonstellationen), aufgrund des Scorings ein schlechterer oder teurerer Service zukommt. Erreicht Werbung einen nach den Wertungen von § 7 UWG belästigenden Charakter, dürfte auch dies als erhebliche Beeinträchtigung zu sehen sein.[249]

Maßnahmen nach § 6a BDSG können nach dessen Absatz 2 Nr. 2 ausnahmsweise zulässig sein, wenn die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist, die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer automatisierten Einzelentscheidung mitteilt und auf Nachfrage deren wesentliche Gründe erläutert. Die Interessenwahrung wird insbesondere durch ein System gewährleistet, in dem der Betroffene von der automatisierten Entscheidung in Kenntnis gesetzt wird und Gelegenheit zur Stellungnahme erhält, wobei die Stellungnahme in eine spätere Überprüfung der automatisierten Entscheidung durch eine natürliche Person münden muss. Bei der Benachrichtigungspflicht handelt es sich um die Pflicht zur Mitteilung derjenigen Faktoren, welche für die Entscheidung ausschlaggebend waren. Entgegen der Linie des SCHUFA-Urteils des BGH,[250] wonach die Methode der Berechnung als Geschäftsgeheimnis einzustufen ist, dürfte hier nicht nur über die der Entscheidung zugrundeliegenden Daten zu informieren sein, sondern auch über die Berechnungsmethode. Da eine derartige Benachrichtigung von aktuellen oder potentiellen Kunden bei den meisten CRM-Anwendungen nicht stattfindet, fällt ein Teil der Big-Data-Anwendungen im Kundenbezie-

[247] Scholz, in: Simitis, BDSG, § 6a, Rn. 21 ff.

[248] Scholz, in: Simitis, BDSG, § 6a, Rn. 28 m.w.N.

[249] Ähnlich Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 6a Rn. 9, a.A. Gola/Schomerus, BDSG, § 6a, Rn. 10

[250] BGH, Urt. v. 28.01.2014, VI ZR 156/13.

hungsmanagement, nämlich die automatische Zuweisung von Konditionen in laufenden Geschäftsbeziehungen oder aus einer marktbeherrschenden Stellung derzeit bereits nach dem klaren Gesetzeswortlaut weg. Nur unter Einhaltung dieser Rahmenbedingungen kann eine automatisierte Einzelentscheidung als Nutzung von Daten nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt sein.

Werbescoring ist als vorbereitende Maßnahme zwar nicht an § 28 Abs. 3 BDSG zu messen, weil nicht der Scorewert selbst, sondern Kontaktdaten und die aufgrund des Scorewerts ausgewählte Werbung zur Ansprache genutzt werden. Allerdings kann die Nutzung der Kontaktdaten zur Werbeansprache nur bei Vorliegen einer Einwilligung des Betroffenen in die Werbemaßnahme zulässig sein. Die Erhebung des Scorewerts ist ohne Vorliegen einer entsprechenden Einwilligung somit wertlos und damit niemals angemessen im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

2.6.3 Auswertung der Kundendatenbank

Ist die genutzte Quelle die **Kundendatenbank**, so liegt in Business Intelligence-Maßnahmen typischerweise die Nutzung von Datensätzen, in denen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zur Vertragsdurchführung erforderliche Kundenstammdaten mit zahlreichen, im Laufe der Geschäftsbeziehung erhobenen weiteren Daten verknüpft sind. Der Wunsch, Kunden auch als Dialogpartner auf sozialen Netzwerken zur Verfügung zu haben und weitere Interessen durch Erhebung von Äußerungen und Profildaten zu erlangen, ist eine der treibenden Kräfte des Social Marketing. Die Datensätze zu einzelnen Kunden im CRM enthalten jedoch typischerweise nur zu einem geringen Teil Social Media-Daten, weil es oft vom Zufall abhängt, ob Bestandskunden für die verantwortlichen Stelle auf sozialen Medien bestimmbar sind und daher die Zuspeicherung von solchen Daten in die Kundendatenbank typischerweise bei Servicefällen und Beschwerden über das soziale Medium erfolgt. Trotzdem ist die wirtschaftliche und datenschutzrechtliche Relevanz enorm.

Die datenschutzrechtliche Einschätzung dieser Konstellation hängt wesentlich von der Zulässigkeit der Zuspeicherung ab[251]. Wenn vorliegend ein Nutzungszweck als rechtswidrig bezeichnet wird, ist nicht nur die Nutzung der betreffenden Social Media-Daten verboten, sondern auch die Daten sind gemäß §§ 28 Abs. 1 Satz 2, 35 Abs. 2 Satz 2 Nr. 1 BDSG umgehend zu löschen, weil im Fall einer unzulässigen Zwecksetzung bereits die Zuspeicherung als rechtswidrig anzusehen ist und nicht hätte erfolgen dürfen.

Zunächst ist wegen der bei der verantwortlichen Stelle stets vorhandenen und nicht zu anonymisierenden Datengrundlage die Nutzung niemals anonym und daher stets rechtfertigungsbedürftig. Das gilt auch dann, wenn eine ordnungsgemäß segmentierte, ohne Namensnennung arbeitende Statistik produziert wird. Die Datengrundlage, ebenso wie die Zuweisung einzelner Attribute und Werte zu einzelnen Betroffenen, ist stets rückverfolgbar. Die Rechtmäßigkeit der Generierung solcher Statistiken ist von zwei Faktoren abhängig, nämlich der Rechtmäßigkeit der Speicherung im Übrigen und den weiteren geplanten Nutzungszwecken.

Dass die Speicherung im Übrigen rechtmäßig ist, bedeutet, dass die verantwortliche Stelle diese im Rahmen der Zweckbindung nutzen kann, weil offensichtlich kein überwiegend entgegenstehendes Interesse

[251] Siehe dazu 2.7 Die Zuspeicherung in das CRM

erkennbar ist. Es kann der verantwortlichen Stelle im Rahmen von § 28 Abs. 1 Satz 1 Nr. 2 BDSG oder auf Grundlage einer wirksamen Einwilligung nicht grundsätzlich verwehrt werden, aus einer solchen rechtlich einwandfreien Datengrundlage interne Statistiken zu generieren. Die reine Aufbereitung (als OLAP-Anfrage oder z. B. in Form von Kundenrankings), auch wenn sie personenbezogen erfolgt, kann also bei rechtmäßiger Zuspeicherung der genutzten Daten ins CRM nur dann rechtswidrig sein, wenn sie im konkreten Fall für den bereits bei der Erhebung gesetzten legitimen Zweck nicht erforderlich ist. Das wird bei rein intern genutzten Statistiken selten der Fall sein, weil allgemeine Formulierungen des Nutzungszwecks für interne Geschäftszwecke (nicht aber die bloße Wiederholung des Normtexts, sog. deklaratorische Klausel) zur wirksamen Zwecksetzung nach § 28 Abs. 1 Satz 2 BDSG ausreichend sind. Eine Ausnahme hiervon stellen besondere Arten personenbezogener Daten dar. Diese dürfen regelmäßig nicht in der gegebenen Form aufbereitet werden, wenn dies nicht für bestimmte Fälle in der Einwilligungserklärung bei Erhebung festgelegt worden ist.[252] Einen weiteren Fall der nicht erforderlichen Abfrage dieser Daten könnte z.B. der Fall darstellen, dass aus Neugier mit Hilfe der Datenbank Persönlichkeitsprofile erstellt werden, obwohl nur die Anzeige von Kontaktdaten erforderlich wäre. Die Grenzen zwischen Zweckverfehlung und fehlender Erforderlichkeit sind insoweit fließend.

Anders liegt es bei Nutzungszwecken, die jenseits der bloßen Anzeige von Datenbankinhalten liegen. Die häufigste Nutzung von Profilen ist selbstverständlich das Marketing. Unternehmen loten Absatzchancen ihrer Produkte danach aus, welcher Käufergruppe ein Kunde basierend auf seinen Interessen und seinem bisherigen Kaufverhalten zuzuordnen ist. Für eine Werbeansprache, die auf einer solchen Analyse basiert, greift keine der Ausnahmen vom Einwilligungserfordernis nach § 28 Abs. 3 BDSG. Daher ist eine Einwilligung des Betroffenen erforderlich, sofern nicht das Listenprivileg greift. [253] Wie beim Werbescoring oben handelt es sich bei der Bildung von Käuferprofilen nicht um Werbung, sondern um die Vorbereitung von Werbung. Ist der Zweck des Werbescorings mangels Aussicht auf rechtmäßige Ansprache bereits nicht erreichbar, dürfte dies bereits die Angemessenheit des Werbescorings in Frage stellen. Ein völliger Ausschluss der Zulässigkeit eines Werbescoring lässt sich daraus jedoch nur ableiten, sofern sicher ist, dass eine Ansprache des Betroffenen in jedem Fall rechtlich unzulässig wäre.

Auch in diesem Fall ist aber denkbar, dass eine nichtwerbliche Ansprache vorbereitet werden soll, etwa weil ein besonders großer Anstieg öffentlicher Beschwerden auf sozialen Netzwerken über ein Produkt zu verzeichnen ist. Hier gelten allgemein die Maßgaben von § 28 Abs. 1 Satz 1 Nr. 2 BDSG mit dem Erfordernis der Berücksichtigung der weiteren Grundrechte des Betroffenen, etwa der Meinungsfreiheit und weiteren Schutzbereichen des Persönlichkeitsrechts.

2.6.4 Auswertung von Datenbanken

Schließlich ergibt sich noch das Problem der Auswertung von Datenbanken, deren Datensätze sich nicht notwendig auf Kunden beziehen. Die Auswertung von „Freundeslisten“ ist bereits besprochen worden.[254] Es bleibt, solche Datenbanken zu besprechen, die auf quasi-natürlichem Wege entstehen, wenn der ge-

[252] Gola/Schomerus, BDSG, § 4a Rn. 34.

[253] Pfeifer, MMR 2010, S. 524 f.

[254] Siehe oben 2.5.2 Kunden und Nichtkunden/Follower und Friends-of-Friends.

samte Datenstrom, auch wenn er so gefiltert ist dass sich alle Postings auf die verantwortliche Stelle und ihre Produkte beziehen, gespeichert und nach und nach angereichert wird. Je nach sozialem Medium beziehen sich die gespeicherten Daten auf Klarnamen und auf Pseudonyme, wobei die Unterscheidung wegen der Möglichkeit, falsche aber plausible Namen zu benutzen, oft nicht zu leisten ist. Echte Pseudonymisierung im Sinne von § 3 Abs. 6a BDSG ist zudem nur selten möglich, da miterhobene Daten wie Foto, Geburtstag, Familienstand, Namen der Kinder und anderer Familienmitglieder häufig eine Bestimmung ermöglichen. Schon eine solche kumulative Speicherung ist in aller Regel unzulässig, und zwar selbst dann, wenn die Zwecke ausreichend konkret festgelegt werden. Zwar mag die Erhebung und Speicherung der einzelnen Daten nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG, und damit ohne Rücksicht auf Erforderlichkeit erfolgen dürfen. Es ist im Schrifttum praktisch unumstritten, dass die allgemeine Zugänglichkeit eines Einzeldatums als Block von Information nicht allein dadurch aufgehoben wird, dass sie auf einen anderen Datenträger transferiert wird, solange das Datum in der Originalquelle noch ohne personale Beschränkungen einsehbar ist.[255]

Diese Wertung und die bereits besprochenen Verarbeitungsprivilegien, welche sich daran knüpfen, sind jedoch nicht einschlägig, wenn, wie im beschriebenen Szenario, eine kontinuierliche Speicherung in einer Datenbank erfolgt. Dann greift der Verkettungseffekt, mit der Folge, dass aus der Zusammenführung neue Daten entstehen. Dies können schlicht Aussagen über Unterschiede zwischen einem neuen und einem bisherigen Zustand sein, aber auch Daten, die mehr als die Summe ihrer Teile darstellen und sich aus der Kumulation ergeben. Beispiele finden sich oben unter 2.4.2.2 Einzelfälle der allgemeinen Zugänglichkeit. Für solche Daten gilt das Privileg nicht.

Die Sammlung und Speicherung von Daten über Betroffene, deren einzige Verbindung mit dem Unternehmen darin besteht, dieses auf einem sozialen Medium erwähnt zu haben, ist daher insgesamt nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu beurteilen. Hier bietet es sich an, zunächst nach dem Zweck zu differenzieren: Die Anlage einer Datensammlung mit Postings aller Betroffenen als Grundlage für Big-Data-Auswertungen kann nur dann zulässig sein, wenn der Personenbezug wegfällt, etwa weil die Umstände einer Äußerung (Autor, Timestamp, Wortlaut des Postings) nicht gespeichert oder unmittelbar gelöscht werden. Wenn die Datengrundlage personenbezogen bleibt, überwiegt bei einer solchen Zwecksetzung in der Regel das Interesse des Betroffenen, nicht zum Objekt statistischer Durchdringung zur Förderung kommerzieller Interessen Dritter zu werden. Dies ist eindeutig in Fällen, in denen die statistische Auswertung etwa der Leadgenerierung, also der Gewinnung neuer Kunden, dient. Da eine Ansprache an einen bisher Unternehmensfremden mit dem Ziel des Vertragsabschlusses ohne Einwilligung hier datenschutzrechtlich unzulässig ist (§ 28 Abs. 3 BDSG), dient die Analyse, welcher Nichtkunde basierend auf seinen aus sozialen Medien erhobenen Daten für eine Anwerbung in Frage käme, keinem rechtlich gebilligten Zweck und ist daher gemäß § 28 Abs. 1 Satz 2 BDSG unzulässig.

Der faktische Zwang zur Eliminierung des Personenbezugs gilt selbst dann, wenn die verantwortliche Stelle keine Absicht hat, in ihren statistischen Auswertungen einen Personenbezug herzustellen. Dann gibt es keinen Grund, entgegen § 3a Satz 2 BDSG den Personenbezug aufrechtzuerhalten. Unterbleibt eine solche Anonymisierung, obwohl sie dem Nutzungszweck nach möglich wäre, setzt sich das Be-

[255] Siehe nur Simitis, in: Simitis, BDSG, § 28, Rn. 160.

troffeneninteresse regelmäßig durch.[256] Insoweit liegt der nicht hinzunehmende Eingriff bereits in der Speicherung, so dass es auf die anonyme Nutzung nicht ankommt.

Nach vorstehender Maßgabe wäre jedoch eine listenförmige Statistik der für das Produkt oder im Zusammenhang mit dem Produkt benutzten besonders häufigen Hashtags durchaus möglich, wenn der Rest der Nachricht nicht gespeichert wird und eine Bestimmung daher ausscheidet. Diese Hashtaganalyse stellt potentiell zudem eine auch gegenüber dem Tonalitäts-Scoring schonende Form der Stimmungsanalyse dar, weil mit diesen Mitteln häufig Einstellungen zum Gegenstand des Postings ausgedrückt werden, diese aber häufig allgemein genug sind, eine Bestimmbarkeit wirksam zu verhindern.

Es ist daneben vorstellbar, dass selbst eine solche umfassende Datenbank dann zulässig bleibt, wenn ihr Zweck nur die Beobachtung besonders aktiver, und damit gegebenenfalls mit der Speicherung rechnender User ist. Dies kann dadurch geschehen, dass nicht der Inhalt der Postings, sondern nur der Umstand der Nennung des Unternehmens oder eines Produkts durch eine bestimmte Person erhoben wird. Es handelt sich um die umgekehrte Praxis zur oben skizzierten Hashtag-Analyse, weil gerade der Name oder Nickname, nicht aber die Aussage gespeichert wird. Solche Daten dürften unter den Bedingungen des oben unter 2.5.3 Visualisierung und Influencer-ListenGesagten (insbesondere mit zulässiger Zwecksetzung etwa bei der Nutzung zur Ansprache) in Form von Influencer-Listen und ähnlichen Aktivitäts-Rankings für den internen Gebrauch verarbeitet und genutzt werden.

2.6.5 Auswertung von zugeschnittenen Datenbanken

Werden einzelne Datenbanken für einzelne Gruppen von Personen angelegt, welche mit dem Unternehmen auf sozialen Netzwerken in Kontakt treten, und erfolgt eine Speicherung insoweit selektiv, ist es dagegen in größerem Maße denkbar, dass auch personenbezogene Auswertungen möglich werden. In allen Fällen ist jedoch streng darauf zu achten, dass nicht mehr Daten gespeichert werden, als zur Zweckerreichung erforderlich und dass die Daten nach Zweckerreichung umgehend gelöscht werden (§ 35 Abs. 2 Nr. 4 BDSG).

Denkbar ist eine Anlage einer solchen Datenbank zunächst für Unternehmen, die keine B2C-Kundendatenbank unterhalten, weil sie Massenverträge abschließen. Im Beschwerdemanagement dürften hier Statistiken mit der Aufbereitung etwa des Ergebnisses und der Bearbeitungszeit von Serviceanfragen pro Fall erstellt werden. Dies gilt grundsätzlich auch in Fällen, in denen der Service nicht vertraglich geschuldet ist und daher die Datenverarbeitung nicht schon nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG gerechtfertigt ist, wenn der Service nicht aufgedrängt, sondern vom Kunden initiiert wurde.

Aber auch bei Nichtkunden dürfte es einzelne Fallgruppen geben, bei denen eine Auswertung auf der Grundlage personenbezogener Daten in Betracht kommt. So kann z.B. durchaus ein überwiegendes Interesse an einem statistischen Tracking ausschließlich zu laufenden Beschwerden über die Auswirkungen eines Produkts auf Nichtkunden bestehen, z.B. in Fragen der Produkthaftung.[257]

---

[256] Zscherpe, in: Taeger/Gabel, BDSG, § 3a, Rn. 48 ff.

[257] Zur Erhebung von Kundendaten durch einen der Produkthaftung unterliegenden Kfz-Hersteller siehe Roßnagel, SVR 2014, S. 281.

Schließlich kann unter engen Voraussetzungen noch Interesse an der Anlage einer Art schwarzer Liste derjenigen Personen bestehen, die durch strafbare Aussagen in sozialen Medien rechtliche Konsequenzen zu erwarten haben. Insoweit, als eine Verfolgung auf sozialen Medien gerechtfertigt ist, ist zur Beweissicherung auch die Speicherung der Postings und ihrer Umstände zulässig.[258]

2.7 Die Zuspeicherung in das CRM

Eine entscheidende Aufgabe des klassischen wie des Social CRM, die oben bereits ausgeführt wurde,[259] ist die Zuspeicherung von Daten aus sozialen Netzwerken in die Kundendatenbank. Dabei sind zunächst nach der Natur der Daten drei Grundtypen zu unterscheiden. Zunächst können Äußerungen von Kunden zugespeichert werden, die diese von sich aus gegenüber der verantwortlichen Stelle getätigt haben. Das klassische Beispiel ist hier die Serviceanfrage, aber auch die Beschwerde oder das Lob kommen in Betracht. Charakteristisch ist, dass die verantwortliche Stelle direkt (etwa unter Verwendung des genauen Accountnamens) angesprochen worden ist. Die Zuspeicherung dient insoweit der Bearbeitung der Anfrage oder der Beschwerde. Gegebenenfalls findet auch eine weitergehende Speicherung statt, um einen Überblick über die Kontakthistorie zu gewinnen, oder etwa statistische Erhebungen über wiederkehrende Beschwerden über das Produkt zu ermöglichen.

Die zweite Form betrifft die Speicherung von Aussagen in Bezug auf das Unternehmen, die nicht notwendig aus einer direkten Ansprache resultieren, etwa die reine Erwähnung des Unternehmensnamens oder von Produkten.

Die dritte Form besteht schließlich in der Speicherung der im Profil abgelegten Interessen und weiteren persönlichen Daten. In allen Formen kommt auch noch die sukzessive Speicherung von Daten über bisher nicht in der Datenbank vorhandene Personen und die Anlage entsprechender Profile in Betracht.

Nahziel der zwei letztgenannten Formen ist der 360-Grad-Blick auf den aktuellen oder potentiellen Kunden. Neben etwa vorhandenen Stammdaten und der auf den CRM-Betreiber bezogenen Verkaufshistorie wird so auch ein Bild über die Interessen und Meinungen des Betroffenen gewonnen. Fernziel ist selbstverständlich ganz überwiegend die Zusendung von zugeschnittener Werbung, und zwar bei Bestandskunden bezogen auf das bereits Gekaufte in der Form des Cross-Selling (Verkauf eines anderen Produkts des Unternehmens) oder des Up-Selling (Verkauf des gleichen Produkts in einer höherwertigen und damit teureren Form), bei Neukunden bezogen auf die erhobenen Interessen. Daten der zweiten Form werden darüber hinaus oft zur nichtwerblichen Ansprache benutzt. Die Erstellung rein interner Statistiken ist oft zweitrangig. Fraglich ist, unter welchen Umständen die Zuspeicherung rechtlich möglich ist.

Sollen Daten ohne Einwilligung gespeichert werden, so ist hierfür § 28 Abs. 1 Satz 1 Nr. 2 BDSG die Rechtsgrundlage. Wegen der Verkettung mit den Stammdaten sowie gegebenenfalls weiteren erhobenen Daten, werden regelmäßig nicht allgemein zugängliche Daten generiert. Die gespeicherten Daten sind regelmäßig auch nicht zur Vertragsdurchführung erforderlich. Fehlt dem Unternehmen ein nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erforderliches Datum, so darf es dieses wegen des Direkterhebungsgrundsat-

[258] Bzgl. E-Mails vgl. Krasemann, MMR 2004, XI (XII).

[259] Siehe oben 1.6.1.6.

zes (§ 4 Abs. 2 BDSG) ohnehin nicht ohne Weiteres aus sozialen Medien erheben. Grundlegend für die Prüfung der Zulässigkeit ist die Zwecksetzung**.** Daten, die zur Durchführung einer von dem Betroffenen ausdrücklich gewünschten Serviceleistung oder Auskunftserteilung erforderlich sind, dürfen für die Dauer des Verwendungszwecks in der Regel gespeichert werden. [260] Es handelt sich um eine Datenerhebung unter Mitwirkung des Betroffenen, so dass sich nachfolgende Aufklärungspflichten nach § 4 Abs. 3 BDSG richten. Wird die verantwortliche Stelle ohne einen konkreten Auftrag, vielleicht ohne ein Interesse am Kontakt durch den Betroffenen direkt angesprochen, wird man der betroffenen Stelle ein Interesse auch an der personenbezogenen Speicherung nicht absprechen können, soweit eine Antwort tatsächlich geplant ist. Bei der Antwort ist ein werblicher Charakter zu vermeiden.

Werden Daten, gleich welcher Kategorie, jedenfalls auch zu Werbezwecken erhoben, unterliegt bereits diese Erhebung indirekt § 28 Abs. 3 BDSG.[261] Wird überhaupt kein Zweck festgelegt, sondern werden die Daten nur aus Interesse oder für noch festzulegende Zwecke „auf Halde" gespeichert, ist diese Erhebung wegen § 28 Abs. 1 Satz 2 BDSG nicht zulässig.[262] Die Kundendatenbank stellt regelmäßig die Grundlage von Werbeansprachen an Bestandskunden dar und gerade die zugespeicherten Erkenntnisse auch außerhalb des Social CRM sind die Entscheidungskriterien dafür, welcher Betroffene welche Werbung erhält. Ist die Nutzung von Daten aus der Kundendatenbank zu Werbezwecken nicht ausgeschlossen, ist damit bereits deren Speicherung von einer Einwilligung abhängig oder muss dem Listenprivileg nach § 28 Abs. 3 BDSG folgen.

Es ist darauf zu achten, dass nach Abschluss der Nutzung die Daten gelöscht werden, soweit sie dem Nutzungszweck gemäß nicht mehr verwendet werden.[263] Ansonsten müssen sie getrennt gespeichert werden (Nr. 8 der Anlage zu § 9 BDSG), um zu verhindern, dass Erkenntnisse zu weitergehenden Zwecken, insbesondere Werbezwecken verwertet werden.

Denkbar ist auch, dass in einer gesonderten Datenbank die Speicherung personenbezogener Daten für bestimmte nichtwerbliche Zwecke erfolgt und im CRM nur Daten zu Servicefällen gespeichert werden. Weitergehende, zu Werbezwecken vorbehaltene Daten werden jedoch nur von solchen Betroffenen gespeichert, die ausdrücklich und wirksam in die Werbezusendung eingewilligt haben oder deren Daten dem Listenprivileg des § 28 Abs. 3 BDSG unterliegen. So kann dem Prinzip der Zweckbindung ausreichend Genüge getan und Missbrauch vermieden werden.

Das berechtigte Interesse der verantwortlichen Stelle im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist am Erhebungszweck abzulesen.[264] Berechtigt ist jedes von der Rechtsordnung allgemein gebilligte Interesse. Vorliegend wird das Interesse an der Beschaffung der Daten bereits bei der Erhebung geprüft. Insofern dürften nahezu alle (nichtwerblichen) Verarbeitungszwecke, die im Rahmen der geschäftlichen Tätigkeit anfallen, von dem Begriff erfasst sein. Erforderlichkeit bedeutet, dass unter Berücksichtigung des rechtlich gebilligten Nutzungszwecks die verantwortliche Stelle nicht zumutbar auf den Verzicht auf die kon-

[260] Krasemann, MMR 2004, XI (XI ff.).

[261] Gola/Schomerus, BDSG, § 18, Rn. 42; Peifer, MMR 2010, S. 524 f.

[262] Petri, in: Simitis, BDSG, § 4e, Rn. 7.

[263] Becker/Ambrock, JA 2011, S. 563.

[264] Gola/Schomerus, BDSG, § 28, Rn. 35.

krete Maßnahme verwiesen werden kann.[265] Diese Definition überschneidet sich weitgehend mit dem verwaltungsrechtlichen Erforderlichkeitsbegriff, an dem staatliche Eingriffe gemessen werden, und nach dem eine Maßnahme immer dann als erforderlich gilt, wenn es zu ihr keine weniger eingriffsintensive, aber gleichwohl gleich wirksame Alternative gibt.[266] Sie trägt aber dem Umstand Rechnung, dass die verantwortliche Stelle im Gegensatz zum Staat nur einer mittelbaren Drittwirkung der Grundrechte ausgesetzt ist. [267] Deswegen entfällt ein strenger Verweis auf das mildeste Mittel und die Grundrechtsabwägung erfolgt im Wege praktischer Konkordanz erst bei der Frage des Überwiegens der Interessen des Betroffenen. Ausschließen soll das Erforderlichkeitskriterium nur die Erhebung solcher Daten, die zu dem verfolgten Interesse nichts beitragen können (Geeignetheit), und solche, deren Erhebung unterbleiben kann, ohne dass die Zweckerreichung in Frage steht (Erforderlichkeit im engeren Sinne). Hieraus ergeben sich bereits zwei Einschränkungen der Zuspeicherung: Zunächst ist tatsächlich zu prüfen, ob ein erhobenes Datum etwa für eine konkret geplante statistische Erhebung relevant ist. Dies verbietet es, einen Datenstrom ungeprüft dem CRM zuzuführen. Zum anderen ist zu prüfen, ob trotz Relevanz nicht auf die Erhebung verzichtet werden kann, bzw., ob ein Verzicht sich negativ auf die Wirksamkeit der zulässigen Maßnahme auswirkt. Dies ist eine praktische Form der Umsetzung in § 3a Satz 1 BDSG ausgestalteten Prinzips der Datenvermeidung**.**

Die Zuspeicherung ist nur rechtmäßig, wenn kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt. Wie bereits im Kapitel zur Erhebung besprochen, ist damit ein grundsätzlicher Vorrang der Betroffenenrechte ausgedrückt, weil der CRM-Betreiber sich wegen der fehlenden allgemeinen Zugänglichkeit nicht auf einen pauschalen Grundrechtsschutz nach Art. 5 Abs. 1 Satz 1, 2. Alt. GG berufen kann. Gleichzeitig geht aus dem Europarecht hervor,[268] dass die verantwortliche Stelle die Wahrscheinlichkeit, dass ihr Interesse bei der Abwägung berücksichtigt wird, verbessern kann, wenn sie sog. *additional safeguards* (weitergehende Sicherungsmittel) bereitstellt, die die Auswirkungen auf die Grundrechte der Betroffenen auf ein hinnehmbares Maß einschränken.

Anders als bei der Verarbeitung und Nutzung zum Zwecke der Statistik steht die Anonymisierung als wirksamstes Werkzeug nicht zur Verfügung. Auch die Getrenntspeicherung der Kundendatenbank wurde bereits als Voraussetzung dafür erwähnt, dass eine Rechtfertigung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG überhaupt in Betracht kommt. Sie kann danach nur in begrenztem Umfang erneut zugunsten der verantwortlichen Stelle als Argument verwendet werden.

Fraglich ist, ob die verantwortliche Stelle die Richtigkeit der zugespeicherten Daten prüfen muss. Es gilt zunächst das Prinzip, dass ein berechtigtes Interesse ausschließlich an zutreffenden Daten besteht[269]. Dieses Interesse ist im Rahmen von § 28 Abs. 1 Satz 1 Nr. 2 BDSG gesondert darzulegen. Auch hier muss

---

[265] Schaffland/Wiltfang, BDSG, § 28, Rn. 110; Taeger, in: Taeger/Gabel, BDSG, § 28, Rn. 150.

[266] OVG Bremen NVwZ-RR 2005, S. 314; Aschke, in: Bader/ Ronellenfitsch, VwVfG, § 40, Rn. 55.

[267] Herdegen in Maunz/Dürig, GG, § 1, Rn. 99.

[268] Insb. WP 217 „Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" der Art.-29-Datenschutzgruppe.

[269] Vgl. Ambs, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 28 BDSG, Rn. 11.

aber auf die geplante weitere Nutzung abgestellt werden. Kann mit den Daten dem Zweck nach ein Nachteil für den Betroffenen eintreten, hat die verantwortliche Stelle die Richtigkeit der Daten zu prüfen, damit die Interessenabwägung zu seinen Gunsten ausschlagen kann. Der Begriff ist weit zu verstehen. Er umfasst nicht nur ungünstige Konditionen für den Betroffenen bei Vertragsabschlüssen oder das versehentliche Zusenden von unbestellten Waren, sondern auch etwa das Anspracheverhalten der verantwortlichen Stelle und jede Form der persönlichen Missbilligung. Daher gilt, dass de facto eine Prüfpflicht für die allermeisten Fälle der Zuspeicherung, in denen der Personenbezug aufrechterhalten bleibt, gegeben ist. Die verantwortliche Stelle ist daher insbesondere verpflichtet, sich zumindest nachweisbar um Verifizierung der Richtigkeit gespeicherter Daten zu bemühen.[270] Das steht folglich jedenfalls einer rein automatisierten Speicherung entgegen. Eine Prüfpflicht dürfte dagegen nicht bestehen, wenn Daten sofort anonymisiert werden und gesondert gespeichert werden. Eine zumindest subjektive Bestandsaufnahme über alle Daten ist jedoch spätestens zur Einhaltung der Berichtigungspflicht (§ 35 Abs. 1 Satz 1 BDSG) zwingend erforderlich. Hier darf sich die verantwortliche Stelle nicht auf eine „Einspruchslösung" verlassen, sondern muss von sich aus die Berichtigung unrichtiger Daten vornehmen.[271]

Gemäß § 33 BDSG ist im Falle der nicht vom Betroffenen initiierten Speicherung von Daten dieser über den Umstand der Speicherung in Kenntnis zu setzen. Gegebenenfalls wird die Pflicht zur Benachrichtigung jedoch von § 33 Abs. 2 Nr. 7, Var. a) BDSG ausgeschlossen, nach dem die Speicherung von Daten aus allgemein zugänglichen Quellen dann keine Benachrichtigungspflicht zur Folge hat, wenn die Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig wäre. Dies ist jedenfalls dann eng auszulegen, wenn die verantwortliche Stelle freiwillig und ohne dazu vertraglich verpflichtet zu sein Daten erhebt, Dabei hat sie den Umfang der Datenerhebung in der Hand und führt die Unverhältnismäßigkeit in der Regel selbst herbei. Des Weiteren muss sich die Unverhältnismäßigkeit gerade aus der Vielzahl der Fälle ergeben. Die schlechte Greifbarkeit der Betroffenen ist dagegen kein grundsätzlicher Ausschlussgrund.[272] Schließlich hat der Wegfall der Benachrichtigungspflicht gemäß § 34 Abs. 7 BDSG auch den Wegfall der Pflicht zur Auskunftserteilung über die zu einer Person gespeicherten Daten zur Folge. Dies bedeutet einen tiefen Einschnitt in das Recht auf informationelle Selbstbestimmung, der nicht bereits aus Bequemlichkeitserwägungen gerechtfertigt werden kann. Unverhältnismäßig ist die Benachrichtigung daher nur, wenn nachgewiesen werden kann, dass eine Überlastung trotz ordnungsgemäßer Ressourcenplanung eintritt, und kann deswegen nur ausnahmsweise und vorübergehend anerkannt werden. Ist die Benachrichtigung praktisch nicht durchführbar, obwohl keine Ausnahme des § 33 greift, ist bereits die Datenerhebung rechtswidrig.

Im Bereich des Social CRM ist die Benachrichtigung des Betroffenen regelmäßig kein Problem. Es genügt meist, das erhobene Datum zu einem Social-Media-Account zurückzuverfolgen. Einer Identifizierung der dahinterstehenden natürlichen Person bedarf es in der Regel nicht. Zwar ist Betroffener immer die natürliche Person, auf die sich das erhobene Datum bezieht. Es ist insoweit denkbar, dass ein Dritter einen Account erstellt. Von einem solchen Sachverhalt muss jedoch nur bei Vorliegen konkreter Anhaltspunkte ausgegangen werden. Ergeben sich indes solche Anhaltspunkte, darf schon das Datum nicht erhoben

[270] Simitis, in: Simitis, BDSG, § 28, Rn. 33.

[271] Gola/Schomerus, BDSG, § 35, Rn. 3; Meents, in: Taeger/Gabel, BDSG, § 35, Rn. 8.

[272] Dix, in: Simitis, BDSG, § 33, Rn. 100; Meents, in: Taeger/Gabel, BDSG, § 33, Rn. 50.

werden, so dass sich das Problem nicht stellt. Weitergehende Aufklärungspflichten hat die verantwortliche Stelle nicht.

Die Befugnis zur formlosen Nachricht über das soziale Medium gilt jedenfalls dann, wenn die betreffende Plattform eine Form der verdeckten Ansprache zulässt. § 33 BDSG enthält keine Formvorschriften,[273] daher reicht die nichtsigniert-elektronische Form zur Benachrichtigung aus, wenn sichergestellt ist, dass die Nachricht dem Betroffenen als Belehrung auffällt.[274] Zu belehren ist über die Art der Daten, die Zweckbestimmung und die Identität der verantwortlichen Stelle, insbesondere Kontaktdaten, die eine unverzügliche Ausübung der Rechte nach §§ 34, 35 BDSG ermöglichen.[275]

Schließlich ist noch auf Probleme der Drittbezogenheit von Äußerungen einzugehen. Dass die Erhebung drittbezogener Aussagen nicht grundsätzlich am Direkterhebungsgrundsatz scheitert, ist bereits oben ausgeführt worden. Allerdings wird man nach § 33 BDSG bei der Erhebung drittbezogener Äußerungen sowohl denjenigen, der die Äußerung getätigt hat, als auch denjenigen, auf den sich die Aussage bezieht, benachrichtigen müssen. Insoweit sind (mindestens) zwei personenbezogene Daten erhoben worden, nämlich der Umstand der Äußerung als Einzelangabe über sachliche Verhältnisse des Accountinhabers und der Inhalt der Aussage. Ist der Dritte, auf den sich die Aussage bezieht, allerdings nicht greifbar, fällt eine Benachrichtigungspflicht als unzumutbar (§ 33 Nr. 7a) weg. Das Datum bleibt dagegen grundsätzlich weiterhin erhebbar.

2.8 Datenschutz auf der eigenen Plattform – Social Community Management

In der Praxis greifen die meisten Unternehmen für ihre Social-Media-Strategie in erheblichem Maße auf die bereits vorhandenen großen Plattformen zurück.[276] Diese haben den Vorteil, dass bereits eine breite Nutzerbasis zur Verfügung steht, und daher die Möglichkeit besteht, ohne besonderen Aufwand ein großes Publikum zu erreichen.

Aus datenschutzrechtlicher Sicht lohnt es sich jedoch, auch die Fälle zu betrachten, in denen Unternehmen auf einer von ihnen selbst unterhaltenen Plattform soziale Inhalte zur Verfügung stellen. Zum einen ist die technische Hemmschwelle für den Aufbau eigener Blogs oder Foren stark gesunken. Zum anderen ist die Rechtslage im Hinblick auf vollständig selbst betriebene Plattformen gesetzlich und in der Rechtsprechung wesentlich besser geklärt als diejenige auf Drittplattformen. Es ist daher angezeigt, bei der Begutachtung zunächst von den Wertungen der selbstbetriebenen Plattformen auszugehen und zu prüfen, inwieweit diese auf Drittplattformen (Kapitel 2.9) übertragbar sind. Erst dann ist es auch möglich, eine Beurteilung der Zulässigkeit einzelner kommunikativer (insbesondere vom Unternehmen in das soziale Medium einwirkender) Verarbeitungs- und Nutzungsschritte (Kapitel 2.10) vorzunehmen.

Das Bereitstellen von Möglichkeiten für Nutzer, sich auf der Webseite der verantwortlichen Stelle gegenseitig auszutauschen und Inhalte zu teilen, macht die verantwortliche Stelle zum Anbieter von Tele-

[273] Auernhammer, BDSG, § 33, Rn. 8; Meents, in: Taeger/Gabel, BDSG, § 33, Rn. 19.

[274] Dix, in: Simitis, BDSG, § 33, Rn. 36.

[275] Meents, in: Taeger/Gabel, BDSG, § 33, Rn. 14.

[276] Draheim/Lehmann, GRUR-Prax 2014, 401.

medien (§ 1 Abs. 1 Satz 1 TMG). Im Folgenden wird im Anwendungsbereich des Telemediengesetzes statt des Begriffs „verantwortliche Stelle“ das Wort „Anbieter“ und für „Betroffener“ das Wort „Nutzer“ gebraucht werden. Für die Regelung des Anbieter-Nutzer-Verhältnisses gelten neben den allgemeinen Datenschutzbestimmungen zusätzlich die Vorschriften des Telemediengesetzes**.** Dies hat erhebliche Auswirkungen insbesondere auf die folgenden Bereiche:

- Befugnis zur Datenerhebung ohne Einwilligung,
- nach TMG einwilligungsfähige Datenerhebungsvorgänge und Wirksamkeitsvoraussetzungen der Einwilligung,
- Befugnis zur Erhebung nach BDSG,
- Transparenz- und sonstige Betreiberpflichten,
- Haftung für Nutzerverhalten.

2.8.1 Einwilligungsfreie Datenerhebung nach TMG

Wie das BDSG sieht auch das Telemedienrecht ein Erhebungsverbot mit Erlaubnisvorbehalt (§ 12 Abs. 1 TMG) vor. Wie die Formulierung der Vorschrift nahelegt, beschäftigt sich das TMG in seinem Datenschutzabschnitt ausschließlich mit Daten, die anlässlich der Bereitstellung von Telemedien anfallen. Dies deckt freilich nur einen Teil derjenigen Daten ab, an deren Auswertung der Anbieter in der Regel interessiert ist. Die beiden Datenarten, für die das Telemedienrecht eigene Vorschriften enthält sind die Bestandsdaten (§ 14 TMG) und die Nutzungsdaten (§ 15 TMG). Sonstige Daten, insbesondere die Postings und Beiträge der Nutzer selbst, gelten als Inhaltsdaten und sind gemäß § 12 Abs. 3 TMG mangels eigener Regelung nach dem BDSG zu beurteilen.

Zunächst sind die Erlaubnistatbestände des TMG zu beleuchten. Bestandsdaten sind danach diejenigen Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen Anbieter und Nutzer erforderlich sind (§ 14 Abs. 1 TMG). Datenverarbeitungen, die das für diese Zwecke erforderliche Maß überschreiten, sind nicht von § 14 TMG erfasst und bedürfen regelmäßig einer Einwilligung. Allerdings kann die erforderliche Einwilligung in diesem Fall an der Freiwilligkeit scheitern. Deutlich wird dies etwa, wenn der Anbieter den Login zu seinem Angebot mit dem eines sozialen Netzwerks verknüpft, um an die Accountdaten des Nutzers bei dem sozialen Medium zu gelangen. Die Erhebung der dadurch erlangten Daten bedarf stets einer rechtmäßigen Einwilligung, jedoch wird bei ordnungsgemäßer Aufklärung regelmäßig ein psychologischer Druck beim Nutzer vorhanden sein, seine Daten preisgeben zum müssen. Eine solche Einwilligung kann unwirksam sein.[277]Das Erforderlichkeitskriterium ist mit Hinblick auf die Tatsache, dass die verantwortliche Stelle nach § 13 Abs. 6 TMG die Nutzung des Dienstes, soweit technisch möglich und zumutbar, anonym oder pseudonym zu ermöglichen hat, hier in einem strengen Sinne zu verstehen. Das bedeutet, dass im Rahmen von § 14 Abs. 1 TMG nur diejenigen Daten erhoben werden dürfen, ohne die ein Vertrag nicht wirksam zustande kommen könnte[278]

[277] Moser-Knierim, ZD 2013, S. 263ff.

[278] Müller-Broich, TMG, § 14, Rn. 2 f.

Ein Vertrag kann zunächst in der Abrede über die entgeltliche Benutzung des Telemediums bestehen. Dies ist im Bereich des Social CRM sehr selten, da es dem Anbieter in der Regel darauf ankommt, die Schwelle zur Teilnahme möglichst niedrig zu halten. Ist ein Telemedium kostenpflichtig, kann es dem Anbieter nicht verwehrt sein, den Nutzer als Schuldner so zu identifizieren, dass im Falle der Nichtzahlung die Einleitung rechtlicher Schritte möglich ist. Dies umfasst jedenfalls die Berechtigung zur Erhebung des vollständigen Namens, einer ladungsfähigen Anschrift und notwendige Details der jeweiligen Zahlungsart.[279]

Wesentlich häufiger ist die unentgeltliche Nutzungsgewährung. Fraglich ist, ob in diesem einseitigen Gewährungsakt bereits ein Vertrag liegt. Ein Vertrag ist ein mehrseitiges Rechtsgeschäft von korrespondierenden Willenserklärungen (Angebot und Annahme), aus dem ein (nicht notwendig mehrseitiges) Schuldverhältnis entsteht.[280] Die Annahme muss durch ein schlichtes „Ja" erfolgen können. So liegt es hier zunächst. Der Anbieter stellt z.B. ein Formular zur Verfügung, das der Nutzer nur ausfüllen muss, um in einem Forum aktiv sein zu können. Alternativ kann auch direkt ein Upload-Formular etwa für Bilder bereitgestellt werden. Dadurch nimmt der Nutzer das Angebot durch Ingebrauchnahme des Telemediums (gegebenenfalls konkludent) an. Voraussetzung für ein Vertragsverhältnis im Sinne von §§ 14 Abs. 1 TMG, 311 BGB ist allerdings, dass es sich nicht um eine reine Gefälligkeit des Anbieters handelt, sondern ein Rechtsbindungswille besteht. Das Landgericht München I hat dies für Foren in einer Entscheidung aus dem Jahre 2006 bejaht.[281] Dem wird man schon wegen des telemedienrechtlich mit der Auferlegung von Pflichten verbundenen Anbieter-Nutzer-Verhältnisses beipflichten müssen. Allerdings treffen den Nutzer üblicherweise keine Verpflichtungen gegenüber dem Anbieter, die die Erhebung von Daten nötig machten, die über die Abgrenzung des Betroffenen von anderen Nutzern hinausgingen. Dies wird typischerweise durch die Registrierung mit einer gültigen E-Mail-Adresse erreicht. Darüber hinaus kann der Anbieter aus § 14 Abs. 1 TMG in solchen Fällen üblicherweise keine weiteren Erhebungsrechte für sich in Anspruch nehmen.

Nutzungsdaten sind gemäß § 15 TMG diejenigen Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Es handelt sich gemäß § 15 Abs. 1 Satz 2 TMG um Daten, die der Nutzer während der Inanspruchnahme des Telemediums ohne sein Zutun hinterlässt, insbesondere ein eindeutiges Identifikationsmerkmal (in aller Regel die IP-Adresse),[282] die Bezeichnung der genutzten Telemedien und die Zeitspanne, für welche die Nutzung erfolgt ist. Auch diese Norm ist ursprünglich auf entgeltliche Nutzungen zugeschnitten worden. Sind die verarbeiteten Daten zur Abrechnung erforderlich, dürfen sie über den Nutzungsvorgang hinaus gespeichert und genutzt werden (§ 15 Abs. 4 TMG). Für die Bereitstellung unentgeltlicher Medien ist die Kenntnis der Nutzungsdaten einschließlich der IP dagegen oft nicht im strengen Sinne erforderlich. Auch das Interesse an der Identifizierung von Nutzern, die das Telemedium missbräuchlich verwenden ist kein Fall der Erforderlichkeit zur Bereitstellung gemäß § 15 Abs. 1 TMG. Einziger Fall zur Berechtigung der rechtmäßigen Datenspeicherung ist die Säumigkeit des Nutzers in der Begleichung des Entgelts (§ 15 Abs. 8 TMG). Soll darüber hin-

---

279 Simitis, in: Simitis, BDSG, § 28, Rn. 60; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 18.

280 Mansel, in: Jauernig, BGB, § 145, Rn. 1 ff.

281 LG München I, 30 O 11973/05.

282 Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 15 TMG, Rn. 2.

aus eine Erhebung stattfinden, muss diese auf andere gesetzliche Erlaubnistatbestände gestützt oder eine Einwilligung eingeholt werden.

Eine besondere, einwilligungsfreie Erlaubnisnorm zur Erhebung von Daten ist § 15 Abs. 3 TMG. Danach darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Es handelt sich dabei um eine im deutschen Datenschutzrecht einzigartige, ausdrückliche Berechtigung zur Profilbildung zu Werbezwecken mit Opt-Out-Regelung.[283] Die kontinuierliche Datenerhebung, die der Profilbildung vorausgeht, wird üblicherweise Tracking genannt.[284] Die Daten werden dazu von einer sogenannten Analytics-Software aggregiert und aufbereitet.

Zweck kann Werbung und Marktforschung sein. Es sind die bereits umrissenen Begriffe der §§ 28 Abs. 3, 30a BDSG entsprechend heranzuziehen. Ebenfalls zulässig als Zweck ist die bedarfsgerechte Gestaltung, d.h. die inhaltliche Anpassung des Telemediums an die Interessen der Nutzer. Voraussetzung ist, dass die Profilbildung „bei Verwendung von Pseudonymen" geschieht. Die Präposition „bei" heißt hier so viel wie „im Falle von". Das bedeutet, dass eine Datenerhebung nach § 15 Abs. 3 TMG nur dann zulässig ist, wenn die Nutzung unter Pseudonym (§ 13 Abs. 6 TMG) gewährt wird.[285] Im Rahmen des § 15 TMG, bei dem Daten gerade vom Nutzer unbeeinflusst entstehen, ist dabei nicht ausreichend, dass der Betroffene selbst ein Pseudonym etwa als Benutzernamen wählt. Die Pseudonymisierungspflicht bezieht sich vielmehr auf das personenbezogene Nutzungsdatum, regelmäßig die IP-Adresse (s.o.). Dass bedeutet, dass die Analytics-Software, welche die genannten Profile erstellt, hierfür im Regelfall keine vollständigen IPs erheben darf, sondern nur einen Teil, der ein von anderen Nutzern abgrenzbares Profil ermöglicht, ohne den Nutzer für die verantwortliche Stelle bestimmbar zu machen. In der Praxis werden hierzu die hinteren Oktette der IP durch Nullzeichen ersetzt. Bei Entfernung zweier Oktette ist eine Bestimmung üblicherweise nicht mehr möglich[286]. Die Nutzungsprofile dürfen nach § 15 Abs. 3 Satz 3 TMG nicht mit Daten über die hinter dem Profil stehende natürliche Person, insbesondere nicht mit Bestandsdaten, zusammengeführt werden. Eine solche Reidentifikation würde den Sinn der Privilegierung konterkarieren. Durch die partielle Löschung der IP wird diese wesentlich erschwert. Wer dagegen Profile mit vollständigen IP-Adressen erheben will, wie dies die meisten Analytics-Programme standardisiert tun, benötigt eine Einwilligung vor Beginn der Nutzung.

Unklarheit herrscht in dieser Hinsicht nach wie vor über die Auswirkungen des Art. 5 Abs. 3 der ePrivacy-Richtlinie (2002/58/EG in der Fassung 2009/136/EG). Der Wortlaut der Richtlinie sieht vor, dass „die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer […] seine Einwilligung gegeben hat. Hauptanwendungsfall ist dabei das Speichern von Cookies. Cookies hingegen sind verbreitete Werkzeuge zur Erstellung der in § 15 Abs. 3 TMG geregelten Nutzungsprofile.

283 Gabriel/Cornels, MMR 2008, XIV (XVI).

284 Alich/Voigt, CR 2012, S. 344.

285 Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 15 TMG, Rn. 7.

286 Vgl. die Ausführungen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zum beanstandungsfreien Betrieb von Google Analytics. Abrufbar unter: https://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html.

Damit ist nach EU-Recht ein Opt-In des Nutzers vor Setzen des Cookies erforderlich während nach deutschem TMG die darauf gestützte Erstellung pseudonymer Nutzungsprofile nur einen Opt-Out erfordert. Dieser Widerspruch ist bisher nicht aufgelöst. Eine Änderung des deutschen Telemedienrechts ist nicht erfolgt. Die deutsche Bundesregierung sowie die EU-Kommission vertreten die Auffassung, dass trotz dieses Widerspruchs eine Umsetzung der Richtlinie bereits erfolgt sei. Vertreter der datenschutzrechtlichen Literatur verweisen stattdessen auf bestehende Diskrepanzen: Ziel der europäischen Richtlinie war die technikneutrale Regulierung von (unter anderem) Cookies. Das deutsche Telemedienrecht unterscheidet hingegen nach wie vor zwischen personenbezogenen Cookies und nach deren Einsatzzweck. Die unterschiedlichen Rechtsfolgen etwa beim Einsatz von Cookies für Nutzungsprofile zeige, dass eine vollständige Umsetzung nach wie vor nicht gegeben sei.[287]. Mangels Umsetzung in deutsches Recht und mangels unmittelbarer Anwendbarkeit der EU-Richtlinie sehen die Aufsichtsbehörden aktuell von Maßnahmen ab.

2.8.2 Einwilligungsfreie Erhebung von Inhaltsdaten

Der Anbieter, der etwa ein Forum einrichtet, hat ein natürliches Interesse daran, auch die Postings zu erheben und auszuwerten, sei es zu Servicezwecken oder zur Beurteilung der Einstellung der Poster gegenüber dem Unternehmen. Dies gilt umso mehr, wenn das Telemedium in einem Preisausschreiben oder einem ähnlichen Wettbewerb besteht, in dem gerade die Einsendung von Beiträgen im Vordergrund steht. Die hierbei entstehenden Daten können nicht den §§ 14, 15 TMG zugeordnet werden.[288] Sie unterfallen als Inhaltsdaten dem BDSG. Der Großteil der datenschutzrechtlichen Lehre geht davon aus, dass alle Vorschriften des Bundesdatenschutzgesetzes auf Inhaltsdaten anwendbar sind.[289] Der Anbieter tritt als verantwortliche Stelle dem Nutzer in Bezug auf Inhaltsdaten wie einem beliebigen Dritten entgegen. Die Erhebung von Daten auf eigenen Foren muss also nicht notwendig auf Basis von Einwilligungen geschehen, sondern kann unter Umständen ebenfalls durch § 28 Abs. 1 Satz 1 Nr. 3 BDSG gerechtfertigt werden.

Es scheint zwar paradox, die eigene Webseite als eine allgemein zugängliche Quelle anzuerkennen. Dass Inhalte, zu deren Übermittlung der Anbieter selbst im Rahmen von Kampagnen die Nutzer aufgerufen hat, nunmehr über § 28 zu erheben sein sollen, ist nicht leicht einzusehen. Die eigenen Telemedien von diesen Erhebungsbefugnissen auszunehmen und damit von einer Einwilligung abhängig zu machen, würde aber zu einem Wertungswiderspruch führen. Folge wäre nämlich, dass der Anbieter unter erhebungsfreundlicheren Bedingungen fremde Webseiten auswerten dürfte als eigene. Gleichzeitig muss der Anbieter auch seiner Pflicht zur nachträglichen Sperrung rechtswidriger Inhalte, die durch Dritte gepostet wurden, nach § 7 Abs. 2 TMG nachkommen können. Ihm darf daher ein Überblick über diese Inhalte nicht grundsätzlich verwehrt werden.

Die Frage der Zulässigkeit hängt damit von der Zwecksetzung ab. Seine Grenzen findet die Rechtfertigung über § 28 Abs. 1 Satz 1 Nr. 3 BDSG abermals im Rahmen der Datenverarbeitung zu Werbezwecken.

---

[287] Vgl. etwa Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 15 TMG, Rn. 9.

[288] Bucher, DuD 2012, S. 767.

[289] Müller-Broich, TMG, § 12, Rn. 3; Schmitz, in: Spindler/Schmitz/Geis, TDG, § 3 TDDSG, Rn 8.

Viele Telemedien betreiben personalisierte Werbung, um sich zu finanzieren. Da dies grundsätzlich die Erhebung von über § 14 TMG hinausgehende Bestandsdaten voraussetzt, besteht für die Anbieter also regelmäßig Veranlassung, eine Einwilligung einzuholen. Dies folgt aus § 28 Abs. 3 Satz 1 BDSG, der abseits des Listenprivilegs die Datenverarbeitung zu Werbezwecken von einer Einwilligung abhängig macht. Die Regelung des § 15 Abs. 3 TMG bezieht sich nur auf die Zulässigkeit der Verarbeitung von Nutzungsdaten, nicht auf die Auswertung von Inhaltsdaten. Sollen also Inhaltsdaten der Nutzer zu Werbezwecken verarbeitet werden, ist dazu trotz der allgemeinen Zugänglichkeit der Inhaltsdaten die Einwilligung der Nutzer notwendig. Diese Einwilligung wird praktisch aber regelmäßig mit dem Akzeptieren der Nutzungsbedingungen verknüpft werden und genügt damit grundsätzlich der Form des § 13 Abs. 2 TMG. Ob die erleichterte Einwilligung des TMG für Datenverarbeitungen von Inhaltsdaten aber überhaupt anwendbar ist, wird später diskutiert[290].

Entscheidend für die Frage, in welchem Maße eine Datenerhebung auf eigenen Foren ohne datenschutzrechtliche Einwilligung denkbar ist, ist also wie stets die Zwecksetzung. Eine Ansprache auf eigenen Foren dürfte in aller Regel zulässig sein. Erhebungen von ansonsten allgemein zugänglichen Inhalten sind daher praktisch immer zulässig. Zulässiger Zweck dürfte auch die Ausübung des von der Rechtsprechung anerkannten „virtuellen Hausrechts" sein,[291] also dem Ausschauhalten nach Äußerungen, die die eigenen Richtlinien verletzen und gegebenenfalls den Ausschluss von Personen zur Folge haben können. Dasselbe gilt für Chaträume, wenn diese dem Service dienen. Kein Einsichtsrecht auch nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG dürfte dagegen an Daten bestehen, die zwischen Nutzern verdeckt ausgetauscht werden, wenn die Plattform einen solchen Austausch zulässt. Dies gilt insbesondere für Privatnachrichten auf Forensystemen und im Chat. Vor dem Hintergrund der in solchen Chats geltenden *reasonable expectation of privacy*[292] dürfte selbst ein Recht zur Speicherung solcher Nachrichten nur zum Abwehr von gegenwärtigen Angriffen auf den Bestand der Plattform zulässig sein. Die Einholung einer ordnungsgemäßen Einwilligung bleibt hiervon unberührt.

2.8.3 Die Einwilligung im Telemedienrecht

Nach alledem können zwei Fälle von Einwilligungserfordernissen unterschieden werden. Im ersten Fall fallen die zu erhebenden Daten bei der Bereitstellung an. Sie entsprechen den Datenarten nach §§ 14, 15 TMG, sind jedoch dem Umfang der Erhebung nach für die Bereitstellung nicht erforderlich. Solche Datenerhebungen erfolgen regelmäßig im Zusammenhang mit Gewinnspielen, bei der Nutzung von Apps, aber auch bei allgemeinen Registrierungsvorgängen, wenn die verantwortliche Stelle sich nicht mit den Grenzen von § 14 TMG begnügen will. Im zweiten Fall werden Inhaltsdaten erhoben und der Vorgang ist nicht nach den gesetzlichen Tatbeständen zu rechtfertigen. Fraglich ist, ob diese beiden Fälle unterschiedliche Voraussetzungen haben.

---

290 Siehe genauer unter 2.8.3 Die Einwilligung im Telemedienrecht

291 LG München I, 30 O 11973/05.

292 Die Rechtsfigur des „reasonable-expectation-of-privacy-test" verwendet der EuGH, u.a. im Urt. v. 25.06.1997, Slg. 1997-III, S.1016.

Die einzige Vorschrift im Telemediengesetz, die sich spezifisch auf die Einwilligungserfordernisse bezieht, ist § 13 Abs. 2 TMG. Die Vorschrift enthält als einzigen Regelungsinhalt eine Formvorschrift, die als Lockerung im Vergleich zu § 4a BDSG konzipiert ist. Während § 4a Abs. 1 Nr. 3 BDSG von der Schriftform und der ihr äquivalenten elektronischen Form durch qualifizierte Signatur ausgeht und eine Abweichung nur in begründeten Ausnahmefällen zulässt, lässt § 13 Abs. 2 TMG die „elektronische Erklärung", d.h. die Textform gemäß § 126b BGB in Gestalt einer unsignierten digitalen Erklärung unter gewissen Umständen ausdrücklich genügen.

Voraussetzung ist zunächst eine „bewusste und eindeutige" Einwilligung (§ 13 Abs. 2 Nr. 1 TMG). Beides ist bereits von der allgemeinen datenschutzrechtlichen Einwilligung zu fordern. Es wird ein Protokoll der Einwilligung gefordert, welches jederzeit abrufbar sein muss (§ 13 Abs. 2 Nr. 2, 3 TMG). Schließlich müssen Arbeitsabläufe vorhanden sein, welche im Falle eines Widerrufs die Weiternutzung der betreffenden Daten verhindern.

Ansonsten gelten die inhaltlichen Anforderungen entsprechend § 4a BDSG. Auf die Bedeutung der Freiwilligkeit wurde bereits hingewiesen. Auch müssen Datenarten und Zwecke ausreichend konkret benannt sein.

Fraglich ist zunächst, ob die Formlockerung des § 13 Abs. 2 TMG auch für die Einwilligung in die Erhebung von Inhaltsdaten gilt, obwohl materiell das TMG gerade unanwendbar ist. Zwar umreißt § 12 Abs. 1 den Anwendungsbereich des TMG auch insoweit scheinbar abschließend auf die Daten nach §§ 14, 15. Die Folge einer ausschließlichen Anwendung von § 4a Abs. 1 Satz 3 BDSG auf die vorliegende Einwilligung wäre allerdings widersinnig. Es wären zwei Varianten der Rechtsanwendung für die Formvorschrift von § 4a BDSG auf Inhaltsdaten von Telemedien denkbar: Entweder, es werden für Telemedien regelmäßig besondere Umstände anerkannt, wegen derer eine Abweichungsbefugnis für die Textform in Frage kommt, oder dies ist nicht der Fall. Wird der Anbieter in letzterem Fall auf die Schriftform verwiesen, müsste auch für Vorgänge, die sich auf Wunsch des Nutzers und ausschließlich auf elektronischen Medien abspielen, dieser auf den Umweg über die Papierform verwiesen werden. Werden aber besondere Umstände anerkannt, so steht der Nutzer mit § 4a BDSG schutzloser und damit schlechter, als er es im Falle von § 13 Abs. 2 TMG täte. § 13 Abs. 2 TMG ist nämlich auf die unsignierte digitale Einwilligung mit sachgerechten Regelungen zugeschnitten, wobei solche Regelungen bei § 4a BDSG vollkommen fehlen. Dies kann so nicht gewollt sein. Es ist daher davon auszugehen, dass § 13 Abs. 2 TMG zumindest insoweit an die Stelle von § 4a Abs. 1 Satz 3 BDSG tritt, als dass die den Nutzer schützenden Vorschriften gemäß § 13 Abs. 2 Nrn. 1-4 und Abs. 3 anwendbar sind. Die Einholung von Online-Einwilligungen und damit eine weite Anwendung des § 13 Abs. 2 TMG auf alle datenschutzrechtlichen Einwilligungen, die sich auf Vorgänge im Anbieter-Nutzer-Verhältnis beziehen, entspricht auch der gängigen Praxis.

2.8.4 Transparenz- und andere Anbieterpflichten

Die entscheidenden Betreiberpflichten ergeben sich aus § 13 TMG. Die wichtigste ist die Aufklärungspflicht nach § 13 Abs. 1 TMG. Die Aufklärung hat „zu Beginn des Nutzungsvorgangs" zu erfolgen. Dies bedeutet, dass die Datenschutzerklärung von der Startseite aus erreichbar sein muss; eine Information

bereits vor Aufruf der Startseite ist hingegen nicht erforderlich.[293] Aufzuklären ist über Art und Umfang der Datenerhebung und deren Zweck sowie gegebenenfalls über die Übermittlung ins Nicht-EWR-Ausland. Werden Profile nach § 15 Abs. 3 TMG angelegt, ist über die Möglichkeit zum Opt-Out zu informieren und eine Option zur unmittelbaren Nutzung dieses Rechts zur Verfügung zu stellen. Wird die Aufklärung mit einer Einwilligungserklärung verbunden, muss zudem über das Widerrufsrecht im Hinblick auf die Einwilligung belehrt werden. Die Aufklärung muss mit einem deutlichen Hinweis von jeder Seite des Telemediums aus verfügbar sein.[294]

Sollen darüber hinausgehende Nutzungsbedingungen zum Gegenstand des Nutzungsvertrags gemacht werden, müssen die besonders hervorgehoben vor Beginn der Nutzung dem Betroffenen zur Kenntnis gelangen.

Etwa zu erteilende Einwilligungen dürfen nicht mit der Belehrung nach § 13 Abs. 1 TMG vermischt werden. Sie müssen möglichst von restlichen Inhalten grafisch abgetrennt sein (z.B. farblich oder durch Umrandung).[295] Da die Einwilligung laut § 13 Abs. 2 Nr. 1 TMG bewusst und eindeutig zu erfolgen hat, und die Opt-Out-Regelung von § 15 Abs. 3 TMG vom Gesetz nicht als Einwilligung angesehen wird, ist üblicherweise ein Opt-In (z.B. durch Setzen eines Häkchens zur Bestätigung der Zustimmung zum vorgefertigten Einwilligungstext nebst Klick auf einen entsprechenden „Zustimmen"-Button) erforderlich.[296]

Da Aufklärung und Einwilligung vor Beginn der Nutzung erfolgen müssen, dürfen vorher keinerlei Bestands- und Nutzungsdaten erhoben werden. Dies wird insbesondere bei den Daten nach § 15 TMG zum Problem, weil diese bereits anfallen, wenn der Browser des Nutzers erstmals die Webseite des Anbieters anspricht. Auch die pseudonyme Profilbildung nebst Tracking nach § 15 Abs. 3 TMG beginnt damit oft bereits, bevor dem Betroffenen die Belehrung zur Kenntnis gelangen kann. Dasselbe gilt für Tracker, die vollständige IP-Adressen verarbeiten. Diese werden regelmäßig bei Seitenaufruf aktiv, ohne dass dem Nutzer Gelegenheit gegeben wurde, seine Einwilligung zur Erhebung dieser Daten zu erklären.

Es ist deshalb von Tracking-Tools abzuraten, die keine Pseudonymisierungsfunktion oder jedenfalls keine Funktion, neue Nutzer bis zur Einwilligungserteilung nicht zu tracken, besitzen. Diese sind nicht datenschutzgerecht einsetzbar, weil sie bereits Daten erheben, ohne dass der Nutzer die Möglichkeit hat, dies zu unterbinden. Bei Tracking-Tools, die von Anfang an und dauerhaft durch die oben dargestellte Verkürzung der IP eine Pseudonymisierung der Profile durchführen, muss jedenfalls bei Beginn des Trackings ein sichtbarer Hinweis erfolgen.[297]

Schließlich ergeben sich aus telemedienrechtlichen Vorschriften noch allgemeine Anforderungen an die Bereitstellung des Dienstes. § 13 Abs. 4 TMG legt wie die Anlage zu § 9 BDSG sog. technisch-organisatorische Maßnahmen fest, die der Anbieter zu treffen hat. In § 13 Abs. 4 Nr. 2 TMG wird die Löschung derjenigen personenbezogenen Daten angeordnet, für deren weitere Speicherung insbesondere

---

[293] Müller-Broich, TMG, § 13, Rn. 1; s.a. BT-Drs. 14/6098, 28.

[294] Zu den Details siehe Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 13 TMG, Rn. 5.

[295] BGH, WRP 2010, S. 278, Tz. 26; Zscherpe, MMR 2004, S. 726.

[296] OLG Brandenburg, MMR 2006, S. 406; v. Nussbaum/Krienke, MMR 2009, S. 373.

[297] So trotz begrifflicher Unklarheiten i.E. richtig LG Frankfurt am Main, Urt. vom 18.02.2014, 3-10 O 86/12.

zu Abrechnungszwecken, nach § 15 Abs. 3 TMG oder aufgrund einer Einwilligung, keine Befugnis besteht. Datenschutzrechtlich wichtig ist auch Nr. 3 der Vorschrift, nach der der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen können muss. Darin liegt nach herrschender Meinung kein Zwang zur Verschlüsselung,[298] aber es müssen nachweisbar Maßnahmen ergriffen werden, welche eine Einsicht Dritter in Beiträge von Nutzern nur dann ermöglichen, wenn dies der Nutzer offenkundig bewusst zugelassen hat. Nr. 4 enthält eine Umsetzung des Getrenntspeicherungsgrundsatzes. Hat der Nutzer mehrere Dienste abonniert, dürfen die Daten über die einzelnen Dienste nicht zusammengeführt werden. So darf die Aktivität eines Betroffenen in einem Forum nur mit dessen Einwilligung etwa mit Daten zusammengeführt werden, die über die Benutzung einer App oder der Teilnahme an einem Wettbewerb gesammelt worden sind. Dies ist insbesondere bei großen Telemedienanbietern immer wieder ein Problem. So führt Google Daten seiner sämtlichen Dienste (Suchmaschine, YouTube, Google Plus, Google Mail, Google Maps u.a.) zusammen, ohne dass für die Betroffenen bei Abgabe ihrer Einwilligung hierüber ausreichende Transparenz besteht[299]. Einzige Ausnahme des Verkettungsverbots ist der Fall der Erforderlichkeit zum Zwecke der Abrechnung (§ 15 Abs. 2 TMG). Der Anbieter hat technisch-organisatorisch dafür Sorge zu tragen, dass die Zusammenführung von Daten aus unterschiedlichen Diensten auf die Abrechnung beschränkt wird und eine Reidentifikation von Profilen nach § 15 Abs. 3 BDSG nicht möglich ist.

Geschäftsmäßig und in der Regel gegen Entgelt angebotene Telemedien unterliegen darüber hinaus einer Impressumspflicht (§ 5 TMG). Wird auf der Plattform Werbung betrieben, ist diese als Werbung kenntlich zu machen (§ 6 Abs. 1 Nr. 1 TMG), seine Identität und die Kontaktdaten für die Möglichkeit des Nutzers zum Widerspruch bereithalten (§ 6 Abs. 1 Nr. 2 TMG i.V.m 7 Abs. 2 Nr. 4 b) UWG). Für das Social CRM von enormer praktischer Bedeutung ist darüber hinaus die Kennzeichnungspflicht für Gewinnspiele nach § 6 Abs. 1 Nr. 4 TMG. Wenn online ein solches Preisausschreiben zu Werbezwecken durchgeführt werden soll, ist besonders darauf zu achten, dass transparent gemacht wird, welche Daten zu welchen Zwecken erhoben werden, damit die Warnfunktion der datenschutzrechtlichen Einwilligung zur Geltung kommen kann.

2.8.5 Haftung für Nutzerverhalten

Fraglich ist für selbstbetriebene soziale Medien schließlich, in welchem Umfang der Anbieter für rechtsverletzende Inhalte auf seiner Webseite einzustehen hat, welche von Dritten eingestellt werden, und welche Ansprüche Dritte gegen ihn richten können.

Zunächst wird vorausgesetzt, dass ein Anspruch, ob auf Unterlassen oder Schadensersatz, in materieller Hinsicht überhaupt besteht. Dies ist keine Frage des Datenschutzrechts, sondern muss mit Hilfe der allgemeinen Gesetze (hier insbesondere §§ 185 ff. StGB, 823, 826 und 1004 BGB, sowie Normen des UrhG, KUG und anderer Gesetze zum Schutz des geistigen Eigentums) und der zu ihnen ergangenen Rechtsprechung geprüft werden.

---

[298] Vgl. Müller-Broich, TMG, § 13, Rn. 7.

[299] Vgl. das deshalb eröffnete Aufsichtsverfahren des Hamburgischen Beauftragen für Datenschutz und Informationsfreiheit, abrufbar unter: https://www.datenschutz-hamburg.de/news/detail/article/wesentliche-aenderungen-bei-der-datenverarbeitung-von-google-notwendig-datenschutzaufsicht-erlaess.html.

Fraglich ist zunächst, für welche Sachverhalte und welche Ansprüche eine Haftung überhaupt besteht. Ausgangspunkt ist § 7 Abs. 2 Satz 1 i.V.m 10 TMG. Danach besteht für Anbieter nach den §§ 8-10 TMG keine Prüfpflicht ohne konkreten Anlass im Hinblick auf rechtswidrige Inhalte. In der vorliegenden Konstellation richtet sich die Haftung des Anbieters nach § 10 TMG, denn er speichert insoweit fremde Inhalte, § 7 Abs. 2 ist demnach anwendbar. Es ist also nicht erforderlich, die Uploads und Postings der Nutzer dauerhaft nach rechtswidrigen Inhalten zu überprüfen. § 10 TMG enthält ein zusätzliches Haftungsprivileg,[300] indem der Anbieter nicht selbst auf Schadensersatz oder in strafrechtlicher Hinsicht haftet, wenn er die rechtswidrige Handlung nicht kannte oder kennen musste, und er sie unverzüglich nach Kenntniserlangung über den rechtswidrigen Inhalt entfernt oder gesperrt hat. Das Privileg gilt strafrechtlich auch dann, wenn von einem bestimmten Nutzer bekannt ist, dass er die Plattform zu widerrechtlichen Zwecken missbrauchen könnte,[301] es findet also keine Vorverlegung der Löschpflicht statt. Die erforderliche unverzügliche Löschung entspricht bereits der geschuldeten Tätigkeit im Falle der Geltendmachung eines Beseitigungsanspruchs (§ 1004 Abs. 1 BDSG), es wird daher deutlich, dass ein solcher nicht von dem Haftungsprivileg umfasst sein kann. Dies wird in § 7 Abs. 2 Satz 2 TMG bekräftigt. Insofern kann eine Unterlassung auch dann verlangt werden, wenn der Anbieter zum Zeitpunkt der Anspruchsstellung nicht Störer im Sinne des § 10 TMG war, weil er keine Kenntnis von der Rechtsverletzung hatte.

Beseitigt der Anbieter rechtswidrige Inhalte dagegen nicht unverzüglich, macht er sich diese zu eigen und haftet für sie wie für eigene Inhalte auch delikts- und strafrechtlich.[302] Diese Konstellation wird im hier vornehmlich relevanten Bereich des Persönlichkeitsrechts regelmäßig auftreten, wenn der angebliche Anspruchsinhaber und der Forumsbetreiber über die Rechtswidrigkeit von Inhalten uneins sind.

Für die Frage, ob eine Löschung infolge eines Unterlassungsanspruchs erfolgen muss, ist zusätzlich § 29 BDSG anzuwenden, weil ein Forumsbetreiber stets eigene oder zu eigen gemachte Beiträge zum Zwecke der Übermittlung an Dritte bereithält.[303] Nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG darf eine Speicherung aufrechterhalten werden, wenn kein Grund zur Annahme eines schutzwürdigen Interesses am Ausschluss der Erhebung vorliegt. Dabei ist die Reichweite des Schutzes des Persönlichkeitsrechts des Betroffenen im Einzelfall mit dem Informationsinteresse der Öffentlichkeit abzuwägen. Dabei muss Berücksichtigung finden, ob der Betroffene in seiner Privatsphäre oder nur in seiner Sozialsphäre (etwa beruflich) betroffen wird.[304] In letzterem Fall überwiegt oft das Informationsinteresse. Fraglich ist jedoch, ob diese Linie nach dem Google-Urteil des EuGH aufrechterhalten werden kann. Dort wird ausgeführt, dass dem Persönlichkeitsrecht grundsätzlich der Vorrang einzuräumen ist, wenn es sich um Fälle handelt, die sich seit längerem erledigt hätten.[305] Der BGH hat jedoch auch in seiner im Berichtszeitraum jüngsten Entscheidung[306]

---

300 Sieber/Höfinger, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 18.1, Rn. 46 ff.

301 KG, Beschl. v. 25.08.2014, 4 Ws 71/14.

302 BGH, GRUR 2004, 860 – Internet-Versteigerung I.

303 BGH, Urt. v. 23.06.2009, VI ZR 196/08 – Spickmich.

304 BGH, aaO.

305 EuGH, Urt. v. 13.5.2014, C-131/12.

306 BGH, Urt. v. 23.09.2014, VI ZR 358/13.

jedoch an seiner Linie festgehalten, bei Betroffenheit der Sozialsphäre der Meinungsfreiheit grundsätzlich den Vorrang einzuräumen.

Umstrittene Frage war lange die Frage der Haftung auf Auskunft gegenüber Dritten über die Identität eines Nutzers, soweit diese bekannt ist. Die Auskunft wurde regelmäßig zur Verfolgung zivilrechtlicher Ansprüche und Strafanzeigen gegen den Poster einer inkriminierten Nachricht begehrt. Trotz des Umstands, dass § 14 Abs. 2 TMG Auskunftsansprüche in Bezug auf Bestandsdaten auf Strafverfolgungs- und Gefahrenabwehrbehörden beschränkt, gaben verschiedene Instanzgerichte Klagen auf Auskunft statt. Sie unterstellten ohne einen echten Anhaltspunkt im Gesetz, § 14 Abs. 2 TMG sei nicht abschließend. Es bedurfte eines Urteils des Bundesgerichtshofs,[307] um klarzustellen, dass § 14 Abs. 2 TMG tatsächlich abschließend ist. Das Gericht führte aus, dass die grundsätzliche Pflicht zur anonymen oder pseudonymen Nutzungsgewährung (§ 13 Abs. 6 TMG) die freie Entfaltung der Meinungen ohne Angst vor Stigmatisierung gewährleiste. In diesem Sinne sei auch der Zwang zur Herausgabe von personenbezogenen Daten, die eine Person bestimmen oder bestimmbar machen, nur in Ausnahmefällen mit der Meinungsfreiheit vereinbar. Private Dritte haben demnach nach der derzeitigen Rechtslage keinerlei Auskunftsanspruch in Bezug auf die Identität von einzelnen Postern und müssen im Fall von strafrechtlich relevantem Verhalten darauf verwiesen werden, Strafanzeige zu erstatten und die notwendigen Daten durch die Strafverfolgungsbehörden erheben zu lassen. Eine Rechtsschutzlücke ergibt sich allerdings in Fällen, in denen eine Äußerung keinen Straftatbestand erfüllt und dennoch das Persönlichkeitsrecht des Betroffenen verletzt, so dass diesem ein, materieller oder immaterieller, Schaden entsteht, der von dem Unterlassungsanspruch nicht ausgeglichen werden kann. Wegen der Geltung der Meinungsfreiheit und der grundsätzlichen Zulässigkeit der Äußerung wahrer Tatsachen ist diese Lücke aber hinzunehmen.

Schließlich hat der Bundesgerichtshof in seiner „Spickmich"-Rechtsprechung[308] der Meinungsfreiheit in Foren viel Raum eingeräumt. Wenn nur die (berufliche) Sozialsphäre des Betroffenen berührt ist, bestänen keine Unterlassungs- und Schadensersatzansprüche.

2.9 Datenschutzgerechte Nutzung von Drittplattformen

Hoch umstritten ist nach wie vor die Frage, inwieweit ein CRM-Betreiber für Datenverarbeitungsvorgänge verantwortlich ist, die sich abspielen, wenn eine Seite auf einem sozialen Medium betrieben wird, das weder der Betreiber noch sein Auftragsdatenverarbeiter hostet.[309] Dies kann die Nutzung einer sog. „Fanpage" oder ähnlicher interaktiver Profile bedeuten, es existiert aber mittlerweile eine Vielzahl von Funktionen, die neben der Hauptaufgabe der Kommunikation für Marketingzwecke genutzt werden können. Thematisch gehören hierhin auch alle Datenerhebungen aus Apps, die über die Plattform betrieben werden. Der Fokus liegt wegen deren Marktübermacht auf Plattformen, deren Betreiber sich in den Vereinigten Staaten befinden, mithin in einem Drittland ohne angemessenes Datenschutzniveau im Sinne von § 4c BDSG.

[307] BGH, Urt. v. 01.07.2014, VI ZR 345/13.

[308] BGH, Urt. v. 23.06.2009, VI ZR 196/08.

[309] Überblick unter https://www.datenschutzzentrum.de/facebook.

Dass Facebook und mit ihm praktisch alle sozialen Netzwerke mehr Daten erheben, als dies nach dem Telemediengesetz ohne Einwilligung geschehen darf, ist allgemein anerkannt.[310] Bei Facebook kommt die rechtswidrige Ablegung von Tracking-Cookies und die Anlage personenbezogener Profile in unangemessen weitem Umfang hinzu, wobei der Umstand, dass entgegen § 13 Abs. 6 TMG die Benutzer zum Gebrauch von Klarnamen gezwungen werden, besonders ins Gewicht fällt. Fraglich ist, in welchem Maße der Betreiber einer Seite in einem sozialen Netzwerk durch die Eröffnung des Angebots eine rechtlich relevante Mitverantwortung daran trägt, dass sich Dritte in die Gefahr begeben, dass ihre Daten rechtswidrig verarbeitet werden. Die schleswig-holsteinische Aufsichtsbehörde vertritt in einem laufenden Verfahren die Ansicht, dass eine Verantwortlichkeit nach § 3 Nr. 7 BDSG iVm Art. 2 d) der Richtlinie 95/46/EG gegeben ist. Sie bestimmt durch das Eigeninteresse an der durch Facebook durchgeführten Datenverarbeitung und die Werbung für ihr Angebot über das Ob und Wie der Datenübermittlung mit. Da die Datenschutz-Richtlinie für die Verantwortlichkeit voraussetzt, dass über Zwecke und Mittel der Datenverarbeitung (mit-) entschieden wird, sei der Fanpage-Betreiber für die Verarbeitung durch Facebook verantwortlich.

Nach alledem müsste eine Einwilligung auch gegenüber dem Fanseitenbetreiber zur Erhebung der betreffenden Daten erfolgen, die formgerechte Einwilligung ist für die verantwortliche Stelle jedoch, wie auch Facebook zugibt, technisch überhaupt nicht zu implementieren, so dass ein rechtmäßiger Betrieb ausscheidet.

Die Instanzgerichte[311] haben diese Auffassung nicht geteilt und vertraten die Auffassung, dass die verantwortliche Stelle im Hinblick auf die Nutzungsdaten nur sein könne, wer selbst (sei es für sich oder im Auftrag für andere) Daten erhebe. Dies sei vorliegend ausschließlich Facebook. Daher benötige der Fanseitenbetreiber keine eigene Einwilligungserklärung zur Datenerhebung. Eine derartige Schutzlücke ist aber weder vom europäischen noch vom deutschen Gesetzgeber beabsichtigt. Die Art.-29-Datenschutzgruppe macht im Working Paper 169 (S. 24) gerade deutlich, dass eine gemeinsame Kontrolle auch durch Benutzung derselben Infrastruktur gegeben sein kann, wenn hieraus eine Entscheidung über die Mittel der Datenverarbeitung herbeigeführt wird. Im Bundesrecht kann nichts anderes gelten. Das Verfahren befindet sich derzeit in der Revision vor dem Bundesverwaltungsgericht[312].

Dieselben Überlegungen gelten für die Einbindung eines Social Media Button. Wie oben besprochen, handelt es sich dabei um ein in die eigene Seite eingebundenes, von einer fremden Social Media-Plattform wie Facebook oder Twitter zur Verfügung gestelltes Skript mit einem grafischen Symbol. Er dient vordergründig dazu, dass ein Betroffener, dem eine Seite gefällt, diese Tatsache mit einem Klick durch Posting auf seinen Account mit anderem teilen kann. Jedoch sorgt das Skript auch dafür, dass die IP-Adresse und gegebenenfalls Merkmale des Browsers auch dann an den Betreiber der Plattform übertragen werden, wenn dieser nicht angeklickt wird.[313] Dadurch wirkt der Button wie ein Analytics-Tool,

---

310 Vgl. Voigt/Alich, NJW 2011, S. 3541.

311 Zuletzt OVG Schleswig, Urt. v. 04.09.2014, 4 LB 20/13.

312 Siehe Pressemitteilung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, abrufbar unter https://www.datenschutzzentrum.de/artikel/770-ULD-OVG-Urteil-zu-Facebook-Fanpages-revisionsbeduerftig.html.

313 Ernst, NJOZ 2010, S. 1917.

welches von einem Dritten betrieben wird. Auf diese Weise entsteht ein umfangreiches Browsing-Profil des Nutzers ohne sein Wissen oder Zutun, welches (sofern Mitglied des Dienstes) sogar für die Anreicherung seines Profils verwendet werden kann. Eine telemedienrechtliche Rechtfertigung für die Erhebung dieser Nutzungsdaten durch die Drittplattform existiert weder in § 15 TMG noch anderswo im Telemedienrecht. Ein Mechanismus zur Einholung einer daher (gemäß § 12 Abs. 1 TMG) notwendigen Einwilligung, sehen die Buttons im unveränderten Zustand nicht vor.

Auch wenn der CRM-Betreiber aus dem Button selbst keine Daten erhebt, führt er doch eigenverantwortlich und bewusst die Gefahr der rechtswidrigen Datenerhebung durch die zugehörige Plattform herbei. Er bestimmt damit über die Mittel der Datenerhebung mit und ist datenschutzrechtlich in dieser Hinsicht ebenso zu behandeln wie im Falle selbsterhobener Daten.[314]

Das Onlinemagazin Heise.de, und ihm folgend eine Vielzahl großer deutscher Websites, hat versucht, durch die sogenannte Zweiklicklösung das genannte Problem zu umgehen. Danach wird der Button von Facebook durch einen ähnlichen Button ersetzt, der vom Server des Websitebetreibers gehostet wird und nicht auf Servern von Facebook. Im Gegensatz zum Original-Button von Facebook wird dieser Button so modifiziert, dass er zunächst ausgegraut und mit einem virtuellen Schalter versehen wird. Erst wenn dieser Schalter umgelegt wird, wird der Button aktiv. Dies kommt einer Einwilligung nach § 13 Abs. 2 BDSG jedoch nur dann gleich, wenn gleichzeitig mit der Möglichkeit dieses Opt-In eine ordnungsgemäße Aufklärung über den Verbleib der Daten, insbesondere deren Verbringung in unsichere Drittländer wie die Vereinigten Staaten, erfolgt. Später hat Heise eine Ein-Klick-Lösung vorgestellt, die ebenfalls einen Button enthält, der erst nach einer Aktion des Nutzers aktiv wird.[315] Der Anbieter, der einen solchen Button auf seiner Seite implementiert, kann sich nicht darauf berufen, dass ihm die genauen Verarbeitungsschritte der sozialen Plattform, der der Button zugehört, nicht bekannt seien und er auf diese keinen Einfluss nehmen könne. Damit liegt nahe, dass der Anbieter nicht nur über den Inhalt seines eigenen Webauftritts, sondern auch über dessen Form ohne weiteres die Entscheidungsgewalt innehat und daher über das Ob der konkreten Datenverarbeitung entscheiden kann.[316]

Wie an der Diskussion der Allgemeinen Geschäftsbedingungen von Facebook zum Einwilligungserfordernis kenntlich, geben solche „Verhaltensregeln" auf sozialen Netzwerken einen für die verantwortliche Stelle verbindlichen Rahmen vor. Da die Nutzer auf ihre Beachtung vertrauen dürfen, hat die verantwortliche Stelle an Erhebungen, die von AGB verboten werden, kein berechtigtes Interesse. In Fällen, in denen Erhebungsvorgänge per AGB auch nach Einwilligung der Betroffenen verboten sind, z.B. weil sie die API überlasten, liegt hingegen kein datenschutzrechtliches Problem vor. Die verantwortliche Stelle hat dürfte nur im Innenverhältnis zu der benutzten Plattform zu haften.

Inwieweit die (Mit-)Haftung für Datenverarbeitungsvorgänge auf Drittplattformen sich auf andere Anbieterpflichten nach dem TMG auswirkt, ist bisher ungeklärt. Es ist nach dem Obenstehenden konsequent, anzunehmen, dass im Fall der Mitbestimmung über die Mittel der Datenverarbeitung auch eine eigene Verantwortlichkeit des CRM-Betreibers für Nutzerverhalten nach den §§ 7, 10 TMG gegeben sein dürfte,

---

[314] Anders unter Ablehnung der Störerhaftung Voigt/Alich, NJW 2011, S. 3543.

[315] http://www.heise.de/-2470103.

[316] A.A. Voigt/Alich, NJW 2011, S. 3543.

da er hier mit hinreichender Einflussmöglichkeit über die Zwecke und Mittel der Datenverarbeitung entscheidet.

2.10 Aktion und Interaktion - Social Media Management

Die eigentliche Revolution im Social CRM aus betriebswirtschaftlicher Sicht liegt in der bilateralen, individualisierten Kommunikationsbeziehung. Zumindest in der Theorie wird der Betroffene gestärkt, indem er erweiterte Möglichkeiten erhält, seine Meinung zu der verantwortlichen Stelle und ihren Produkten zu äußern. Die Stelle erhält im Gegenzug die Gelegenheit, ihrerseits mit potentiellen und gegenwärtigen Kunden in Kontakt zu treten. Hierdurch tritt zwar, wie besprochen, keine gleichwertige Kommunikationssituation ein, Äußerungen von Betroffenen auf sozialen Medien, soweit sie nicht Gegenstand von Statistiken werden sollen, werden inzwischen jedoch hauptsächlich zum Kontakt auf dem Medium genutzt. Es lohnt sich also, zu prüfen, inwieweit Ansprachen von einzelnen Nutzern, aber auch drittbezogene Formen der kommunikativen Datennutzung auf sozialen Medien rechtlich zulässig sind.

Leitlinien sind bereits oben in der Frage einer möglichen konkludenten Einwilligung besprochen worden. Die in Abschnitt 2.3.3.4. hergeleiteten Wertungen können selbstverständlich nicht direkt übernommen werden. Bei der Einwilligung liegt der Schwerpunkt eher auf formellen und inhaltlichen Anforderungen an die Erklärung, in den vorliegenden Fällen dagegen auf der tatsächlichen Interessenlage, soweit sie zutage tritt. Insbesondere das Erfordernis der Eindeutigkeit von Einwilligungserklärungen ist jedoch durchaus auf die im Rahmen des § 28 BDSG regelmäßig notwendigen Interessenabwägung übertragbar. So kann unter Umständen bei Vorliegen einer eindeutigen, wenn auch formlosen, Zustimmung zu der geplanten Datenverarbeitungsmaßnahme ein Ausschlussinteresse des Betroffenen im Sinne der Nrn. 2 und 3 der Vorschrift wegfallen. Für weitere Fallbeispiele wird daher auf den genannten Abschnitt verwiesen, wobei die (bloße) Berechtigung zur Ansprache zu nichtwerblichen Zwecken jedoch an weit weniger strenge Voraussetzungen gekoppelt ist als die konkludente elektronische Einwilligung in Ansprachen mit Werbeeffekt.

Wichtigste Voraussetzung für die Anwendung des § 28 Abs. 1 Satz 1 BDSG ist damit, dass von der beabsichtigten Kommunikation kein Werbeeffekt ausgehen darf. Für eine werbende Ansprache ist nach § 28 Abs. 3 BDSG in den hier interessierenden Fallkonstellationen immer eine Einwilligung einzuholen. Die Anwendung von § 28 BDSG erfährt daher eine Einschränkung, denn die Serviceabwicklung und Informationserteilung in sozialen Netzwerken geschieht sehr häufig öffentlich. In diesen Fällen ist immer die Publizitätswirkung zu berücksichtigen, die, regelmäßig als gewollte Folge, dem Betroffenen, aber insbesondere auch Dritten in imagefördernder Weise die Qualität der Serviceleistungen demonstriert. Dies erfüllt den oben dargelegten Werbebegriff der Richtlinie.[317] Die reine, auch öffentlich einsehbare Serviceleistung ist nicht per se als Werbung anzusehen. Sie wird jedoch zu Werbung, wenn die verantwortliche Stelle nicht nur neutral z.B. eine erbetene Auskunft erteilt, sondern unter Verwendung von Phrasen des Eigenlobs oder durch Hinweis auf die Auskunftserteilung gegenüber Dritten sich die verkaufsfördernde und publizitätsstiftende Wirkung der Öffentlichkeit zunutze macht. Da die Einholung von formgerechten

[317] Für Beispiele wird auf den Abschnitt zur Werbung bei der Einwilligung verwiesen.

Einwilligungen in diesem Zusammenhang unüblich ist, dürfte die verantwortliche Stelle in der Regel auf eine neutrale Bearbeitung des Sachverhalts reduziert sein.

2.10.1 Fallgruppen

Ansprachen in sozialen Netzwerken lassen sich danach einteilen, wer den Dialog initiiert hat. Mögliche Konstellationen sind weiter oben bereits vorgestellt worden. So ist denkbar, dass die verantwortliche Stelle auf eine direkte Ansprache reagiert. Charakteristisch für diese Fallgruppe ist, dass die Ansprache eine unmittelbare Aufforderung zum Tätigwerden enthält.

Eine weniger direkte Form der Ansprache charakterisiert solche Postings, die sich zwar an das Unternehmen richten, allerdings keine Handlungsaufforderung enthalten. Dies betrifft meist Lob, Kritik oder Verbesserungsvorschläge. Inhaltlich verwandt ist die Fallgruppe der „in den Raum gestellten" Äußerungen über das Unternehmen, welche nicht an es gerichtet sind, und die durch Social Media Monitoring abgefangen und beantwortet werden. Solche Äußerungen sind den obenstehenden inhaltlich vergleichbar. Für das Social Media Management insbesondere bedeutsam sind auch hier die Schilderung von Problemen und allgemeine Kritik. Die verantwortliche Stelle hat häufig ein Interesse daran, auch auf Nachrichten zu antworten, die nicht an sie gerichtet sind, etwa, um aus ihrer Sicht zu einer kritischen Meinungsäußerung Stellung zu nehmen, als Gerücht oder Missverständnis empfundene Sachverhalte zu klären, oder allgemein um die bereits erwähnten Wellen negativer Meinungsäußerungen zu eigenen Produkten zu unterbinden. Auch unaufgefordert, etwa durch Hinweise bei Bedienproblemen, Serviceleistungen zu erbringen, ist eine häufige Motivation im Social CRM.

Schließlich existiert unter den Konstellationen, in denen das Unternehmen reagiert, die Fallgruppe, bei der das ursprüngliche Posting zwar allgemein zugänglich war, sich jedoch nicht einmal an die Allgemeinheit gerichtet hat, sondern eine Unterhaltung über das Produkt mit einem spezifischen Dritten über einen öffentlich einsehbaren Kanal darstellt.

Letztlich gibt es noch die Ansprache, der keinerlei vorherige Kommunikation vorausgegangen ist. Eine solche, nichtwerbliche, Konstellation besteht etwa bei Erinnerungen an fällige Wartungen, Rückrufaktionen oder anderen produktbezogenen Hinweisen.

2.10.2 Beantwortung von Anfragen

Bei der Beantwortung von direkten Anfragen auf sozialen Netzwerken handelt es sich in aller Regel um die Erhebung und Nutzung personenbezogener Daten. Dies gilt auch, wenn Postings ohne weitere Profildaten erhoben werden. Das ursprüngliche Posting muss zur Beantwortung inhaltlich ausgewertet werden. Es ist durch Einsatz einer Suchmaschine aufgrund seiner individuellen Formulierung unproblematisch dem ursprünglichen Poster zuzuordnen, der zumindest mit einem Pseudonym auf der sozialen Plattform firmiert. Ein solches Pseudonym ist mit entsprechendem Zusatzwissen stets personenbeziehbar, so dass es auch der Text selbst ist. Ausnahmen ergeben sich höchstens, wenn mehrere Postings mit derselben Formulierung in kurzer Zeit auftreten, so dass bei dem Verzicht auf die Erhebung von Metadaten eine genaue Zuordnung nicht vorgenommen werden kann. Ein typisches Beispiel wäre:

Gibt es noch Karten für @FestivalX ?

In diesem Fall würde sich das Unternehmen in der Praxis jedoch ohnehin die individuelle Beantwortung der Vielzahl gleichlautender Anfragen ersparen und von sich aus den Verfügbarkeitsstatus der Karten allen Interessierten mitteilen. Im Folgenden wird auf die praktisch relevanteren Fälle der fortbestehenden Bestimmbarkeit eingegangen.

Dabei fällt auf, dass auf dem Gebiet des Service auf direkte Anfrage die Frage nach der Rechtmäßigkeit der Ansprache fast vollständig hinter die Frage nach der Rechtmäßigkeit der Speicherung und Weiternutzung personenbezogener Daten zu anderen Zwecken zurücktritt. In vielen Fällen ist die Berechtigung der verantwortlichen Stelle zur Ansprache nicht problematisch, jedoch ist die Serviceleistung für die CRM-Betreiber regelmäßig kein reiner Selbstzweck. Vielmehr erhoffen diese sich Erkenntnisgewinn und weitere Verkaufsmöglichkeiten, weswegen die datenschutzrechtlich relevante Speicherung zu allgemeinen Geschäftszwecken fast nie unterbleibt. Deswegen muss zunächst unterschieden werden zwischen Fällen, in denen eine Speicherung personenbezogener Daten in das CRM in Vorbereitung der Antwort oder flankierend zu dieser erfolgt, und Fälle, in denen dies unterbleibt.

Unproblematisch nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG zulässig ist regelmäßig die Beantwortung von Fragen auf sozialen Medien, die keinen Abgleich mit Kundendaten nach sich ziehen. Dies gilt etwa für Anfragen nach Zugverspätungen, freien Hotelzimmern usw., ohne dass eine Absicht, eine konkrete Leistung in Anspruch nehmen zu wollen, deutlich wird. Beispiel:

@Unternehmen – ich sehe das Modell „Allegro“ auf eurer Website nicht mehr, ist das noch im Programm?

Dies ist keine Serviceanfrage oder Beschwerde, die einer längeren Betreuung bedürfte, die Identität des Fragenden ist letztlich irrelevant. Wenn seine persönlichen Daten nicht im CRM gespeichert werden, darf die Frage unter Vermeidung des Werbeeffekts ohne weiteres beantwortet werden, denn insoweit ist bei der Abwägung im Rahmen von § 28 Abs. 1 Satz 1 Nr. 3 BDSG kein Gegeninteresse des Betroffenen erkennbar. Die Antwort enthält keine über die Anfrage hinausgehenden personenbezogenen Daten, so dass es auf die wahre Identität des Betroffenen und das Medium der Übermittlung nicht ankommt.

Ein Argument gegen diese einfache Lösung könnte lauten, dass die Anfrage gegebenenfalls das personenbezogene Datum „die hinter dem Account stehende natürliche Person interessiert sich für X“ in sich trägt. Durch die Antwort, welche eine Übermittlung dieses Datums darstellt, kann sich diese Präferenz durch die Auskunft im Vergleich zur Anfrage um ein Vielfaches verbreiten, ohne dass die verantwortliche Stelle deren Wahrheitsgehalt inhaltlich nachprüfen kann. Dadurch könnte ein Nutzer, der unbefugt die Identität eines spezifischen Dritten benutzt, diesen Dritten dadurch bloßstellen, dass er öffentlich Interesse an gesellschaftlich problematischen Produkten oder Leistungen bekundet. Rechtlich bleibt es indes dabei, dass wegen der Privilegierung des § 28 Abs. 1 Satz 1 Nr. 3 BDSG die einzelnen Verarbeitungsschritte nur dann mangels berechtigten Interesses rechtswidrig sein könnten, wenn die Unrichtigkeit der Daten auf der Hand liegt.[318] Insoweit ist die verantwortliche Stelle nicht zu einer tiefergehenden Prüfung verpflichtet. Drängen sich allerdings derartige Hinweise auf, weil sich etwa die Nachricht oder der Account als offenkundig übertrieben darstellt, oder der Name eines Prominenten benutzt wird, hat die verantwortliche Stelle dies zu berücksichtigen.

[318] Vgl. Eschenbacher, Datenerhebung im arbeitsrechtlichen Vertragsanbahnungsverhältnis, S. 159.

Die Form der Nutzung seiner Daten gibt der Betroffene im vorliegenden Fall durch die Anfrage selbst vor, diese entspricht damit seinen Interessen. Nicht ohne weiteres zulässig ist wegen § 28 Abs. 3 BDSG als Antwort dagegen etwa die Unterbreitung eines besonderen Angebots, wenn hierfür keine Einwilligung vorliegt.

Die Privilegierung greift nur, wenn personenbezogene Daten nur bis zur Beantwortung der jeweiligen Frage im System der verantwortlichen Stelle gespeichert bleiben und nicht mit anderen Daten zusammengespeichert werden, so dass eine Weiterverwendung ausgeschlossen ist. Wird eine Speicherung vorgenommen, ist hierfür eine gesonderte Zwecksetzung und damit Rechtfertigung erforderlich. Ausgenommen hiervon sind reine Zählstatistiken (Zahl der Anfragen zu einem bestimmten Thema in einem bestimmten Zeitraum), die nicht personenbezogen sind.

Ist zur Beantwortung der Frage hingegen ein Abgleich mit CRM-Daten erforderlich, kann sich die verantwortliche Stelle bei der öffentlichen Antwort auf die gestellte Frage regelmäßig nicht auf § 28 Abs. 1 Satz 1 Nr. 3 BDSG berufen, denn sie übermittelt notwendigerweise Daten, welche nicht allgemein zugänglich sind. Beispiele sind die Nachfrage nach dem Status bestimmter Lieferungen und Aufträge, aber auch alle Auskunftsersuchen, die sich mit § 34 BDSG decken, insbesondere Auszüge, gleich welcher Art, aus den zu dem Betroffenen gespeicherten personenbezogenen Daten. Dies gilt auch für Bitten um Bestätigung. Hier wird zwar das Datenvolumen nicht in dem Sinne vergrößert, dass die Antwort inhaltlich neue personenbezogene Daten enthielte, allerdings ist die Bejahung oder Verneinung einer Einzelangabe zu einer Person selbst ein personenbezogenes Datum, für dessen Übermittlung eine Rechtsgrundlage erforderlich ist. Diese Praxis ist auch praktisch erforderlich, weil Identitätsdiebstahl sich auch in solchen Bitten um Bestätigung manifestiert.

Bei einem öffentlichen Posting werden Daten nicht nur dem Fragenden zugänglich gemacht, sondern zugleich an einen unbestimmten Personenkreis Dritter, welche an der Information keinerlei rechtliches Interesse haben, übermittelt. Diese Dritten, einschließlich dem Plattformbetreiber, werden regelmäßig auch in Ländern ohne angemessenes Datenschutzniveau (§ 4b Abs. 2 Satz 2 BDSG) belegen sein. Fraglich ist, ob ein solches Posting gerechtfertigt werden kann.

Zunächst ist § 4b Abs. 2 Satz 2 BDSG wohl seinem Sinn entsprechend auf solche Fälle zu reduzieren, in denen eine gezielte Weitergabe in unsichere Drittstaaten erfolgt. Ansonsten wäre jedes Bereitstellen einer Webseite wegen ihrer grundsätzlichen Einsehbarkeit durch Dritte aus solchen Staaten als Fall von § 4c BDSG anzusehen, was von der Richtlinie 1995 ersichtlich nicht beabsichtigt war.[319]

Die Berechtigung zu einer solchen Maßnahme kann sich daher entweder aus § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG ergeben. Eine Anwendung von Nr. 1 ist hier grundsätzlich denkbar, da Auskünfte als Nebenpflichten (§ 241 Abs. 2 BGB) Gegenstand von Verträgen sein können. Allerdings wird in beiden Fällen regelmäßig keine Erforderlichkeit vorliegen. Die verantwortliche Stelle besitzt von Bestandskunden stets weitere, verifizierte Kontaktdaten, über die sie dem Betroffenen unter Ausschluss der Öffentlichkeit Antworten auf die gestellten Fragen geben kann. Damit entfällt einerseits die Übermittlung an unbestimmte Dritte. Gleichzeitig erübrigt sich jedoch auch die Unsicherheit über die Identität des ursprünglichen Fragestellers. Der Betroffene kann die etwaige Falschanfrage korrigieren und wird gleichzeitig auf den Iden-

[319] Gola/Schomerus, BDSG, § 4b, Rn. 6b.

titätsdiebstahl aufmerksam gemacht. Hier hilft ein Hinweis auf die Umstände der Erhebung einschließlich des verwendeten Accounts. Dies ist zwar nicht durch das Gesetz vorgeschrieben, durch ein solches Vorgehen kann die verantwortliche Stelle jedoch vermeiden, ein weiteres Mal Mitbetroffene eines solchen Identitätsdiebstahls zu werden. Die Nutzung der Kontaktdaten des Betroffenen auch im Falle eines Irrtums ist aber jedenfalls dann rechtlich unbedenklich, wenn die Daten mit einer Zwecksetzung erhoben wurden, die auch die Bearbeitung von Serviceanfragen erlaubt.

War die ursprüngliche Anfrage an die verantwortliche Stelle gerichtet, enthält sie aber keine Handlungsaufforderung, darf die verantwortliche Stelle unter Beachtung der Meinungsfreiheit antworten und insoweit in einen Dialog eintreten. Der bloßen Nutzung der Accountdaten als solcher stehen insoweit keine schutzwürdigen Interessen entgegen, weil der Betroffene eine Konversation offensichtlich wünscht. Abermals ergibt sich jedoch die Aufspaltung in solche Fälle, in denen personenbezogene Daten mit dem CRM abgeglichen oder in dieses gespeichert werden, und solche Fälle, in denen die Kommunikationsinhalte nur in dem Maße und so lange bei der verantwortlichen Stelle verbleiben, wie es zur Kommunikation erforderlich ist. In letzterem Fall wird eine Nutzung gemäß § 28 Abs. 1 Satz 1 Nr. 3 BDSG regelmäßig rechtmäßig sein. In ersterem Fall ist nach dem Inhalt der ursprünglichen Äußerung und der Zwecksetzung zu differenzieren:

Der Abgleich mit dem CRM ohne Speicherung als solches ist wohl kein datenschutzrechtlich erheblicher Vorgang in Bezug auf die Ausgangsdaten. Es handelt sich allerdings regelmäßig um die rechtfertigungsbedürftige Erhebung neuer, aus der Verknüpfung der CRM-Daten und der Äußerung des Betroffenen entstehender, nicht allgemein zugänglicher Daten. Beispiel:

Kunde K postet unter Klarnamen folgenden Beitrag auf Twitter:

@Fluggesellschaft – Eure Piloten können nichts, die letzte Landung war viel zu hart!

Die Fluggesellschaft gleicht nun den kenntlichen Klarnamen mit dem CRM ab, um den letzten von dem Betroffenen benutzten Flug zu ermitteln und das elektronische Log des Fluges, FG527, nach besonderen Vorkommnissen zu durchsuchen, um dem Kunden antworten zu können. Gleichzeitig soll die Äußerung für das Beschwerdemanagement in der Kundenhistorie gespeichert werden. In diesem Szenario entsteht das nicht allgemein zugängliche Datum „K hat der Flug FG527 nicht gefallen". Gleichzeitig bedarf die weitere Kommunikation insoweit einer Rechtsgrundlage, als die verantwortliche Stelle das bei ihr bereits vorhandene, aber ebenfalls nicht allgemein zugängliche Datum „K war Passagier von Flug FG527" gegebenenfalls an Dritte übermitteln würde. Falls eine Antwort von der verantwortlichen Stelle beabsichtigt wird, ist wie oben das Ausweichen auf individuelle Kontaktkanäle erforderlich. Anders liegt es, wenn der Betroffene selbst die Flugnummer beiträgt. In diesem Fall bedarf es keines Abgleichs mit dem CRM, weswegen auch die Antwort öffentlich zulässig ist. Soll eine Speicherung gleichwohl erfolgen, muss diese nach den im vorhergehenden Kapitel bezeichneten Grundsätzen erfolgen.

Will die verantwortliche Stelle auf eine direkte Anfrage sachlich ihren Standpunkt zu einer öffentlichen Kritik darlegen, dürfte dies nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG regelmäßig rechtmäßig sein. Zu beachten ist aber die weiter oben besprochene Gefahr der Verkürzung der Meinungsfreiheit des Betroffenen durch Einschüchterung unter Ausnutzung wirtschaftlichen Ungleichgewichts. In der Form ist daher äußerungsrechtlich Zurückhaltung geboten.

Die Zuspeicherung des Vorgangs muss abermals unter der Wahrung der Bindung an einen zulässigen Zweck erfolgen. Die Führung von „Kritikerlisten" ist regelmäßig nicht zulässig, wohl aber eine anonymisierte Registrierung des Vorgangs zur Verbesserung des Service auf bestimmten Routen.

Nichts anderes gilt, wenn die ursprüngliche Ansprache ein Lob oder eine wohlwollende Anregung enthält. Auch einer positiven Stellungnahme gegenüber der verantwortlichen Stelle ist keineswegs ohne Weiteres die freie Verwendbarkeit des Postings für eigene Zwecke implizit.

Einen Sonderfall bilden Angriffe auf die verantwortliche Stelle, die über eine übliche, auch scharfe Kritik hinausgehen. Ein Speicherungsrecht kann hier zur Verfolgung rechtlicher Ansprüche und zur Beweissammlung für Strafanzeigen gesondert von den üblichen Geschäftszwecken gegeben sein. Dies ist freilich nur dann der Fall, wenn der Verdacht eines solchen Anspruchs oder einer Straftat tatsächlich besteht. Das äußerungsrechtlich Hinzunehmende ist dabei jedoch sehr weit umrissen, da juristischen Personen kein Persönlichkeitsrecht im Sinne von Art. 1 Abs. 1, 2 Abs. 1 GG zukommt, und die beteiligten natürlichen Personen (in der Regel) ausschließlich in der persönlichkeitsrechtlich schwach geschützten Sozialsphäre betroffen werden. Für das Unternehmen bleibt nur der Schutz nach § 823 Abs. 1 BGB in Verbindung mit dem Recht am eingerichteten und ausgeübten Gewerbebetrieb, der dem Schutzbereich von Art. 14 GG zugehört.[320]

Fraglich ist, wie weit die Meinungsfreiheit Äußerungen schützt. Zunächst ist festzustellen, dass Äußerungen, in denen Meinungen mit Tatsachenbehauptungen vermischt werden, grundsätzlich als Meinungsäußerung unter den Schutz von Art. 5 GG fallen.[321] Weiterhin sind Äußerungen so auszulegen, dass sie nur dann als unzulässig gelten dürfen, wenn es keine naheliegende Lesart gibt, unter der die betreffende Aussage rechtmäßig sein könnte, d.h. es darf nicht voreilig eine Schmähkritik unterstellt werden, wo eine vernünftige Interpretation als hinzunehmende Meinungsäußerung möglich ist (Zitat = „Babycaust"-Rspr.!). Unter Berücksichtigung der Meinungsfreiheit tritt ein über das Recht auf Antwort und die anerkannten Geschäftszwecke hinausgehendes Verarbeitungs- und Speicherungsrecht nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG damit nicht schon deswegen ein, weil sich ein Kommentar als unsachlich oder aggressiv darstellt. Vielmehr muss alle Bemühung um eine Auseinandersetzung um die Sache selbst aufgegeben worden und es dem Äußernden offenkundig ausschließlich um die Diffamierung des Gegenübers zu tun sein. Nur dann fällt die Meinungsäußerung aus dem Schutzbereich von Art. 5 GG heraus. So ist die Äußerung

@Fluggesellschaft – Ihr und euresgleichen seid Schuld, wenn bald 100.000 Menschen durch Überflutung sterben!

zwar reduktionistisch und überspitzt formuliert, im Hinblick auf die Debatte zur Klimaerwärmung aber grundsätzlich hinzunehmen, ohne dass eine Speicherung des Postings in seinem Wortlaut zusammen mit den Accountdaten ins CRM allein auf seine äußerungsrechtliche Unzulässigkeit gestützt erfolgen darf. Im Übrigen ist nach ganz herrschender Rechtsprechung das entgegenstehende Recht auf den eingerichteten und ausgeübten Gewerbebetrieb nur bei gegen seine Existenz gerichteten Eingriffen betroffen,[322]

[320] Papier, in: Maunz/Dürig, GG, Art. 14, Rn. 95 ff.

[321] Schemmer, in: Epping/Hillgruber, GG, Art. 5, Rn. 5 f.

[322] BGH, NJW 1983, S. 812.

wofür eine einzige negative Äußerung nicht ausreicht, auch wenn sie durch Repost theoretisch massenhaft verbreitet werden kann. Ein theoretisch denkbarer mittelbarer Eingriff in die Berufsausübungsfreiheit nach Art. 12 GG iVm 19 Abs. 3 GG ist regelmäßig nicht gegeben, weil dieser nach ständiger verfassungsgerichtlicher Rechtsprechung eine sog. berufsregelnde Tendenz voraussetzt. [323] Dies bedeutet, der Eingriff muss darauf abzielen oder jedenfalls in gleichem Maße wie ein staatlicher Eingriff geeignet sein, die Arbeitsbedingungen für bestimmtes Berufsbild negativ zu beeinflussen. Allgemeine Proteste gegen Praktiken in einzelnen Industrien sind hiervon nicht erfasst.

Fraglich ist zuletzt, ob die verantwortliche Stelle berechtigt ist, eine ihr gegenüber geäußerte Beschwerde über ihr Produkt ohne Handlungsanweisung als Serviceanfrage zu deuten und gegebenenfalls ohne weitere Nachfrage einen entsprechenden Vorgang im CRM anzulegen. Auch dies ist eine Frage der Interessenabwägung. Sie kann nicht pauschal, sondern nur aus der Formulierung der Anfrage und der Natur des geschilderten Problems heraus beantwortet werden. Die verantwortliche Stelle muss versuchen, zu erforschen, ob der Betroffene sein Problem, obwohl unausgesprochen, dennoch gelöst sehen möchte, oder ob er an einer Problemlösung nicht interessiert ist. Letzteres kann der Fall sein, wenn er äußert, ein Konkurrenzprodukt erwerben zu wollen. Eine aufgedrängte Serviceleistung erfolgt gegen die erkennbaren Interessen des Betroffenen und ist sowohl datenschutzrechtlich, als auch unter wettbewerbsrechtlichen Aspekten (§ 7 Abs. 2 Nr. 1 UWG) unzulässig. Der geschilderte Fall dürfte für das sogenannte Retentionsmarketing, also die Aufgabe, Kunden, die die eigenen Produkte zugunsten anderer Anbieter aufgeben, zu halten oder zurückzugewinnen, von besonderer Bedeutung sein. Anders kann sich dies darstellen, wenn eine Einwilligung in derartige Rückgewinnungsaktionen vorliegt. Auch hier ist zudem danach zu differenzieren, ob einfache, sachbezogene Hinweise zur Bedienung gegeben werden, oder ob unter Zuhilfenahme von CRM-Daten ein personalisierter, gezielter Beeinflussungsversuch erfolgt. Ersteres wird regelmäßig in der Folge der allgemeinen Berechtigung der verantwortlichen Stelle zur Beantwortung direkt an sie gerichteter Äußerungen zulässig sein. Hier ist jedoch besonders auf Zurückhaltung in der Formulierung zu achten, um einen Werbeeffekt nach § 28 Abs. 3 BDSG zu vermeiden. Letzteres ist üblicherweise eine Form von Werbung und wird auch von den Unternehmen selbst so betrachtet, so dass eine Einwilligung erforderlich ist.

2.10.3 Antworten auf Äußerungen gegenüber der Allgemeinheit und Dritten

Häufig in sozialen Netzwerken ist die Nennung von Produkten und Unternehmen nebst einer Meinungsäußerung, welche ohne erkennbaren Rezipienten verbreitet wird. Dies kann der Fall sein, wenn der Betroffene gerade das betreffende Produkt in Gebrauch genommen hat, einem Flugzeug entstiegen ist oder ein Restaurant besucht hat. Hier existieren mindestens drei Formen, der explizite Gebrauch des Accountnamens der verantwortlichen Stelle, wodurch diese zwangsläufig auf das Posting aufmerksam wird, die Benutzung von Auszeichnungssyntax (z.B. „Hashtag“) zur Hervorhebung von Produkt- oder Unternehmensnamen, womit angedeutet wird, dass allgemein Auffindbarkeit beabsichtigt ist, sowie die bloße Nennung der Firma oder des Produkts ohne besondere Hervorhebung. Innerhalb dieser Fallgruppen ist es absteigend wahrscheinlich, dass das Nutzungsinteresse der verantwortlichen Stelle ein etwaiges Ausschlussinteresse des Betroffenen überwiegt.

[323] BVerfGE 13, 181 (186), stR.

Zunächst steht das Betroffeneninteresse, von der Zuspeicherung ins CRM und der damit einhergehenden Verkettung seiner Daten freizubleiben, einem ungefragten Abgleich mit CRM-Daten entgegen. Ausnahmen sind situationsabhängig allerdings denkbar. Beispiel:

Bevor K den Flug FG527 besteigt, ist er unsicher, ob sein Flug überhaupt in die Luft gehen kann, da am Flughafen gestreikt wird. Er postet unter seinem Klarnamen das Folgende:

Ich wünschte, @Fluggesellschaft könnte checken, ob mein Flug morgen stattfindet!

In einem solchen Fall ist es nicht ausgeschlossen, dass die Fluggesellschaft rechtmäßigerweise durch Abgleich im eigenen CRM den von K gebuchten Flug ermittelt und ihm (freilich nicht öffentlich) die gewünschte Information zukommen lässt. Auch wenn das Posting nicht als direkte Aufforderung formuliert ist, spricht die äußere Form dafür, dass ein Interessengegensatz im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG nicht besteht. Die Äußerung eines Wunsches kommt der Aufforderung zwar nicht gleich, aber im Einzelfall ausreichend nahe, wenn zumindest deutlich wird, dass der Betroffene weiß, welche Verarbeitungsschritte für die Erteilung der gewünschten Information erforderlich sind. Dies kann vorliegend zumindest vertreten werden. Zusätze, die sich ausdrücklich auf den Abgleich mit dem CRM beziehen, sind insoweit nicht notwendig. Im Übrigen hat er mit der Benutzung des @-Zeichens spezifisch dafür gesorgt, dass die verantwortliche Stelle Kenntnis von der Passage erhält. Dies wird zwar nicht immer, aber doch meistens bewusst geschehen.

Anders muss dies wohl gesehen werden, wenn statt des Accountnamens entweder nur ein Hashtag oder gar kein Markup benutzt wird. In diesem Fall rechnet der Betroffene, der von der Existenz und Natur des Social Media Monitoring typischerweise keine Vorstellung hat, in der Regel nicht mit einer Kenntnisnahme durch die verantwortliche Stelle, die Kontaktaufnahme gilt daher als nicht ausdrücklich erwünscht.

Ohne Abgleich und personenbezogene Speicherung darf die verantwortliche Stelle unter Beachtung der Meinungsfreiheit hingegen auch in dieser Fallgruppe allgemeine Hinweise geben, auf Kritik reagieren und aus ihrer Sicht unrichtige Tatsachen richtigstellen. Insoweit richten sich die Statements regelmäßig an einen unbestimmten Personenkreis, dürfen also auch von jedermann aufgefangen und beantwortet werden. Dies gilt umso mehr auf Bewertungsplattformen, auf denen das Produkt der verantwortlichen Stelle von Nutzern eingeschätzt wird. Hier ist die Wertung gerade auf Außenwirkung gerichtet. Nicht selten geschieht dies auch explizit durch direkte Ansprache der verantwortlichen Stelle für den Fall, dass diese den Eintrag liest. Aber auch ohne eine solche direkte Ansprache ist das Interesse, von einer Antwort freizubleiben, nur im Ausnahmefall beachtlich. Ausnahmen sind insgesamt meistens bereits bei der Erhebung zu berücksichtigen, so etwa die fehlende Einsichtsfähigkeit des Betroffenen.

Schließlich existiert noch die Fallgruppe, bei der sich Personen öffentlich in Dialogform austauschen. Wegen der gleichbleibenden allgemeinen Zugänglichkeit ändert dies nichts am Recht der verantwortlichen Stelle zur privilegierten Verarbeitung gemäß § 28 Abs. 1 Satz 1 Nr. 3 BDSG. Allerdings stehen der Nutzung zur Kommunikation regelmäßig offenkundige Gegeninteressen entgegen, denn das Interesse, dass auch eine öffentlich geführte Unterhaltung kein Dritter für seine Zwecke nutzt, dürfte regelmäßig schutzwürdig sein. Dies kann die verantwortliche Stelle auch erkennen, da sie ja eine Auswahl der zu beantwortenden Fragen trifft und diese daher einzeln begutachtet. In eine Unterhaltung darf die verantwortliche Stelle nur in Wahrnehmung von Abwehrrechten oder zu allgemeinen Richtigstellungen ohne

Personenbezug eingreifen. Anders kann es dann zu beurteilen sein, wenn die Gesprächspartner das Zwiegespräch erkennbar öffnen und eine Äußerung des Unternehmens erwarten.

Die oben genannten Wertungen beziehen sich auf Plattformen, die nach der Verkehrsanschauung mehrheitlich Freizeitzwecken dienen. Sie sollen den Konflikt zwischen der überwiegenden Freizeitnutzung einerseits und der Nutzung zum Kundenmanagement andererseits sachgerecht lösen. Eine Ansprache ist unter erleichterten Bedingungen auf berufsbezogenen sozialen Netzwerken wie XING möglich, wo ein Interesse an relevanter Kommunikation regelmäßig größer ist. Dies gilt umso mehr für den Business-to-Business-Bereich. Betroffener kann nur eine natürliche Person sein. Unternehmen werden vom Schutzbereich nicht erfasst, solange sie nur mit einer Firma auf sozialen Netzwerken auftreten, die keinen Namen eines Lebenden enthalten.[324] Werbende Kommunikation mit Unternehmenskunden muss aber die Grenzen des Gesetz gegen den unlauteren Wettbewerb beachten.

[324] Zur Frage des Personenbezugs von Funktionsträgern und Namensgebern im Unternehmenskontext siehe Gola/Klug/Körffer, in: Gola/Schomerus, Bundesdatenschutzgesetz,§ 3, Rn. 11a.

3. Betroffenenrechte, Ansprüche und Rechtsbehelfe

Der Betroffene hat auf Antrag bei der verantwortlichen Stelle jederzeit das Recht auf Auskunft (§ 34 BDSG) über die zu seiner Person gespeicherten Daten. Bei Rechtswidrigkeit der Speicherung bzw. Unrichtigkeit von Daten kommt regelmäßig ein Lösch-, Berichtigungs- oder Sperranspruch hinzu. Im Big-Data-Bereich ergeben sich hierbei Abgrenzungsprobleme und praktische Schwierigkeiten hinsichtlich der Verfügbarkeit von Daten. Zudem gilt es, das sogenannte „Recht auf Vergessen" zu betrachten, welches aufgrund der Google-Entscheidung des EuGH wieder größere Beachtung erhalten hat. Dann soll auf die zivilrechtlichen und mittelbaren wettbewerbsrechtlichen Möglichkeiten des Einzelnen eingegangen werden, gegen unrechtmäßige CRM-Maßnahmen vorzugehen. Schließlich soll noch erörtert werden, unter welchen Umständen ein gegebenenfalls gerichtlich durchsetzbarer Anspruch auf ordnungsbehördliches Einschreiten gegeben sein kann.

3.1 Auskunftsrecht (§ 34 BDSG)

Das Auskunftsrecht ist das zentrale Institut zur Durchsetzung des Rechts auf informationelle Selbstbestimmung. Der Betroffene erhält nur durch seine Ausübung davon Kenntnis, welche Stelle welche Daten über ihn bereithält. Sie ist Grundvoraussetzung für die Löschungs- und Berichtigungsansprüche gemäß § 35 BDSG, da nur bei vollständiger Kenntnis des Datensatzes prüfbar wird, ob und gegebenenfalls welche Daten rechtswidrig oder unrichtig gespeichert wurden.[325]

Das Auskunftsrecht besteht unabhängig davon, ob der Betroffene über die erhobenen Daten nach § 4 Abs. 3 BDSG, nach § 33 BDSG oder überhaupt nicht aufgeklärt worden ist. Auch wenn Daten ausschließlich unter seiner Mitwirkung erhoben wurden, hat er jederzeit das Recht, sich über den Bestand an Daten bei einer verantwortlichen Stelle zu vergewissern. Die Praxis zeigt, dass vom Auskunftsrecht in den meisten Fällen dann Gebrauch gemacht wird, wenn der Betroffene mit einem Vorhandensein seiner Daten bei der verantwortlichen Stelle zum ersten Mal konfrontiert wird. Bei der Benachrichtigung nach § 33 BDSG über die Datenspeicherung ohne Kenntnis des Betroffenen müssen nämlich nur die gespeicherten Datenarten genannt werden. Einen Überblick über den konkreten Inhalt des Datensatzes erhält der Betroffene erst mit dem Auskunftsverlangen.[326]

Nach § 34 Abs. 1 Satz 1 Nrn. 1-3 BDSG bezieht sich die Auskunftspflicht zunächst auf sämtliche gespeicherten Daten nebst ihrer Herkunft, deren Speicherungszweck sowie mögliche Empfänger. Da eine Rechtspflicht zur Erteilung der Auskunft besteht, müssen über die Anlage zu § 9 BDSG hinaus auch technisch-organisatorische Maßnahmen unternommen werden, die es der verantwortlichen Stelle ermöglichen, die genannten Komponenten der gespeicherten Daten tatsächlich in abrufbarer Form vorzuhalten. Hieraus ergeben sich in der SCRM-Praxis Probleme.

Zunächst sind Kundendaten oft dezentral verteilt. Dies erfolgt teils aus internen organisatorischen Gründen, teils aus der Befolgung des Grundsatzes der Getrenntspeicherung. So befinden sich oft Daten zu

[325] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten, S. 187; Gola/Schomerus, BDSG, § 34, Rn. 1.

[326] Schaffland/Wiltfang, BDSG, § 33 Rn. 5, 6.

derselben Person in der eigentlichen Kundendatenbank, in Spezialdatenbanken zu einzelnen Werbekampagnen, in Datenbanken, deren Aufgabe es ist, das Vorliegen von Einwilligungen zu managen, oder in speziellen Servicedatenbanken. Speziell im Bereich der sozialen Medien kommt hinzu, dass Daten oft nicht eindeutig zugeordnet wurden, aber dennoch im System vorhanden sind. Dies ist bei isolierter Erhebung, aber auch bei Namensgleichheit der Fall. Ist sich die verantwortliche Stelle unsicher, ob Social-Media-Daten zu einem Klarnamen gehören, muss sie diese solange beauskunften, wie bei Anwendung der üblichen Sorgfalt nicht erkennbar ist, dass es sich um Social-Media-Daten eines anderen Betroffenen handelt.[327]

Zweitens werden Datensätze in der Praxis häufig ohne Quellenangabe und ohne Verwendungszweck gespeichert. Geschieht letzteres, liegt bereits nach dem Gesetzeswortlaut Rechtswidrigkeit vor (§ 28 Abs. 1 Satz 2 BDSG) und die Daten sind zu löschen.[328] Dies muss nach der Beauskunftung erfolgen, denn diese bezieht sich immer auf den Zeitpunkt des Eingangs der Anfrage. Ein Weglassen der Quelle ist, soweit ersichtlich, sanktionslos, allerdings dient sie zur Überprüfbarkeit der materiellen Befugnis zur Speicherung (Entnahme aus allgemein zugänglicher Quelle, aufgrund von Einwilligungen…). Das Weglassen kann zu einer Situation führen, in der weder die Befugnis zur Speicherung noch ihr Fehlen bewiesen werden kann. Da die Beweislast über diese Frage grundsätzlich bei der speichernden Stelle liegt, kann das Weglassen der Quelle mittelbar eine Löschpflicht auslösen.

Ferner können im System Datensätze vorliegen, die in dem Sinne personenbezogen sind, dass sie den Betroffenen vollständig beschreiben, ohne jedoch seinen Namen zu nennen. Ihre Erhebung kann nach den oben dargelegten Wertungen materiell rechtswidrig sein und ihre fehlende Zuordnung zu einem Betroffenen schließt es praktisch aus, eine rechtswidrige Erhebung zu sanktionieren. Trotzdem besteht in solchen Fällen keine Auskunftspflicht, weil die verantwortliche Stelle keine Befugnis und vor allem keine Pflicht hat, den Klarnamen selbst nachträglich zu erheben und damit die Bestimmbarkeit zu erhöhen.

Fraglich ist, ob Social-Media-Nutzer verlangen können, Auskunft über diejenigen Daten zu erhalten, die unter dem von ihnen benutzten Pseudonym erhoben wurden. Ein Problem besteht hier wiederum in der Identität des Accountinhabers. Wird der Account eines Nutzers durch Passwortdiebstahl übernommen und stellt der Eindringling sodann die Anfrage nach § 34 BDSG, könnte er Daten über den eigentlichen Accountinhaber erheben, die ihm nicht zustehen. Allerdings hat er in diesem Fall ohnehin Zugriff auf die gesamte Nutzungshistorie, soweit diese nicht gelöscht wurde. Im Übrigen ist diese Gefahr eher fernliegend, da die Datenerhebung durch die verantwortliche Stelle zu einzelnen Nutzern, soweit sie rechtmäßig erfolgt, nur sehr selektiv sein dürfte und das Wissen des „Hackers“ im Vergleich zum nötigen Aufwand und zu der Zeit, die investiert werden müsste, nicht wesentlich erweitern dürfte.

Am Ende ist ein Recht auf Auskunft unter Pseudonym grundsätzlich zu bejahen.[329] Genauso wie die verantwortliche Stelle ihren Datenbestand nicht zur Benachrichtigung (§ 33 BDSG) aktiv erweitern darf, kann auch hier die Anfrage unter Pseudonym geschehen. Voraussetzung ist allerdings, dass die verantwortliche Stelle Anzeichen für einen Identitätsdiebstahl berücksichtigt und die Korrespondenz unter Nutzung

[327] Vgl. Meents, in: Taeger/Gabel, Kommentar zum BDSG, § 34, Rn. 14.

[328] Simitis, in: Simitis, BDSG, § 28, Rn. 338.

[329] Dix, in: Simitis, BDSG, § 34, Rn. 45; a.A. Schmitz, in: Spindler/Schmitz/Geis, TDG/TDDSG/SigG, § 4 TDG, Rn. 51 f.

der verifizierten Kontaktdaten stattfindet, wenn der Account bereits einem bekannten Kunden zugeordnet worden ist.

Da Scoring ausschließlich auf Basis von Social Media-Daten regelmäßig unzulässig ist, fallen die Benachrichtigungsprobleme beim Scoring aus dem Rahmen dieser Begutachtung heraus. Erwähnt sei nur die Entscheidung des Bundesgerichtshofs zu § 34 Abs. 2 Satz 1 Nr. 3 BDSG, nach der die Beauskunftung des „Zustandekommens und der Bedeutung der Wahrscheinlichkeitswerte" nur die Aufzählung der in die Berechnung eingeflossenen Faktoren, nicht aber die Formel zur Scoreberechnung umfasst.[330] Dies soll dem geistigen Eigentum des Scorers an der Formel Rechnung tragen. Diese Entscheidung, die dem Betroffenen keinerlei Gelegenheit bietet, die Richtigkeit der Berechnung nachzuprüfen, ist überwiegend auf Ablehnung gestoßen. Richtigerweise müsste die verantwortliche Stelle zumindest die Wertungen und Gewichtungen einzelner Merkmale mitteilen, weil nur dann der Betroffene selbst nachvollziehen kann, ob der über ihn berechnete Score zutreffend ist. Aber auch wenn ausschließlich die in die Berechnung einfließenden Werte zu beauskunften wären, wären die allermeisten CRM-Betreiber hierzu nicht in der Lage, weil diese vom Business-Intelligence-System-Hersteller festgelegt werden und der Betreiber über sie in aller Regel keine Kenntnis hat. Die Unkenntnis resultiert dabei regelmäßig schon daraus, dass der Hersteller sein Betriebsgeheimnis auch gegenüber den Anwendern nicht preisgeben will.

3.2 Löschung, Berichtigung und Sperrung (§ 35 BDSG)

Hat der Betroffene einen Überblick über die zu seiner Person gespeicherten Daten erhalten, kann er gegebenenfalls gemäß § 35 die Löschung, Berichtigung oder Sperrung seiner Daten verlangen. Die Norm hat eine Doppelnatur, Adressat ist in erster Linie die verantwortliche Stelle selbst. Sie wird nicht nur auf Antrag tätig, sondern muss auch selbständig nach Maßgabe der Vorschrift löschen, berichtigen und sperren.[331] Eine Einschätzung ist der verantwortlichen Stelle nur in Bezug auf das Vorliegen der Tatbestandsmerkmale vorbehalten, nicht aber hinsichtlich der Entscheidung, ob der Pflicht Folge geleistet wird. Verlangt der Betroffene eine solche Maßnahme und sind ihre gesetzlichen Voraussetzungen gegeben, besteht daher ein unbedingter Anspruch auf Ausführung der beantragten Maßnahme.

Von den zu treffenden Maßnahmen sind zwei, nämlich die Löschung und die Sperrung, in § 3 Abs. 4 Nr. 4 und Nr. 5 BDSG als Unterformen der Verarbeitung legaldefiniert. Sperren ist ein Kennzeichnungsvorgang, der die Nutzbarkeit der Daten einschränkt. Löschen die Unkenntlichmachung personenbezogener Daten derart, dass sie nicht wiederhergestellt werden. Berichtigung ist eine Unterform der Veränderung (Nr. 2 der Vorschrift). Es handelt sich danach grundsätzlich um Vorgänge, die dem Erlaubnisvorbehalt nach § 4 Abs. 1 BDSG unterstehen. Dies ist sinnvoll, da die weitere Speicherung von Daten auch im Interesse des Betroffenen, etwa zur Beweissicherung, erfolgen und etwa eine „Berichtigung" ohne Antrag auch eine Manipulation darstellen kann.

§ 35 Abs. 1 Satz 1 BDSG verpflichtet die verantwortliche Stelle, personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Die Vorschrift postuliert keine permanente Pflicht zur Überprüfung der Richtigkeit von Daten sondern nur die Pflicht zur Berichtigung von Daten, die als unrichtig auffallen. Die Richtig-

330 BGH, Urt. v. 28.01.2014, VI ZR 156/13.

331 Dix, in: Simitis, BDSG, § 35, Rn. 1, 9.

keit von Daten kann allerdings in einigen Fällen für die materielle Zulässigkeit von Verarbeitungsschritten, insbesondere für das berechtigte Interesse an Speicherung und Nutzung nach § 28 Abs. 1 BDSG, eine Rolle spielen, wonach die verantwortliche Stelle de facto eine Verifizierungspflicht trifft.

Voraussetzung für die Berichtigung ist, dass der verantwortlichen Stelle das richtige Datum bekannt ist oder dieses beim Betroffenen nacherhoben werden kann.[332] Dies wird bei Social-Media-Daten eher die Ausnahme darstellen. Häufiger sind Fälle, in denen entweder die Unrichtigkeit auffällt, allerdings mangels positiver Kenntnis und Verifizierbarkeit eine Berichtigung nicht stattfinden kann und solche Fälle, in denen weder die Richtigkeit noch die Unrichtigkeit erweislich ist. Diesen Fällen wird häufig mit dem Mittel der Sperrung begegnet.

§ 35 Abs. 2 Satz 1 BDSG bestimmt, dass eine Löschung als tendenziell datenschutzfreundliche Maßnahme jederzeit zulässig ist, es sei denn es stehen Aufbewahrungsfristen aus Gesetz oder Vertrag entgegen, oder der Betroffene hat ein schutzwürdiges Interesse an der fortdauernden Speicherung (§ 35 Abs. 2 Satz 1 iVm Abs. 3 Nrn. 2 und 3 BDSG). Ersteres betrifft Pflichten der verantwortlichen Stelle gegenüber zuständigen Aufsichtsbehörden, der Finanzverwaltung etc. Eine Löschung ist auch dann ausgeschlossen, wenn diese der Durchführung eines Vertrags dient, sei es ohne (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) oder mit Einwilligung in die Datenspeicherung. Insoweit hat der Betroffene regelmäßig ein Interesse daran, dass zur Vertragsdurchführung erforderliche Daten vollständig gespeichert bleiben. Die Vorschrift bezieht sich nicht auf darüberhinausgehende Daten, welche die verantwortliche Stelle löschen darf, soweit dies kein schutzwürdiges Interesse des Betroffenen beeinträchtigt.

§ 35 Abs. 2 Satz 2 BDSG bestimmt, wann die verantwortliche Stelle verpflichtet ist, Daten zu löschen. Der praktisch wichtigste Tatbestand ist Nr. 1 der Vorschrift. Danach ist eine Löschung vorgeschrieben, wenn das Datum rechtswidrig gespeichert ist. Dies umfasst insbesondere den Fall, dass die Speicherung bereits zum Zeitpunkt ihrer Ausführung rechtswidrig war.[333] Fraglich ist, wie mit Fällen umzugehen ist, in denen die Rechtswidrigkeit der Speicherung nicht erweislich, aber auch nicht auszuschließen ist. Grundsätzlich ist zu sagen, dass die verantwortliche Stelle immer für die Rechtmäßigkeit ihrer Verarbeitungsschritte verantwortlich ist. Hält sie eine Speicherung für potentiell rechtswidrig, obliegt es ihr in eigener Verantwortung, über die Löschung zu entscheiden. Sie ist jedoch in Zweifelsfällen stets zu einer eingehenden Prüfung verpflichtet. Es empfiehlt sich im Zweifel die Löschung, da im Falle eines Irrtums die rechtswidrige Speicherung gemäß § 43 Abs. 2 Nr. 1 BDSG mindestens ordnungswidrig sein kann.

Nr. 2 der Vorschrift verpflichtet die verantwortliche Stelle, besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG zu löschen, deren Richtigkeit sie nicht verifizieren kann. Da eine Erhebung aus sozialen Netzwerken wegen § 28 Abs. 6 BDSG in der Regel unzulässig ist, werden besondere Arten personenbezogener Daten, soweit sie gespeichert sind, oft schon unter Nr. 1 fallen. Da die zulässig verwendeten Daten entweder offenkundig öffentlich gemacht wurden oder mit Einwilligung erhoben wurden, dürfte eine Verifizierung keine größere Hürde darstellen.

Nr. 3 ist eine für den Bereich Social CRM zentrale Vorschrift. Danach sind Daten stets zu löschen, sobald sie für die Erreichung des (zulässigen) Zwecks ihrer Speicherung nicht mehr erforderlich sind, d.h. die

[332] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten, S. 186.

[333] Vgl. Meents, in: Taeger/Gabel, BDSG, § 35, Rn. 10.

Vorschrift betrifft den Fall, dass eine gedachte erneute Speicherung nunmehr rechtswidrig, weil nicht erforderlich, wäre. Dies bedeutet, dass ein Datum, das nur zur Abwicklung eines Servicefalls erhoben wurde, nach Erreichung dieses Zwecks zu löschen ist, wenn nicht, was zulässig ist, mehrere Speicherungszwecke festgelegt worden sind. In der Praxis werden Daten oft für unbestimmte Zeit nach ihrer Verarbeitung gespeichert, eine Praxis, die nach dieser Vorschrift unzulässig ist. Aus der Vorschrift folgen einige rechtliche und tatsächliche Konsequenzen:

Will die verantwortliche Stelle Daten über eine einzelne Abwicklung hinaus speichern, so muss dies aus der Zwecksetzung der Datenerhebung hervorgehen.[334] Die Zwecksetzung muss bestimmt genug gefasst sein, dass eine Löschfrist mit ihrer Hilfe bestimmt werden kann, sie darf nicht unverhältnismäßig über den Auslöser der Datenerhebung hinausgehen. Die Länge der zulässigen Speicherung ergibt sich aus dem Nutzungszweck in Verbindung mit dem Rechtsverhältnis zu dem Betroffenen. Besteht keine über den einmaligen Datenaustausch hinausgehende Beziehung (z.B. Gespräch mit Kritiker, informeller Service), müssen die betreffenden Daten grundsätzlich unmittelbar nach Erreichung des Zwecks (Abwehr von Angriffen, Fehler behoben) gelöscht werden. Andererseits ist der verantwortlichen Stelle das Recht nicht abzusprechen bei ordnungsgemäßer Zwecksetzung und Rechtmäßigkeit der einzelnen Verarbeitungsmaßnahmen, Daten für die Dauer einer Geschäftsbeziehung (und gegebenenfalls darüber hinaus) vorzuhalten. Liegt der letzte Kontakt mit einem Kunden allerdings bereits einige Zeit in der Vergangenheit, muss auch hier eine Löschung erfolgen. Daten die neben ihrem primären Zweck zu statistischen Zwecken erhoben worden sind, sind abhängig vom Einzelfall ebenfalls nach einiger Zeit zu löschen, weil das berechtigte Interesse an ihnen wegen ihrer schwindenden Aussagekraft zunehmend von dem Betroffeneninteresse verdrängt wird.

Neben die Löschung tritt nach § 35 Abs. 5 BDSG noch ein Nutzungsverbot für Fälle, in denen der Betroffene widersprochen hat und wegen seiner persönlichen Situation sein Ausschlussinteresse das der verantwortlichen Stelle überwiegt. Ausgestaltet ist er als Ausnahme für besondere Fälle, in denen entgegen der grundsätzlichen Erlaubnis eine Weiternutzung ausgeschlossen sein soll.[335] Dies berührt nicht den Fall, in dem wegen neuer Informationen das Ausschlussinteresse an der weiteren Nutzung bereits nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG nachträglich überwiegt. Eine Anwendung kann stattdessen ausschließlich auf solche Fälle erfolgen, in denen die Verarbeitung materiell rechtmäßig bleibt, etwa, weil eine Einwilligung vorliegt. Anerkannt werden können daher nur überragende Grundrechtsgefahren.

Nach Abs. 3 ist in den bereits zu § 35 Abs. 2 Nr. 1 BDSG besprochenen Fällen das betreffende Datum zu sperren. Dies ist die logische Konsequenz des Umstands, dass eine Verwendung deren Rechtswidrigkeit, der Löschung aber das Beweisgewinnungsinteresse entgegensteht. Dadurch wird auch das Problem gelöst, dass es Konstellationen geben kann, in denen dasselbe rechtswidrige Datum zwei Betroffene berührt, deren einer ein Interesse an der Löschung hat, den anderen die Löschung in seinen Interessen verletzen würde.

[334] Gola/Schomerus, BDSG, § 35, Rn. 12.

[335] Vgl. Meents in Taeger/Gabel, BDSG, § 35, Rn. 44.

Schließlich ist nach Nr. 3 der Vorschrift von der Löschung auch dann abzusehen, wenn dies unverhältnismäßigen Aufwand verursachen würde. Dies ist eng auszulegen.[336] Ist ein zu löschendes Datum identifiziert worden, darf seiner Löschung in aller Regel nichts entgegenstehen. Die „Destabilisierung" eines CRM, die gelegentlich befürchtet wird, wenn Datensätze unvollständig gemacht werden, kann nicht zur Unzumutbarkeit führen. Das CRM ist von vornherein so zu betreiben, dass die verantwortliche Stelle ihren Löschpflichten vollumfänglich nachkommen kann.

Ein letzter Fall der Sperrung ist der der Unerweislichkeit des Wahrheitsgehalts eines Datums (§ 35 Abs. 4 BDSG), soweit es vom Betroffenen bestritten wurde.

Rechtsfolge der Sperrung ist indes keineswegs ein vollständiges Nutzungsverbot. Nach § 35 Abs. 8 BDSG bleibt die Nutzung u.a. dann zulässig, wenn nur dadurch eine Beweisnot der verantwortlichen Stelle abgewendet werden kann oder die Nutzung aus anderen überwiegenden Interessen der verantwortlichen Stelle unerlässlich ist und „die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären."

3.3 Widerspruch gegen die Zusendung von Werbung (§ 28 Abs. 4 BDSG)

Dass Werbung im Rahmen des Social CRM grundsätzlich nur nach Einwilligung zugesandt werden darf, ist bereits besprochen worden. § 28 Abs. 4 Abs. 1 BDSG macht das Recht des Betroffenen deutlich, der verantwortlichen Stelle auch bei Vorliegen einer derartigen Einwilligung, die Nutzung seiner Daten zur Zusendung von Werbung ex nunc zu untersagen. Im Falle der Einwilligung liegt in einem solchen Widerspruch regelmäßig auch der (Teil-)Widerruf der Einwilligung, dies ist jedoch durch Auslegung festzustellen. Die beiden Rechtsinstitute sind jedenfalls voneinander unabhängig. Der Widerspruch ist nicht formgebunden, § 28 Abs. 4 Satz 4 BDSG bestimmt, dass die verantwortliche Stelle für den Widerspruch keine strengere Form bestimmen darf als diejenige des Schuldverhältnisses. Da die allermeisten Schuldverhältnisse ebenfalls keinem Schriftformerfordernis unterliegen, kann ein Widerspruch grundsätzlich formlos eingelegt werden. Das Formerfordernis der Einwilligung nach § 4a Abs. 1 Satz 3 BDSG gilt nicht.

3.4 Recht auf Vergessenwerden?

Das sogenannte Recht auf Vergessenwerden ist kein gesetzlich verbürgter Anspruch, wird aber in der datenschutzrechtlichen Diskussion als zentraler Teil des Rechts auf informationelle Selbstbestimmung diskutiert, gerade unter den Bedingungen von Big Data.[337] Gemeint ist der Anspruch, dass im Internet veröffentlichte Daten über Betroffene nach einiger Zeit gelöscht werden oder sogar mit einem technischen Verfallsdatum ausgestattet werden. Die Löschung soll so automatisch erfolgen, sobald anzunehmen ist, dass das Interesse des Betroffenen an der Streichung der Daten wegen Zeitablaufs gegenüber dem Informationsinteresse der Öffentlichkeit überwiegt. Konkret gelöst werden sollte das Problem, dass biographische Details von Betroffenen, sei es durch wiederholten Upload durch Dritte, durch Caching in Suchmaschinen oder durch Archivierung von Snapshots großer Webseiten, wie sie die Seite archive.org

[336] Dix, in: Simitis, BDSG, § 35, Rn. 50; Wedde, in: Rosnagel, Handbuch Datenschutz, Kap. 4.4, Rn. 74.

[337] Überblick bei Nolte, ZRP 2011, S. 236.

vornimmt, faktisch für unbestimmte Zeit abrufbar sind. Die Befürchtung war, dass Betroffene dadurch an ihrem beruflichen und privaten Fortkommen gehindert werden, weil ungünstige biographische Details permanent recherchierbar bleiben, auch wenn sie sich nicht wiederholt haben oder ihre Rahmenbedingungen sich grundlegend geändert haben, wodurch potentielle Arbeitgeber oder Geschäftspartner einen verzerrten Eindruck von der Zuverlässigkeit des Betroffenen bekommen könnten.

Im Social CRM entspricht der Anwendungsbereich des Rechts auf Vergessenwerden Löschungsansprüchen auf Foren und gegebenenfalls dem Verbot der Weiternutzung dieser Daten. Ein bereuter Beitrag soll dem Betroffenen danach nicht grundsätzlich und unbegrenzt zum Nachteil gereichen.

Das Recht auf Vergessenwerden befindet sich somit in einem offenkundigen Spannungsfeld zwischen dem Informationsinteresse der Öffentlichkeit und dem grundsätzlichen Recht des Betroffenen, den Verbleib seiner Daten zu steuern, was auch den Rückzug von Veröffentlichungen einschließen kann andererseits.[338] Es geht nicht um Fälle, in denen Daten des Betroffenen von Anfang an unbefugt durch Dritte veröffentlicht werden, dies kann durch die üblichen Rechtsbehelfe unterbunden werden. Vielmehr geht es um die Grenze der materiellen Befugnis zur fortgesetzten Speicherung eines zunächst rechtmäßig veröffentlichten Datums und damit letztlich um die Frage, ob und wann der Speicherungszweck „Information der Öffentlichkeit" sich im Sinne von § 35 Abs. 2 Nr. 3 und 4 BDSG erledigt hat.

Fraglich ist, ob sich bereits aus dem geltenden Recht ein Recht auf Vergessen herauslesen lässt.[339] Die genannten Löschvorschriften legen selbst keinen Erledigungszeitpunkt fest, sondern setzen diesen voraus. Das Bundesverfassungsgericht hat äußerungsrechtlich, und damit bezogen auf den nichtinformationellen Teil des Persönlichkeitsrechts, in seiner Lebach-Rechtsprechung[340] die Auffassung vertreten, der Anspruch eines Straftäters auf Unterlassung einer erneuten Berichterstattung über ein Verbrechen hänge außer vom Zeitablauf von der fortgesetzten gesellschaftlichen Relevanz des Themas auf der einen und den Rehabilitationsinteressen der Straftäter und der Schwere des Eingriffs durch die Berichterstattung auf der anderen Seite ab. Es gäbe jedoch kein grundsätzliches Recht, von der Konfrontation mit vergangenem Tun verschont zu werden. In der Praxis ist die Zuerkennung des Unterlassungsanspruchs die Ausnahme geblieben.[341] Soweit der Betroffene sich bewusst exponiert, indem er etwa eine Straftat zu Lasten eines Prominenten oder allgemein eine besonders schwere Straftat begeht, ist er auch nach Zeitablauf regelmäßig nicht schutzwürdig.

Diese Linie der Rechtsprechung ist zwar für Medienberichterstattung im klassischen Sinne zu bejahen, sie ist jedoch auf die Bedingungen des Internetzeitalters nicht in vollem Umfang übertragbar. Dies ergibt sich aus zwei Merkmalen der Online-Datenspeicherung, der Permanenz der Daten und der unproblematischen Auffindbarkeit. Es geht vorliegend nicht, wie in Fällen nachträglicher Medienberichterstattung, um das „Aufwühlen" von Sachverhalten, über die mittlerweile der Rechtsfrieden eingekehrt ist. Vielmehr kann dieser Rechtsfrieden bei permanenter Verfügbarkeit der Daten niemals eintreten. Eingriffe in das

338 Schweda, ZD-Aktuell 2014, 04371.

339 Zu dieser Frage ausf. Nolte, ZRP 2011, S. 238.

340 Im Anschluss an BVerfGE 35, 202.

341 Siehe etwa die sog. Sedlmayr-Rechtsprechung, BGH, Urt. v. 15.12.2009, VI ZR 227/08.

Persönlichkeitsrecht ergeben sich insoweit bereits durch die Verfügbarkeit, sie werden aktualisiert durch die jederzeit möglichen Seitenabrufe.

Zudem existiert der bereits besprochene Löschanspruch des Betroffenen gegen einen Plattformbetreiber, welcher für sich selbst § 29 Abs. 1 BDSG als Rechtsgrundlage der Speicherung in Anspruch nehmen kann. Hier existiert eine äußerungsrechtliche Rechtsprechung, die zwar das öffentliche Interesse oder sein Fehlen als Abwägungskriterium in Betracht zieht, ein generelles Recht auf Löschung von Informationen, weil an ihnen gerade wegen Zeitablaufs kein überwiegendes öffentliches Interesse mehr besteht, lässt sich aus der recht verarbeitungsfreundlichen höchstrichterlichen Rechtsprechung nicht ersehen. Im Gegenteil müssen nach der Spickmich-Rechtsprechung,[342] die sich inzwischen verstetigt hat,[343] die Sozialsphäre betreffende Meinungsäußerungen auf Foren, auch wenn sie, als Tatsachenbehauptungen gelesen, nicht erweislich wären, grundsätzlich hingenommen werden.

Es wurde angesichts dieser Sachlage im Zuge der Erarbeitung einer Datenschutz-Grundverordnung[344] von einigen Seiten eine Einarbeitung des Rechts auf Vergessen gefordert. Dieses Konzept in die Beratungen über die Verordnung unterzubringen, war auch von deutscher Seite geplant. Eine Mehrheit fand sich jedoch nicht, und die Regulierung der Profilbildung und verwandter Phänomene durch Werbende und Wirtschaftsunternehmen bildeten sodann die Hauptpunkte der Reform, so dass sich im Entwurf der Grundverordnung keine über die geltende Rechtslage hinausgehende Regelung findet und eine solche wohl auch nicht mehr zu erwarten ist.[345]

Ohne den Begriff des Rechts auf Vergessenwerden zu erwähnen und ohne eine Gesetzesänderung, leitete jedoch der EuGH in seiner Google-Entscheidung die Grundstrukturen des Konzepts kurzerhand aus der geltenden Rechtslage ab. Danach ist Art. 7 f) der Datenschutzrichtlinie so zu lesen, dass eine fortgesetzte Speicherung fortlaufend zu rechtfertigen sei, und eine Löschung immer dann vorzunehmen sei, wenn das berechtigte Interesse der Öffentlichkeit das Betroffeneninteresse am Recht auf Datenschutz nicht mehr überwöge. Dabei ist die Entscheidung nicht auf Suchmaschinen beschränkt, der Umstand, dass Unterlassungsansprüche neben dem Zweitverwerter selbstverständlich auch gegenüber der ursprünglich verantwortlichen Stelle geltend gemacht werden können, ergibt sich bereits aus Art. 2 d) der Richtlinie. Die sich aus dem Tenor ergebende Vermutungsregel, dass im Zweifel die Betroffenenrechte an der Löschung überwögen, wird vom EuGH in der Urteilsbegründung ausdrücklich bestätigt. Mit dieser Vermutung obliegt daher einem Seitenbetreiber grundsätzlich die Pflicht, ständig das fortgesetzte Interesse der Öffentlichkeit an der Information zu prüfen und diese bei Bedarf zu löschen. Dies betrifft insbesondere, aber nicht ausdrücklich nur, nachteilige Einzelangaben. Im Bundesrecht kann aber in Einzelfällen § 35 Abs. 3 Nr. 2 BDSG der Löschung vorteilhafter Daten entgegenstehen.

---

342 BGH, Urt. v. 23.06.2009, VI ZR 196/08.

343 U.a. durch BGH, Urt. v. 29.04.2014, VI ZR 138/13; Urt. v. 23.09.2014, VI ZR 358/13.

344 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung), (COM(2012)0011.

345 Hören/Giurgiu, NWB 2012, S. 1602.

Die Entscheidung hat neben einigen wohlwollenden Kommentaren[346] viel Kritik erfahren,[347] da sie bisherigem nationalen Äußerungsrecht widerspricht und die Meinungs- und Medienfreiheit weit einschränken kann. Kritik wurde nicht zu Unrecht an der pauschalen Postulierung des Vorrangs von Datenschutz gegenüber der Informationsfreiheit geübt. Die scheinbare Radikalität des Ansatzes des Gerichtshofes entspricht jedoch seiner etwa aus der Rechtsprechung zur Warenverkehrsfreiheit bekannten Entscheidungstechnik, zunächst einfache Regeln aufzustellen und diese in weiteren Entscheidungen zu präzisieren. Daher ist zu erwarten, dass der EuGH in späteren Entscheidungen Einschränkungen des Löschungsrechts entwickeln wird und es daher bei der einfachen Formel „im Zweifel für die Löschung" nicht bleiben wird. Aus der Umsetzung des Urteils durch Google wird deutlich, dass eine umsichtige Löschpraxis zur sachgerechten Umsetzung des „Rechts auf Vergessenwerden" führen kann. Es ist zu erwarten, dass die Rechtsprechung in der Bearbeitung von Fällen auch hierzu Kriterien erarbeiten kann und wird.

3.5 Zivilrechtliche Ansprüche

Neben die Ansprüche auf Berichtigung, Sperrung und Löschung tritt der praktisch kaum relevante Anspruch auf Ersatz des von einer rechtswidrigen Verarbeitungsmaßnahme verursachten Schadens (§ 7 BDSG). Die Norm ist auch im telemedienrechtlichen Anbieter-Nutzer-Verhältnis anwendbar. Das Verschulden wird vermutet,[348] der verantwortlichen Stelle steht indes der Exkulpationsbeweis in Form der Darlegung, dass die erforderliche Sorgfalt beachtet wurde, zur Verfügung (S. 2 der Vorschrift). Die Schadensersatzpflicht tritt danach nicht ein, wenn die verantwortliche Stelle die Einhaltung der Vorschriften des BDSG, insbesondere zum Datenschutzmanagement, durch kontinuierliche Prüfung überwacht hat und im Fall einer erkennbaren Gefahr das Zumutbare unternommen hat, diese abzuwenden. Dies wird in der Regel durch die Offenlegung der Verfahrensdokumentation erfolgen. Bei gemeinsamer Datenverarbeitung durch mehrere Stellen haften diese als Mittäter (§ 840 BGB) gesamtschuldnerisch. Nach § 7 liquidierbar ist nur der materielle Schaden.[349]

Bei Persönlichkeitsverletzungen ist ein Ersatz des immateriellen Schadens gemäß § 823 Abs. 1 i.V.m dem allgemeinen Persönlichkeitsrecht als sonstigem Recht gegeben.[350] Die praktischen Hürden für dessen Geltendmachung sind im Social CRM, schon allein wegen des Haftungsprivilegs des Forumsbetreibers nach §§ 7 Abs. 2, 10 TMG, recht hoch. Eine unzulässige Profilbildung allein wird grundsätzlich keine Ersatzpflicht nach sich ziehen, auch wenn dadurch eine gewisse Beeinträchtigung auch der Privatsphäre des Betroffenen eintreten mag.

Der in der Praxis mit Abstand wichtigste Anspruch ist der sog. quasinegatorische Unterlassungsanspruch analog § 1004 Abs. 1 Satz 2 i.V.m dem allgemeinen Persönlichkeitsrecht.[351] Er steht selbständig neben dem Löschanspruch nach § 35 BDSG. Störer wird die verantwortliche Stelle, indem sie eine persönlich-

346 Z.B. Boehme-Neßler, NVwZ 2014, S. 830; Kühling, EuZW 2014, S. 527.

347 Z.B. Masing, wiedergegeben in MMR-Aktuell 2014, 361039; Rohleder, wiedergegeben in MMR-Aktuell 2014, 358540.

348 Gola/Schomerus, BDSG, § 7, Rn. 9.

349 Gabel in Taeger/Gabel, BDSG, § 7, Rn. 9.

350 Kopp, RDV 1993, S. 8; Wuermeling, DB 1996, S. 670.

351 Berger, in: Jauernig, BGB, § 1004, Rn. 2.

keitsrechtsverletzende Maßnahme entweder selber durchführt oder diese durch Dritte geschehen lässt. Der Unterlassungsanspruch ist in der Regel auf die Einstellung der persönlichkeitsrechtsverletzenden Maßnahme gerichtet und umfasst nur Maßnahmen unter der Kontrolle der verantwortlichen Stelle einschließlich ihrer Auftragnehmer. Allerdings kann diese analog § 35 Abs. 7 BDSG verpflichtet sein, Stellen, an die die betreffenden Daten weitergegeben wurden, von der Unverwertbarkeit dieser Daten zu informieren.

3.6 Verbraucherschutz- und wettbewerbsrechtliche Rechtsbehelfe

Der Betroffene kann sich an nach §§ 3, 4 Unterlassungsklagengesetz (UKlaG) qualifizierte Einrichtungen wenden, um Allgemeine Geschäftsbedingungen prüfen zu lassen. Diese Einrichtungen, typischerweise Verbraucherverbände, sind nach § 2 UKlaG befugt, Verstöße gegen verbraucherschützende Normen zu rügen. In Bezug auf Social CRM gelten als verbraucherschützend u.a. Vorschriften aus der eCommerce-Richtlinie 2000/31/EG.[352] Ein aktueller Gesetzesentwurf sieht zudem vor, auch AGB über Profilerstellung und Datenverarbeitung zu Werbezwecken ausdrücklich dem UKlaG zu unterwerfen.[353] Daneben gibt das UKlaG nach § 1 den qualifizierten Einrichtungen Allgemeinen Geschäftsbedingungen zu rügen und die Unterlassung von deren Verwendung zu erwirken. In der Vergangenheit wurde dies insbesondere gegen große Anbieter wie Apple und Facebook erfolgreich getan.

Neben den aus dem UKlaG folgenden Unterlassungsansprüchen wegen Verwendung unwirksamer AGB, ist auch das Gesetz gegen den unlauteren Wettbewerb (UWG) relevant. Nach der Definition des Gesetzeszwecks des UWG in dessen § 1 dient das Wettbewerbsrecht nicht nur dem Schutz von Mitbewerbern, sondern auch dem Schutz der Verbraucher und sonstiger Marktteilnehmer vor unlauteren geschäftlichen Handlungen. Einerseits soll es Verfälschungen im Wettbewerb verhindern, andererseits das allgemeine Verbraucherschutzrecht im Hinblick auf die Lauterkeit des Geschäftsgebarens erweitern. Hauptwerkzeuge des Wettbewerbsrechts, soweit es nicht um Sanktionen geht, sind der Unterlassungsanspruch (§ 8 UWG), dessen Geltendmachung typischerweise die wettbewerbsrechtliche Abmahnung vorgeschaltet ist, und der Schadensersatzanspruch mit Gewinnabschöpfung (§ 9 f. UWG).

Der wettbewerbsrechtliche Unterlassungsanspruch kann außer von Mitbewerbern und Berufsverbänden auch von Institutionen nach § 4 UKlaG wahrgenommen werden (§ 8 Abs. 3 Nr. 3 UWG). Träger des Schadensersatzanspruchs sind jedoch ausschließlich Mitbewerber. Ein verbleibender Gewinn fällt allerdings dem Bundeshaushalt zu (§ 10 Abs. 1 UWG). Es sind daher vornehmlich die Fälle eines datenschutzrechtlich relevanten Unterlassungsanspruchs darzustellen.

Ausdrücklich finden sich Verbote bestimmter Werbeansprachen, was datenschutzrechtlich einer Nutzung personenbezogener Daten entspricht. Diese sind in § 7 UWG beispielhaft aufgeführt. Zunächst enthält § 7 Abs. 1 Satz 2 UWG eine Generalklausel, die besagt, dass die individuelle Zusendung von Werbung im-

[352] Siehe § 2 Abs. 2 Nr. 2 UKlaG.

[353] So der geplante § 2 Abs. 2 Nr. 11 des Gesetzesentwurf der Bundesregierung zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts, BT-Drucks. 18/4631.

mer bereits unzulässig ist, wenn erkennbar ist, dass der Betroffene diese nicht wünscht. Ein Beispiel ist die Anbringung eines Schildes am Briefkasten oder die Eintragung in der sog. Robinsonliste.[354]

Darüber hinaus enthält Abs. 2 spezielle Fälle rechtswidriger Werbung. Dies betrifft nach Nr. 2 zunächst Telefonanrufe ohne „zumindest mutmaßliche" Einwilligung. Das bedeutet, dass konkrete Anhaltspunkte für die Annahme bestehen müssen, der Betroffene werde mit dem Anruf einverstanden sein. Solche Signale dürften auf sozialen Netzwerken fast nie vorkommen. Insbesondere ist keineswegs die bloße Verfügbarkeit einer Telefonnummer etwa auf einem Profil ausreichend. Deswegen ist deren Sammlung zur Vorbereitung einer Werbeaktion auch dann unzulässig, wenn für die allgemeine Werbeansprache eine Einwilligung vorliegt.

Nach Nr. 3 ist Werbung mit sog. Anrufautomaten, Faxwerbung und „elektronischer Post" ohne ausdrückliche Einwilligung verboten. Dem Gesetzeszweck nach fällt unter den Begriff „elektronische Post" nicht nur das E-Mail-Postfach, sondern auch Postfächer auf sozialen Netzwerken und Chatsoftware, so dass auch eine solche Ansprache als unzumutbar gelten muss.[355] Dasselbe dürfte für die Pinnwand einer Facebook-Seite sowie alle Äquivalente eines Posteingangs gelten, also allen Seiten, bei denen der Betroffene über neu eingegangene Meldungen benachrichtigt wird und diese dann zur Kenntnis nehmen muss.

Ausnahmen ergeben sich nach Abs. 3 nur in Fällen, in denen die verantwortliche Stelle Zugang zu einem Postfach im Zusammenhang mit einem abgewickelten Kauf-, Werk- oder Dienstvertrag erhalten hat und gleichartige Waren oder Dienstleistungen feilbieten will. In diesem Fall ist bei der Einholung der Postfachdaten wie bei jeder Zuschrift auf die Opt-Out-Möglichkeit hinzuweisen. Selbstverständlich kann danach eine Zusendung von Werbung nur so lange geschehen, wie von dem Opt-Out kein Gebrauch gemacht worden ist.

Schließlich ergibt sich der Unterlassungsanspruch noch bei Werbung, deren Absender, insbesondere zur Geltendmachung der Opt-Out-Möglichkeit, verschleiert wird. Da in Messages auf sozialen Medien diese Kontaktdaten nur selten sinnvoll einzubinden sind,[356] kann dies durchaus Relevanz erlangen. Verboten ist wie bei jedem Telemedium (s.o.) die Verschleierung des werblichen Charakters der Nachricht gemäß § 6 Abs. 1 Nr. 1 TMG.

Darüber hinaus verbietet § 3 Abs. 1 sogenannte unlautere geschäftliche Handlungen. § 4 UWG zählt beispielhaft („insbesondere") Fälle von Unlauterkeit auf. In § 4 Nr. 3 -5 UWG finden sich erneut die in § 6 TMG bereits sanktionierten Verschleierungen des Werbecharakters und des Absenders von Werbung. Die wichtigste Verbotsnorm für das Datenschutzrecht ist allerdings die Auffangnorm § 4 Nr. 11 UWG. Danach handelt unlauter, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln. Welche Datenschutzvorschriften unter diesen Begriff fallen, ist von der Rechtsprechung noch nicht abschließend geklärt und war über die vergangenen Jahre einem steten Wandel unterworfen. Die eindeutige Tendenz geht jedoch dahin, Datenschutzvor-

354 Weichert, WRP 1996, S. 531.

355 Ohly, in: Ohly/Sosnitza, UWG, § 7, Rn. 65.

356 Vgl. Pießkalla, ZUM 2014, S. 371.

schriften als grundsätzlich marktverhaltensregelnd anzusehen.[357] Der bereits angesprochene Gesetzesentwurf der Bundesregierung sieht in jedem Fall eine Ausweitung auf für Werbung wesentliche Verarbeitungsschritte vor.[358]

Als marktverhaltensregelnd gelten bereits heute insbesondere § 13 TMG, [359] § 28 Abs. 3 BDSG,[360] sowie § 4a BDSG.[361] Auch § 29 BDSG dürfte hierunter fallen, soweit die Übermittlungsbefugnis der verantwortlichen Stelle beschränkt wird.

[357] Überblick bei Ohly, in: Ohly/Sosnitza, UWG, Rn. 11/79.

[358] Siehe Fußnote 353.

[359] OLG Hamburg, Urt. v. 27.06.2012, 406 HKO 155/11; KG, Urt. v. 29.04.2011, 5 W 88/11.

[360] OLG Karlsruhe, Urt. v. 09.05.2012, 6 U 38/11, KG, Urt. v. 24.01.2014, 5 U 42/12, OLG Köln, Urt. v. 17.01.2014, 6 U 167/13.

[361] KG, Urt. v. 24.01.2014, 5 U 42/12.

4. Sanktionen

Die datenschutzrechtlichen Spezialgesetze enthalten Ordnungswidrigkeits- und Nebenstrafrechtsnormen. Daneben sind die Normen des Strafgesetzbuchs, insbesondere die der §§ 201- 206 StGB, relevant.

Die Vorschrift des § 43 BDSG, die die grundlegenden Ordnungswidrigkeitstatbestände für Zuwiderhandlungen gegen Normen des BDSG enthält, ist zweigeteilt. Sowohl Absatz 1 als auch Absatz 2 enthalten Tatbestände, bei deren Verwirklichung ein Bußgeld droht. Allerdings ist der Rahmen des Bußgelds in den Fällen von Absatz 2 weiter, der Gesetzgeber ging also davon aus, dass es sich in den Fällen von Absatz 2 regelmäßig um das schwerere Fehlverhalten handelt. Allgemein kann gesagt werden, dass die Ordnungswidrigkeiten nach Absatz 1 die Umstände der Datenverarbeitung betreffen, während diejenigen nach Absatz 2 rechtswidrige Datenverarbeitungsmaßnahmen selbst sowie Maßnahmen, die mit der Datenverarbeitung in unmittelbarem Zusammenhang stehen, sanktionieren. Gemäß § 44 Abs. 1 BDSG werden Taten nach Absatz 2 bei zusätzlichem Vorliegen einer Bereicherungs- oder Schädigungsabsicht zu Straftaten.

§ 43 Abs. 3 S. 2 und 3 BDSG geben nähere Anweisungen zur Bemessung des Bußgelds. So soll ein etwaiger Gewinn des Täters aus dem unrechtmäßigen Vorgehen abgeschöpft werden. Dazu darf der Bußgeldrahmen auch überschritten werden. Da jedoch maximal der wirtschaftliche Vorteil zuzüglich des Höchstmaßes der Geldbuße angesetzt werden kann, ist diese Regelung bestimmt genug und damit verfassungsgemäß.[362] Sie entstammt konzeptionell dem Wettbewerbsrecht (konkret § 10 UWG, wo allerdings eine wesentlich komplexere Regelung getroffen wird). Dadurch, dass die verantwortliche Stelle selbst abzuschätzen in der Lage ist, welchen finanziellen Vorteil sie aus der rechtswidrigen Maßnahme gezogen hat, kann sie auch vorhersagen, in welchem Rahmen sich das zu gewärtigende Bußgeld bewegen wird.

Nach § 43 Abs. 1 Nr. 2b BDSG handelt ordnungswidrig, wer ein Auftragsdatenverhältnis ohne ordnungsgemäßen, schriftlichen Vertrag gemäß § 11 BDSG begründet oder sich nicht von der technisch-organisatorischen Leistungsfähigkeit des Auftragnehmers überzeugt hat. Dies dürfte für alle Hosting-Lösungen genauso wie für Auftragsdatenverarbeitung im Intelligence- und Monitoring-Bereich gelten. Das Unterlassen der Aufklärung über das Widerspruchsrecht gegen werbliche Datennutzung nach § 28 Abs. 4 ist ebenso ordnungswidrig wie die Forderung der Schriftform für die Ausübung dieses Rechts. Das Unterlassen der Benachrichtigungspflicht nach § 33 BDSG und die unterlassene, verspätete oder unvollständige Auskunft nach § 34 BDSG sind ebenfalls nach Abs. 1 ordnungswidrig. Schließlich handelt ordnungswidrig, wer seinen Mitwirkungs- und Duldungspflichten gegenüber der Aufsichtsbehörde nach §§ 38 Abs. 3 und 4 BDSG bzw. einer vollziehbaren Ordnungsverfügung nach Abs. 5 der Vorschrift nicht nachkommt.

Der in der Praxis am häufigsten verwirklichte Bußgeldtatbestand findet sich in § 43 Abs. 2 Nr. 1 BDSG. Danach handelt ordnungswidrig, wer personenbezogene Daten, die nicht allgemein zugänglich sind, unbefugt erhebt oder verarbeitet. Nicht bußgeldbewehrt ist dagegen wieder die Nutzung der Daten. In

[362] Klebe, in: Däubler/Klebe/Wedde/Weicher, BDSG, § 43, Rn. 24.

der Praxis ist damit nur die Speicherung und gegebenenfalls Veränderung der Daten, etwa zu Scores, verfolgbar. Dies lässt im Social CRM eine erhebliche Sanktionslücke, da insoweit die Früchte eines nicht zweckgebundenen und dadurch unzulässigen Monitorings öffentlicher Quellen als Big-Data-Grundlage ohne Gefahr einer ordnungsrechtlichen Sanktion gesammelt werden können. Anderes gilt nach dem oben Ausgeführten gegebenenfalls für die Weiterverarbeitung, da durch die Verkettung die allgemeine Zugänglichkeit oft beseitigt wird.

Ordnungswidrig und potentiell sogar strafbar sind schließlich die Nichtbeachtung des Kopplungsverbots im Falle von Werbung (Nr. 5a), die Nutzung von Daten zu Zwecken der Werbung trotz Widerspruchs (Nr. 5b) und eine unterlassene Anzeige nach einem Datenleck im Sinne von § 42a BDSG.

Auch das Telemediengesetz enthält in § 16 einen Bußgeldkatalog. Grundsätzlich sind alle Tatbestände auch auf CRM-Betreiber anwendbar, soweit sie ein eigenes Telemedium anbieten. Dies betrifft Zuwiderhandlungen gegen

- die Impressumspflicht (§ 5),
- die Pflicht zur Aufklärung darüber, welche Daten über den Nutzer erhoben werden (§ 13 Abs. 1),
- die technischen Vorkehrungen nach § 13 Abs. 4 Nrn. 1-4,
- das Verbot der Zusammenführung von pseudonymen Profilen nach § 15 Abs. 3 mit personenbezogenen Daten der dahinterstehenden natürlichen Person und
- das Verbot der Verschleierung des Werbecharakters eines Angebots (§ 6 Abs. 2).

Mit Ausnahme des letzten Punkts ist Fahrlässigkeit ausreichend.

Nach § 20 UWG ist nur ein tatsächlich werbender Telefonanruf oder automatischer Anruf ordnungswidrig, für die Datenverarbeitung muss auf die entsprechenden Vorschriften von BDSG und TMG zurückgegriffen werden.

Gegenüber den datenschutzrechtlichen Sanktionsnormen ist das StGB in der CRM-Praxis eher unbedeutend. Es ist nicht zu erwarten, dass CRM-Betreiber etwa unter Bruch fremder Passwörter Daten erlangen wollen (§ 202a StGB). Dasselbe gilt für das Abfangen von Daten aus einem nichtöffentlichen Sender (§ 202b StGB). Dass Berufs- und Dienstgeheimnisse nicht auf soziale Medien gehören, und der Verstoß hiergegen strafbar ist, ist selbstverständlich (§ 203 StGB).

5. Rechtliche Zulässigkeit des Prototypen

Der von den Projektpartnern entwickelte Prototyp, dessen Verfahrensweise und die geplante Nutzung sind aus juristischer Sicht zu skizzieren. Er besteht aus einer grafischen Oberfläche mit Eingabemöglichkeiten und einer Wissensdatenbank. Die Wissensdatenbank wird gespeist von Excel-Tabellen, die Prüfungsskizzen für datenschutzrechtliche Normen enthalten. Die Listen sind nach Sachgebieten geordnet, die zu prüfenden Normen sind den Betätigungsfeldern im Social CRM (Forumsbetrieb, Social Media Monitoring etc.) zugeordnet. Der Sachbearbeiter wählt das passende Sachgebiet aus. Ihm wird sodann ein Fragebogen angezeigt. Mit den Fragen wird in der Reihenfolge, die sich aus den zu prüfenden Normen ergibt, das Vorliegen von Tatbestandsmerkmalen abgefragt. Der Sachbearbeiter beantwortet diese Fragen nach seiner Kenntnis und bekommt von der Software, basierend auf seinen Eingaben, eine Reihe von Warnungen ausgegeben, auf welche Umstände nach den gegebenen Antworten zu achten sei, insbesondere, welche Verarbeitungsvorgänge aufgrund der Eingabe voraussichtlich rechtswidrig seien. Die ausgegebenen Warnungen sind ausdrücklich nicht abschließend und stehen unter dem Vorbehalt, dass im Einzelfall weitere Normen einschlägig sein können. Außerdem kann es praktisch nie zu einer Entwarnung kommen. Die Warnungen legt der Sachbearbeiter sodann dem betrieblichen Datenschutzbeauftragten vor. Ziel ist eine Vorstrukturierung des Falles zur selbständigen Lösung durch die zuständigen Mitarbeiter sowie die Sensibilisierung für wiederkehrende datenschutzrechtliche Probleme.

Der Anwendungsbereich des Rechtsdienstleistungsgesetz (RDG) wird nach der derzeitigen Softwarearchitektur aus hiesiger Sicht nicht eröffnet. Das RDG findet laut seinem § 2 auf Tätigkeiten in konkreten fremden Angelegenheiten Anwendung, die eine rechtliche Prüfung des Einzelfalles erfordern. In persönlicher Hinsicht können, auch wenn dies nicht aus dem Gesetzeswortlaut hervorgeht, nach systematischer Sicht nur natürliche und juristische Personen für die Erteilung von Rechtsdienstleistungen in Frage kommen. Dies wird deutlich, wenn man sich die Struktur des RDG vergegenwärtigt. Es enthält in § 3 ein Verbot der Erbringung derartiger Dienstleistungen mit Erlaubnisvorbehalt, wobei sich Erlaubnistatbestände auch außerhalb des RDG finden. Die meisten Ausnahmen von § 3 sind personal definiert, so unterscheidet das Gesetz selbst die Dienstleistungserbringung durch registrierte (§ 10-15b RDG) und nichtregistrierte (§ 6-9 RDG) Personen. Lediglich § 5 enthält eine nicht explizit personale Erlaubnis zur Erbringung von „Rechtsdienstleistungen im Zusammenhang mit einer anderen Tätigkeit“, unter die die Software indes nicht fällt, und die offenkundig akzessorisch zur Tätigkeit einer natürlichen Person ist.

Als Rechtsdienstleister käme somit allenfalls der Hersteller der Software in Frage, allerdings fällt dieser unter keinen Erlaubnistatbestand des RDG, da er weder registriert ist, noch einen Erlaubnistatbestand für unregistrierte Personen erfüllt, insbesondere die Dienstleistung nicht unentgeltlich und im familiären Rahmen (§ 6 Abs. 1 RDG) erbringt.

Dies verbietet also die juristische Beurteilung von Einzelfällen durch die Software. Das scheint problematisch, denn der Sachbearbeiter wird regelmäßig mit einem konkreten Problem an die Software herantreten und eine Antwort erwarten, die praktisch verwertbare Hinweise zur Zulässigkeit zu geplanten Maßnahmen oder Verfahren erteilt. Allerdings ist eine Lösung des Einzelfalls ausdrücklich nicht Ziel der Auswertung. Ziel ist vielmehr eine verallgemeinerte, auf das CRM-Anwendungsfeld bezogene Ausgabe allgemeiner Warnungen und Hinweise auf möglicherweise erforderliche weitere Nachforschungen zur Vor-

bereitung der eigentlichen Fallprüfung durch einen Mitarbeiter und zur Sensibilisierung. Zu einer Einzelfallbetrachtung eignen sich die Excel-Tabellen nicht. Diese erlauben zwar die Auswertung von einzelnen Parametern des Einzelfalls, diese selbst sind jedoch so generell, dass sie die Besonderheiten des Falles weder berücksichtigen können noch sollen.

Gerade in Fällen, in denen nicht nur einfach zu identifizierende Tatbestandsmerkmale checklistenartig abgefragt werden, sondern Abwägungen stattfinden müssen, beschränkt sich die Prüfung auf die Sammlung und Gegenüberstellung von Kriterien. Dies ist zugleich eine notwendige technische Beschränkung des Prototypen. Abwägungen sind zum heutigen Tag ihrer Struktur nach nicht geeignet, von künstlicher Intelligenz nachvollzogen zu werden. Dies liegt vor allem daran, dass die einzelnen Argumente bis auf wenige Ausnahmen aus juristischer Sicht keine kommensurablen „Wichtungen" besitzen. Da sich der Abwägungsvorgang nach alledem nur äußerst begrenzt darstellen lässt, muss sich die Software bei der Durchführung solcher Abwägungen stets auf die Darstellung der von dem Betroffenen selbst eingegebenen Argumente in Form einer juristischen Relation (Gegenüberstellung) beschränken. Was jedoch geschehen kann, ist, dass dem Bearbeiter die rechtliche Vermutung bei der Abwägung nahegebracht wird, so die Regel, dass eine Erhebung aus allgemein zugänglichen Quellen gemäß § 28 Abs. 1 Satz 1 Nr. 3 BDSG im Zweifel zulässig ist. Dies kann etwa durch entsprechende Formulierungen und die Festlegung eines Regel-/Ausnahmeverhältnisses im Prüfaufbau deutlich gemacht werden.

6. Ausblick und Zusammenfassung

6.1 Ausblick

6.1.1 Technische und gesellschaftliche Trends

Die Zukunft im CRM hält in Bezug auf Datenschutz auseinanderstrebende Tendenzen bereit. Zum einen scheint sich das bedenkenlose Eindringen in die Privatsphäre Dritter seiner Intensität nach noch zu verschärfen, indem sowohl immer mehr Daten ohne Kenntnis der Betroffenen erhoben als auch immer mehr automatisierte Big-Data-Auswertungen für Entscheidungen mit teils großer Tragweite für den Betroffenen erfolgen. Auf der anderen Seite haben die Snowden-Enthüllungen ein selten dagewesenes öffentliches Interesse an der Integrität von Privatsphäre und Übermittlungswegen ausgelöst. Hier ist berechtigte Hoffnung angebracht, dass in Form einer Gegenbewegung zumindest der Selbstdatenschutz sowohl auf Seiten der CRM-Betreiber (etwa durch die Nutzung sicherer Clouds) wie der Nutzer von sozialen Medien wieder an Bedeutung gewinnen wird. Insoweit ist gerade im kleingewerblichen und mittelständischen Bereich eine vermehrte Sensibilität für Datenschutzfragen zu spüren. Dieser steht jedoch eine Unsicherheit und fehlende Vertrautheit mit den rechtlichen Fragen zur Seite.

6.1.1.1 Gefahren

Zwar steigt bei den verantwortlichen Stellen zunehmend das Bewusstsein für die Verantwortung, die mit datenschutzrechtlich erheblichem Handeln einhergeht. Es herrscht dennoch weiterhin nicht nur Unsicherheit über die rechtlichen Anforderungen, sondern auch über die Funktionsweise benutzter Tools. Diese Unkenntnis von den genauen Verarbeitungsvorgängen veranlasst die verantwortlichen Stellen aber nicht etwa dazu, den Einsatz von Software zu unterlassen. Vielmehr wird diese nach pragmatischen Gesichtspunkten ausgewählt und betrieben. Es ist daher dringend notwendig, das Bewusstsein darüber zu schärfen, dass der Funktionsumfang von zur Erhebung, Speicherung und Nutzung von Daten geeigneter Tools bei dem Betreiber unbedingt bekannt sein muss, um auch nur eine Einschätzung zu erlauben. Es ist diese Unbefangenheit und Gleichgültigkeit, die in der Praxis häufig mehr Schaden anrichtet als die wenigen CRM-Betreiber, die gezielt aggressive Datenerhebung betreiben.

Es muss aber auch von riskanten Tendenzen bei den einzelnen CRM-Funktionen gesprochen werden.

So vergrößert sich der Umfang der erhobenen Datenarten sprunghaft. Bestanden Kundendatenbanken früher vornehmlich aus Stammdaten und Kontakthistorie mit dem Unternehmen, werden heute immer mehr Datenarten zugespeichert, die für das Vertragsverhältnis in keiner Weise erforderlich sein können. Diese Tendenz beschränkt sich nicht auf die Speicherung und Auswertung von Social-Media-Daten. Sie umfasst durch Smartphone-Apps dieser Tage auch Gesundheitsdaten sowie Informationen über den Standort. Erstere, deren Erhebung oft entgegen § 28 Abs. 6 BDSG nicht von wirksamen Einwilligungen gedeckt sind, können zur Zusendung von Lifestyle- oder Gastronomie-Werbung eingesetzt werden, allerdings auch zur Verweigerung von Krankenversicherungsschutz oder für diskriminierende Angebote. Mit Geodaten kann ein vollständiges Bewegungsprofil einer Person erstellt werden. Die Mitübertragung des Standortes bei Postings ist für den technischen Laien oft nicht erkennbar und führt zu erheblichen

Eingriffsmöglichkeiten in die Privatsphäre sowohl durch die verantwortliche Stelle als auch durch Dritte.[363]

Die genannten Datenarten, und viele mehr, werden heute aus mehr Quellen als jemals zuvor erhoben. Das Phänomen, dass sich Datensammlungen nicht nur durch Computer, sondern auch und gerade in einfachen Alltagsgegenständen (Internet of Things)[364] abspielen, ist ein Aspekt des unter dem Begriff Ubiquitous Computing zusammengefassten Problemkomplexes.[365] So existieren längst sog. Wearables, also Datenerhebungssoftware in der Kleidung, in Ringen oder in Uhren, welche Gesundheitsdaten erfassen können und über intransparente Verbindungen übermitteln, und sodann nicht nur auf sozialen Medien posten, sondern auch zu Werbezwecken auswerten. Das Bewusstsein der Betroffenen, was mit diesen Daten tatsächlich geschieht, hat hier nur begrenzt Schritt halten können. Gleichermaßen besorgniserregend ist die Ausweitung von Datenerhebungsmechanismen in Verbrauchsgütern und die darauf aufbauende Ansammlungen von Datenbergen. Inzwischen existieren etwa Fernseher, welche nicht nur das gesehene Programm zu Marktforschungszwecken auswerten, sondern durch eine Kamera auch erkennen können, wie viele Personen vor ihm sitzen.[366]

Einen erheblichen, in die Zukunft anhaltenden Aufschwung haben in den letzten Jahren Bewertungsportale erfahren. Mehr und mehr Kunden verlassen sich bei der Auswahl von Hotels, Restaurants oder Fachverkäufern auf die Empfehlungen von Dritten. Da die Außenwirkung eines solchen Geschäfts in erheblichem Maße von den Äußerungen auf solchen Plattformen abhängt, stellt es für Unternehmen geradezu eine unabweisbare Notwendigkeit dar, auf diesen präsent zu sein, Monitoring zu betreiben und gegebenenfalls selbst aktiv einzugreifen. Hierdurch ergeben sich (bei der Benutzung von Klarnamen) datenschutzrechtliche Fragestellungen, die virulenter werden, je tiefer ein solcher Eingriff erfolgt.

Mit den so erhobenen Daten werden zunehmend intransparente und von dem Betroffenen nicht erwünschte Zwecke verfolgt.

Die Personalisierung von Webangeboten ist dann zu begrüßen, wenn diese von dem Betroffenen beeinflussbar bleibt. So ist es noch verhältnismäßig unproblematisch, aufgrund einer Zuordnung der IP zu einem Herkunftsland darauf zu schließen, dass der Betroffene in der dominierenden Sprache dieses Landes angesprochen werden möchte, soweit der Betroffene dieses Recht abweichend ausüben kann.

In vielen Fällen ist die Personalisierung, die aufgrund der Auswertung von Profildaten möglich wird, d.h. die algorithmengesteuerte Anpassung angezeigter Inhalte an die angeblichen oder tatsächlichen Präferenzen des einzelnen Nutzers, allerdings nicht erkennbar und nicht erwünscht. So führt die personalisierte Anzeige von Suchergebnissen, wie inzwischen mehrfach festgestellt, zu einer zunehmenden Verengung des Blicks bei der Wahrnehmung gesellschaftlicher Ereignisse.

---

363 Art.-29-Datenschutzgruppe, Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185 v. 16.05.2011.

364 Art.-29-Datenschutzgruppe, Opinion 8/2014 on Recent Developments on the Internet of Things, WP 223 v. 16.09.2014.

365 Polenz, in: Tamm/Tonner, Verbraucherrecht, Rn. 15 f.

366 Weichert, Internet-TV und Datenschutz – ein Annäherungsversuch, abrufbar unter https://www.datenschutzzentrum.de/vortraege/20140516-weichert-internet-tv.html.

Der Einsatz von Profilingsystemen zur (scheinbaren) Übernahme der Letztentscheidung durch einen Computer verbreitet sich ebenso rasch. Er droht nicht nur, auf weitgehend unwissenschaftlicher Grundlage den eingeschätzten Personen schwere Nachteile meist wirtschaftlicher Art zuzufügen, sondern schwächt auch das Bewusstsein der verantwortlichen Stelle für sich selbst als Verantwortlichem der Datenverarbeitung. Zudem generiert die Auswertung von Social-Media-Daten notwendigerweise eine verzerrte Identität des Betroffenen, weil sie auf Tatsachen gründet, die ihres Kontexts entrissen wurden. Diese zweite Identität im System der verantwortlichen Stelle kann von ihm kaum beeinflusst werden. Das wirft neben den datenschutzrechtlichen auch allgemein persönlichkeitsrechtliche Fragen, insbesondere zum Schutz des Selbstbilds, auf.

Ein besonderes Problem bei allen intern ablaufenden Prozessen ist, dass sie weder für den Betroffenen, noch für die Aufsichtsbehörden erkennbar sind. Da Business Intelligence keine Schnittstelle nach außen besitzt, kann der Betroffene meist nicht erkennen, dass der ihm angebotene Preis oder der ausgeschlagene Vertrag auf Profilbildung beruhen. Dadurch ist es praktisch nahezu unmöglich, gegen einzelne Datenschutzverstöße vorzugehen. Der Betroffene muss darauf vertrauen, dass eingesetzte Verfahren aller Unternehmen, welche Daten von ihm erheben, die Vorabprüfung durchlaufen und bestanden haben.

Die weiter zunehmende Auslagerung von Daten in Clouds, insbesondere in unsichere Drittländer, stellt weiterhin ein Problem für den Datenschutz dar. Erstens werden oft unbefangen Subunternehmer eingesetzt, ohne dass den Betreibern ihre Pflichten nach § 11 BDSG bewusst sind. Aus der oft mangelhaften Überwachung resultiert ein Kontrollverlust und eine fehlende Kenntnis vom Verbleib und Schicksal der ausgelagerten Daten. Zweitens setzen sich die CRM-Betreiber, ebenfalls oft unbewusst, über die europarechtlich bedingten Vorschriften über die Übermittlung in Länder ohne gleichwertiges Datenschutzniveau hinweg. Dies macht die Daten anfällig gegen unbefugte Kenntnisnahme und gegen die widerrechtliche Weiterbenutzung durch den Diensteanbieter.

Dies gilt schließlich, analog zu den Facebook-Fanpages, auch dann, wenn Betroffene aufgefordert werden, personenbezogene Daten in soziale Plattformen, die dem Telemedienrecht nicht entsprechen, hochzuladen. Unabhängig von dem Ausgang des beim Bundesverwaltungsgericht anhängigen Rechtsstreits über die datenschutzrechtliche Zulässigkeit des Betriebs von Facebook-Fanseiten[367] ist die zunehmende Tendenz zu beobachten, Betroffene zur eigenhändigen Übermittlung ihrer Daten an einen solchen Webseitenbetreiber zu verleiten, etwa bei Foto-Wettbewerben auf sozialen Medien. Ob nach der Rechtsprechung hier eine Äquivalenz zu der Cloudproblematik besteht, bleibt abzuwarten.

6.1.1.2 Chancen

Zwar ist die Erkenntnis, dass ein Wettbewerbsvorteil durch Datenschutz möglich ist, noch nicht sehr weit verbreitet. Gleichzeitig hat sich jedoch die Erkenntnis durchgesetzt, dass ein unzureichender Datenschutz neben den rechtlichen Konsequenzen ein Makel ist, der Unternehmen Kunden und Auftraggeber kosten

[367] Pressemitteilung des ULD v. 29.09.2014, abrufbar unter https://www.datenschutzzentrum.de/artikel/770-ULD-OVG-Urteil-zu-Facebook-Fanpages-revisionsbeduerftig.html#extended.

kann. Spätestens seit den Enthüllungen im NSA-Skandal besteht eine erhöhte Sensibilität etwa für die Sicherheit von Cloud-Lösungen.[368]

Ebenfalls zu beobachten ist eine zunehmende Sensibilisierung von Nutzern sozialer Netzwerke für den Verbleib ihrer Daten. Zwar ist festzustellen, dass viele Betroffene weiterhin die inzwischen bekannten Gefahren im Gegenzug gegen unterhaltsame und kostenlose Services in Kauf nehmen. Allerdings ist der Datenschutz allgemein durch die Enthüllungen der vergangenen beiden Jahre jedenfalls ansatzweise in den Fokus der Aufmerksamkeit und der Berichterstattung gerückt. In praktischer Umsetzung des gestiegenen Bewusstseins für den Datenschutz auf Wirtschaftsseite ist eine gestiegene Anzahl von Produkten auch im CRM-Bereich zu verzeichnen, die unter den Schlagworten privacy-by-default und privacy-by-design bereits durch die Gestaltung des Produkts den rechtlichen Anforderungen Rechnung zu tragen bemüht sind. Hierin liegt üblicherweise ein Verzicht auf Erhebung und Nutzung personenbezogener Daten. Privacy by Design ist dabei die Gestaltung eines Verfahrens dergestalt, dass Verstöße nicht vorkommen können. Ein Beispiel ist die effektive Anonymisierung von Daten unmittelbar nach ihrer Erhebung. Privacy by Default bedeutet, dass die Privatsphäreeinstellungen auf einem datenschutzfreundlichen Niveau standardisiert sind. Die Erhebung von zusätzlichen Daten bedarf damit weiterer Einstellungen, was das Bewusstsein der verantwortlichen Stelle wie auch das des Nutzers erhöht.

6.1.2 Rechtliche Entwicklungen

Abschließend ist noch auf die rechtlichen Veränderungen, die sich für das Datenschutzrecht abzeichnen, einzugehen.

Auf der Ebene der Europäischen Union unterliegt das Datenschutzrecht derzeit einem Reformprozess. Bisher ist die Materie in Form von Richtlinien geregelt, die zwar Auslegungsgrundlage für das Bundesrecht sind, aber keine unmittelbare Wirkung für den Rechtsunterworfenen beanspruchen können. Dies soll sich nach dem Willen des Europäischen Parlaments und zumindest eines Großteils von Kommission und Rat mit der geplanten Einführung einer Datenschutzgrundverordnung[369] ändern. In Nr. 7 der inoffiziellen Fassung des Europäischen Parlaments wird beklagt, dass die Richtlinie von 1995 in den Mitgliedsstaaten zu uneinheitlich umgesetzt worden sei. Daher sei es notwendig, Datenschutzpraktiken über Grenzen hinweg zu harmonisieren. Dies ist im Europarecht nur mit Hilfe des Rechtsinstituts der Verordnung möglich.

Inwieweit im Sinne der begrenzten Einzelermächtigung im Bundesrecht noch Möglichkeiten bleiben, eigene gesetzgeberische Vorstellungen umzusetzen, die gegebenenfalls noch über die Verordnung hinausgehen, bleibt abzuwarten. Die Verordnung selbst enthält einige Verweise auf die genauere Gestaltung durch nationales Recht. Es ist dennoch damit zu rechnen, dass die zentralen Vorschriften insbesondere des BDSG zur Datenerhebung damit hinfällig werden.

Auch im Falle ihres Erlasses wird sie erst zwei Jahre nach Inkrafttreten die inländischen Gesetze innerhalb ihres Regelungsbereichs ablösen. Im Folgenden sollen, basierend auf dem vorliegenden konsolidierten

[368] Voigt, MR 2014, S. 158.

[369] Siehe Fußnote 344.

Entwurf, welcher das Europäische Parlament in erster Lesung passiert hat, die wichtigsten Änderungen für CRM-Betreiber skizziert werden.

6.1.2.1 Sachlicher und örtlicher Anwendungsbereich

Bisher galt, dass eine verantwortliche Stelle aufgrund des Sitzlandprinzips grundsätzlich bestimmen konnte, welchem nationalen Datenschutzrechtsregime, und damit welcher Form von Umsetzung der Datenschutzrichtlinie sie sich unterwerfen wollte. So war es für CRM-Betreiber aus Übersee möglich, ihre Geschäftstätigkeit in Ländern abzuwickeln, deren Umsetzung der Richtlinie zwar den Anforderungen entsprach, um nicht von der Kommission gerügt zu werden und wegen unklarer Umsetzungsvorschriften oder der Aufsichtspraxis Verarbeitungsvorgänge zuließ, die nach den Umsetzungen anderer Mitgliedsstaaten rechtswidrig gewesen wären. In der erwähnten Google-Entscheidung schränkte der EuGH diese Praxis bereits deutlich ein, indem er entschied, dass bereits die Durchführung von Nebentätigkeiten wie die Anzeigenakquise in einem Mitgliedstaat zur Anwendung des nationalen Rechts dieses Mitgliedsstaats führen kann. Der Verordnungsentwurf geht hierüber nicht nur dadurch hinaus, dass er weitgehend die unterschiedlichen nationalen Datenschutzrechtsregimes vereinheitlicht. Vielmehr wird auch der Anwendungsbereich des europäischen Rechts selbst erweitert, indem gemäß Art. 3 Nr. 2 des Verordnungsentwurfs Europarecht auch für im Ausland belegene Stellen immer dann anzuwenden ist, wenn Datenverarbeitung im Rahmen eines auch an EU-Bürger gerichteten Angebots erfolgt. Nach Nr. 1 der Vorschrift gilt außerdem wie bisher, dass EU-Recht anzuwenden ist, wenn die verantwortliche Stelle oder ihre Auftragnehmer ihren Sitz in der EU haben, und zwar unabhängig vom Ort der Datenverarbeitung. Dadurch soll ein einheitlicherer Rechtsschutz der EU-Bürger gewährleistet werden, die oft die Faktoren, von denen ihre Rechtsschutzmöglichkeiten und die für sie geltenden Datenschutzstandards abhängen, nicht erkennen können. Inwieweit ein effektiver Rechtsschutz gegen juristische Personen außerhalb der EU möglich sein wird, bleibt abzuwarten.

6.1.2.2 Grundvoraussetzungen der Datenverarbeitung

In der Frage der Zweckbindung (Art. 5 b) des Verordnungsentntwurfs) wird der Richtlinie darin gefolgt, dass zwar ein legitimer Zweck bei Erhebung festzulegen ist, die Zweckbindung im Vergleich zu derzeitigen Bundesrecht allerdings weniger streng ist. So darf die Nutzung der erhobenen Daten zum festgelegten Zweck nur nicht inkompatibel sein, eine formelle Zweckänderung im Sinne von § 28 Abs. 2 BDSG ist nicht erforderlich. Die Art.-29-Datenschutzgruppe war in ihrem Working Paper 203 aus dem Jahre 2013 bemüht, den Begriff der Kompatibilität zu umreißen. Sie zog dabei v.a. Transparenz- und Erwartbarkeitskriterien heran.[370] Der Begriff der Kompatibilität wird in der Praxis dennoch eine genauere Form erhalten müssen, soll er nicht zu einem Freibrief für Unternehmen werden, willkürlich aus ihrer Sicht „verwandte“ Tätigkeiten an den Erhebungszweck anzuhängen.

Art. 5 c) des Verordnungsentwurfs enthält ein generelles Erforderlichkeitskriterium. Die Privilegierung der verantwortlichen Stelle bei der Erhebung von Daten aus öffentlich zugänglichen Quellen wird damit wegfallen. Daneben ist wohl daran gedacht, das Prinzip der Datenvermeidung entgegen § 3a BDSG zu einer Zulässigkeitsvoraussetzung der Datenverarbeitung zu machen, d.h. wer personenbezogene Daten

[370] Art. 29-Datenschutzgruppe, WP 203, S. 39.

erhebt, obwohl anonyme Daten dem Zweck genügen würden, handelt bereits deswegen rechtswidrig, ohne dass es auf die Interessenabwägung ankäme.

Art. 5 d) des Verordnungsentwurfs bestimmt ausdrücklich, dass zu verarbeitende Daten richtig sein müssen. Dies wird Big-Data-Verarbeitern zumindest im Rahmen des Zumutbaren eine Prüfpflicht auferlegen, die einen weiteren Anreiz zur weitestgehenden Anonymisierung darstellen dürfte. Art 5 e) des Verordnungsentwurfs enthält darüber hinaus eine ausdrückliche Pflicht, die das BDSG nur implizit kennt, nämlich das Vorhalten von Daten in einer Form, die dem Betroffenen die Ausübung seiner Rechte gestattet.

Entgegen der bisherigen deutschen Rechtsprechungspraxis wird in Art. 24 des Verordnungsentwurfs zudem klargestellt, dass die Verantwortung für datenschutzrechtliche Maßnahmen wie bisher auch zweigeteilt sein kann. Die Vorschrift zwar legt nur die Rechtsfolgen fest, setzt aber die Möglichkeit der gemeinsamen Verantwortlichkeit voraus.

Art. 40 ff. des Verordnungsentwurfs enthalten ausgeweitete Bestimmungen über den Datentransfer in unsichere Drittländer. Im Kern bleibt es bei den Rechtsgrundlagen Einwilligung, Standardvertragsklauseln und Binding Corporate Rules.

6.1.2.3 Rechtsgrundlagen für die Zulässigkeit von Maßnahmen

Der Katalog der Rechtsgrundlagen zulässiger Datenverarbeitung folgt dem Grundmuster der Richtlinie. Er wird das zersplitterte System der teils sachlich, teils rechtlich definierten, und sich daher überschneidenden Rechtsgrundlagen des BDSG ablösen. Auch das neue Recht wird Abgrenzungsprobleme bringen, aber im Vergleich zu den unübersichtlich und unlesbar gewordenen bundesrechtlichen Vorschriften (elf Absätze zu § 28 BDSG, sieben Absätze zu § 29 BDSG und eine Handvoll Spezialnormen, deren Anwendungsbereich und Verhältnis zu den Generalklauseln §§ 28, 29 BDSG häufig unklar ist) hält der Verordnungsentwurf eine willkommene Vereinfachung bereit. Nachteil wird sein, dass die bereits als für Praktiker kaum handhabbar bekannte Notwendigkeit der Abwägung weiterhin einen Großteil der Zulässigkeitsprüfung in Fällen ausmachen wird, in denen vom Betroffenen keine Einwilligung vorliegt. Hier wären mehr Vorgaben für die Abwägung wünschenswert gewesen.

Die drei entscheidenden Rechtsgrundlagen, welche in §§ 4a, 28 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG ihre grundsätzliche Entsprechung finden, sind die Einwilligung (Art. 6a) des Verordnungsentwurfs), die Erforderlichkeit zur Vertragsdurchführung auf Veranlassung des Betroffenen (Art. 6b) des Verordnungsentwurfs) und die Erforderlichkeit für eigene Geschäftszwecke nach Abwägung (Art. 6f) des Verordnungsentwurfs).

Voraussetzungen und Wirkungen der Einwilligung (Art. 7 des Verordnungsentwurfs) entsprechen weitestgehend der gegenwärtigen Rechtslage. In Art. 7 Nr. 4 des Kommissionsentwurfs war vorgesehen[371], dass Einwilligungen bei Vorliegen eines erheblichen Ungleichgewichts unwirksam sein können. Hierzu sollten nach dem inzwischen folgerichtig ebenfalls gelöschten Erwägungsgrund 34 insbesondere rechtliche Abhängigkeitsverhältnisse wie das Arbeitsverhältnis zählen. Die Vorschrift findet sich im vorliegen-

[371] Vorschlag der Europäischen Kommission für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 2012/0011 (COD).

den Entwurf nicht mehr. Eine weiterhin im Entwurf des Parlaments vermerkte Änderung betrifft die Grenzen der konkludenten Einwilligung. Bisher musste die Einwilligung nur unzweideutig („unambiguously") abgegeben werden. Nach Art. 4 Nr. 8 des Verordnungsentwurfs besteht das Erfordernis der ausdrücklichen („explicit") Einwilligung. Dies kann insbesondere auf diejenigen Einwilligungen durchschlagen, die derzeit im Wege des Opt-Out eingeholt werden, so z.B. bei der postalischen Werbezusendung. Die Folgen bleiben abzuwarten.

Ausdrücklich wird das Recht zum Widerruf ex tunc (Art. 7 Nr. 3 des Verordnungsentwurfs) geregelt, wobei wie bisher von einer Berechtigung der verantwortlichen Stelle zum Unterlassen der Gegenleistung ausgegangen wird. Gemäß Art. 7 Nr. 4 des Verordnungsentwurfs ist eine Einwilligung unwirksam, wenn ihr Zweck nicht mehr erreicht werden kann.

Die Abwägung im Falle der Erforderlichkeit der Datenverarbeitung zu Geschäftszwecken bewegt sich im Bereich dessen, was der Betroffene „vernünftigerweise erwarten" durfte. Ist die Datenverarbeitung vernünftigerweise zu erwarten, wird die Maßnahme nur dann unzulässig sein, wenn die berechtigten, regelmäßig grundrechtlich geschützten Rechtspositionen des Betroffenen den Ausschluss erfordern. Dies erlaubt auch eine Berücksichtigung des Allgemeinen Persönlichkeitsrechts nach dem Grundgesetz. Insoweit können mitgliedsstaatliche Verfassungsprinzipien auch dann bei der Auslegung Anwendung finden, wenn sie, wie das Recht auf informationelle Selbstbestimmung, in keiner anderen mitgliedsstaatlichen Verfassung geschützt sind (wohl auch gemäß Art. 21 Nr. 1 f) desVerordnungsentwurfs).

Art. 8 des Verordnungsentwurfs enthält ausdrückliche Vorschriften zur Datenverarbeitung in Bezug auf Kinder und definiert eine Untergrenze der Einsichtsfähigkeit bei 13 Jahren. Auch diese Vorgabe ist im Vergleich zu der derzeit geltenden Einzelfalllösung des Bundesrechts willkommen.

„Profilbildung" , die gemäß Art. 2 Nr. 3a) des Verordnungsentwurfs inhaltlich weitgehend der automatisierten Entscheidung nach § 6a BDSG entspricht, ist unter folgenden Voraussetzungen zulässig: Entweder sie ist strikt erforderlich für den Vertragsschluss (z.B. Wiedererkennung zur Betrugsvermeidung), sie wird im Europarecht oder dem Recht der Mitgliedsstaaten spezialgesetzlich erlaubt, oder sie basiert auf Einwilligung des Betroffenen. In jedem Fall sind Schritte zu unternehmen, im Gegenzug die schutzwürdigen Interessen des Betroffenen zu schützen. Es liegt nahe, dass mit der Formulierung ähnliche Maßnahmen wie in § 6a Abs. 2 Nr. 2, 1. Alt. BDSG gemeint sind, also insbesondere die Herstellung von Transparenz und die Schaffung von Einflussmöglichkeiten für den Betroffenen. Ausdrücklich verboten werden schließlich Profilbildungen auf Basis besonderer Arten personenbezogener Daten, was angesichts der Tatsache, dass diese oft im Rahmen der Vertragsabwicklung rechtmäßig an die verantwortliche Stelle gelangen können, eine willkommene Einschränkung der legitimen Zwecke darstellt.

6.1.2.4 Betroffenenrechte und Betreiberpflichten

Eine Ausweitung der Betreiberpflichten betrifft die Benachrichtigungspflichten gegenüber dem Betroffenen. Diese sind zweistufig ausgebaut. Auf der ersten Stufe (Art. 13a des Verordnungsentwurfs) soll der Betroffene durch die Nutzung von Tafeln mit Standardsymbolen darauf hingewiesen werden, ob etwa mehr Daten als notwendig erhoben oder ob Daten an Dritte übermittelt werden. Auf der zweiten Stufe (Art. 14 des Verordnungsentwurfs) sollen dem Betroffenen schließlich Informationen über die geplante Datenverarbeitung zukommen. Zu den Daten, über die benachrichtigt werden soll, gehören neben denjenigen nach § 33 BDSG unter anderem die Datenquellen, die geplante Speicherdauer oder deren Be-

rechnungsmethode, der Umstand der Anlage eines Profils sowie dessen Nutzung, aber auch, ob Daten an Geheimdienst- und Strafverfolgungsbehörden weitergegeben wurden. Zu der Belehrung gehört neben Auskunft über die Betroffenenrechte auch der Hinweis auf das Recht zur Eingabe bei der Aufsichtsbehörde, was im Ergebnis einer Pflicht zur Erteilung einer Rechtsbehelfsbelehrung nahekommt.

Weitgehende Entsprechung zur geltenden deutschen Rechtslage herrscht im Bereich der Berichtigungs- und Löschungsansprüche. Auch die Voraussetzungen der Sperrung wurden in Art. 17 Nr. 4 ff. des Verordnungsentwurfs sinngemäß weitgehend dem geltenden deutschen Recht entsprechend formuliert.

Der Betroffene darf gemäß Art. 19 Nr. 2 ff. des Verordnungsentwurfs nunmehr auch über § 28 Abs. 4 BDSG hinaus solchen Datenverarbeitungsvorgängen widersprechen, an denen die verantwortliche Stelle ansonsten nach Art. 7 Nr. 1 f) des Verordnungsentwurfs ein überwiegendes Interesse hat. Es wird abzuwarten sein, inwieweit dies etwa die Beweisgewinnung oder andere Formen der „Selbstverteidigung" verantwortlicher Stellen in sozialen Netzwerken beeinflusst. Dasselbe gilt für die Profilbildung.

In einer eher deklaratorischen Vorschrift wird die Nutzung von Privacy-by-default- und Privacy-by-design-Technologien nahegelegt. Art. 32a und 33 des Verordnungsentwurfs enthalten die Verpflichtung zu einer Risikoanalyse hinsichtlich der Grundrechtsrelevanz von Verfahren, und nennt in der Form rechtlicher Vermutungen Beispiele solcher Risiken, was angesichts der unklaren Rechtslage über den Umfang der Vorabprüfung zu begrüßen ist.

6.1.2.5 Aufsichtsrechtlicher Rahmen

Wichtigste aufsichtsrechtliche Neuerung ist das Prinzip des sog. One-Stop-Shop. Betroffene wie verantwortliche Stellen können grundsätzlich alle rechtlichen Fragen bei der Datenschutzaufsicht ihres Heimatorts bzw. Sitzes klären lassen. Ist eine Rechtsangleichung in bestimmten Fragen notwendig, muss die Aufsichtsbehörde diese dem neu zu gründenden Europäischen Datenschutzausschuss vorlegen, die im Wege des sogenannten Konsistenzmechanismus über europarechtlich einheitliche Behandlung entscheidet (Art. 54a ff. des Verordnungsentwurfs). Schließlich wurde noch der Bußgeldkatalog auf alle Zuwiderhandlungen gegen die Verordnung erweitert, was in Zusammenhang mit der Befugnis der Aufsichtsbehörde, gegebenenfalls von der Verhängung eines Bußgelds abzusehen, Sinn macht. Die Möglichkeit einer Bemessung des Bußgelds nach Anteilen am Jahresumsatz der verantwortlichen Stelle wird zusätzlich eröffnet.

Immer wieder wird erwogen, mit der Neuordnung des europäischen Datenschutzrechts auch den Datentransfer in Drittstaaten, insbesondere in die USA, zu regeln. Eine Verpflichtung von US-Unternehmen auf die sog. Safe-Habor-Grundsätze erwies sich bisher nicht als ausreichendes Regulierungsinstrument. Unternehmen in den EU-Mitgliedstaaten sind daher aufgefordert, vor allem die Verwendung von EU-Standardvertragsklauseln zu prüfen. Dass dies notwendig ist, ist seit Jahren der Standpunkt der Aufsichtsbehörden.[372] Der Verordnungsentwurf enthält keinen Hinweis auf die Safe-Harbor-Grundsätze. Mit

[372] Zuletzt im März 2015 bekräftigte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass kein ausreichendes Datenschutzniveau durch Safe Harbor gewährleistet würde. Abrufbar unter: http://www.datenschutz.sachsen-anhalt.de/konferenzen/nationale-datenschutzkonferenz/entschliessungen/entschliessungen-der-89-datenschutzkonferenz-18-und-19-maerz-in-wiesbaden/safe-harbor-bietet-keinen-ausreichenden-schutz-fuer-den-datentransfer-in-die-usa.

der Grundverordnung hat das europäische Datenschutzrecht die Chance, einen großen Teil der Übermittlungen im CRM-Bereich auf eine rechtmäßige Grundlage zu stellen.

Das gestiegene Interesse hat schließlich dazu geführt, dass viele Unternehmen Pläne für die Compliance der eigenen Arbeitsabläufe speziell im datenschutzrechtlichen Bereich geschaffen haben. So ist das Interesse etwa am BSI-Grundschutz sowie an Zertifizierungen in den letzten Jahren gestiegen.

6.2 Zusammenfassung der Ergebnisse des Projekts

Im Folgenden sollen die wichtigsten juristischen Erkenntnisse der vorangegangenen Begutachtung kapitelübergreifend zusammengefasst und abschließend erläutert werden. Dabei sollen auch Anregungen zur Verbesserung des geschriebenen Rechts für spätere Gesetzesvorhaben gegeben werden.

6.2.1 Kontrolle und klare Verantwortlichkeit

Zum rechtmäßigen Betrieb eines CRM gehört eine vollständige Kenntnis von dessen Funktionen, die jederzeit mögliche Ausübung von Kontrolle und die klare Zuordnung von Verantwortlichkeit für die eingesetzten Verfahren. In der Praxis kranken viele CRM-Systeme daran, dass ihre Betreiber keinen vollständigen Überblick über die datenschutzrechtlich relevanten Vorgänge haben, die von komplexer Software ausgelöst werden. Darüber hinaus ist ein Kontrollverlust bemerkbar, indem die verantwortliche Stelle die Software laufen lässt und sich nicht in der Rolle des datenschutzrechtlich Verantwortlichen sieht.

Das Gesetz hat dem in § 11 BDSG Rechnung getragen, indem dem Auftraggeber in Auftragsdatenverarbeitungsverhältnissen die vorsätzliche oder fahrlässige Unkenntnis von tatsächlichen Abläufen rechtlich unmöglich gemacht wird. Nur im Ausnahmefall kann ein Verantwortlicher, der keine Kenntnis von der Arbeitsweise der von ihm eingesetzten Software hat, gegebenenfalls der bußgeldrechtlichen Haftung für hierdurch verursachte Datenschutzverstöße entgehen, wenn ihn kein Fahrlässigkeitsvorwurf trifft.

6.2.2 Rechtmäßiger Betrieb des Social Media Accounts

Der Betrieb eines Accounts auf einem sozialen Medium ist unzulässig, wenn das Medium entweder nicht dem Telemediengesetz genügt, oder die verantwortliche Stelle einen qualifizierten Anreiz dafür bietet, dass die Daten der Nutzer in unrechtmäßiger Art und Weise verarbeitet werden. In solchen Fällen wird der Betreiber des Accounts nach telemedien- bzw. ordnungsrechtlichen Maßstäben für den Zustand der Seite mitverantwortlich, weil er die Zwecke und Mittel der Datenverarbeitung mitbestimmt und eine adäquate Gefahr für die Rechte der Nutzer setzt. Dies verbietet nach deren derzeitigem Zustand den Betrieb von Facebook-Fanpages.

6.2.3 Ausreichende Informationen bei elektronischer Einwilligung

Elektronische Einwilligungen nach § 4a BDSG und § 13 Abs. 2 TMG durch spontane Äußerung auf sozialen Medien sind zwar denkbar. Erklärungen in diesem Sinne scheitern jedoch regelmäßig an der Bestimmtheit oder an der fehlenden vorherigen Information.

Einwilligungen sind daher weiterhin in Schriftform oder geeigneter elektronischer Form nach Belehrung einzuholen. Dies gilt auch dann, wenn dem Betroffenen auf dessen, über sozialen Medien geäußerten, Wunsch Material zugesandt werden soll, das Werbung enthält.

6.2.4 Allgemeine Zugänglichkeit von Social Media Daten

Daten auf sozialen Netzwerken, die der Nutzer nicht geschützt hat, sind regelmäßig allgemein zugänglich im Sinne des § 28 Abs. 1 Satz 1 Nr. 3 BDSG. Aus der Tatsache, dass in den Datenschutzrichtlinien der Social Media Plattformen oft bestimmte erlaubte Zwecke festgelegt werden, folgt aber eine Begrenzung der nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG erhebbaren Daten auf diejenigen, deren Nutzung für den festgelegten Zweck zulässig ist.

Dabei handelt es sich um eine praktisch wichtige Einschränkung des verarbeitungsfreundlichen § 28 Abs. 1 Satz 1 Nr. 3 BDSG. Er erlaubt gerade nicht die Speicherung von Daten in beliebigem Umfang. Da für die möglichen Nutzungen wegen der Verkettung mit CRM-Daten fast immer § 28 Abs. 1 Satz 1 Nr. 2 BDSG anwendbar ist, ist die verantwortliche Stelle bereits bei der Erhebung gehalten, nur die für diese Nutzung erforderlichen und zulässigen Daten zu erheben. Die Möglichkeit der Zweckänderung nach § 28 Abs. 2 BDSG ändert hieran nichts.

6.2.5 Datensparsamkeit und Datenvermeidung

§ 3a BDSG enthält zwar keine zusätzliche Zulässigkeitsvoraussetzung für Datenerhebungen. Finden allerdings Datenerhebungen ohne Rücksicht auf Datenvermeidung und Datensparsamkeit statt, überwiegt im Falle einer Abwägung in der Regel das Interesse des Betroffenen, von der Maßnahme freizubleiben. Dadurch ist die verantwortliche Stelle gehalten, auch in Fällen des § 28 Abs. 1 Satz 1 Nr. 3 BDSG das eingesetzte Verfahren darauf auszurichten, nur so viele Daten zu erheben, wie es dem Zweck entspricht. Werden Daten nicht anonymisiert, obwohl der legitime Verwendungszweck keinen Personenbezug erfordert, wird sich das Interesse des Betroffenen am Ausschluss der Speicherung regelmäßig durchsetzen.

6.2.6 Ankauf von Social Media Daten

Der Ankauf von Social-Media-Daten, die Dritte erhoben haben, ist außerhalb des Listenprivilegs des § 28 Abs. 3 BDSG grundsätzlich nur dann erlaubt, wenn der Nutzer eingewilligt hat. Nur in diesem Fall kann die verantwortliche Stelle gewährleisten, dass Datenerhebungen unter Wahrung der Rechte von Betroffenen erfolgen. Die Tätigkeit von Datenbrokern außerhalb des von den §§ 28 Abs. 3, 29 BDSG erlaubten Adresshandels verstößt regelmäßig gegen den Zweckbindungsgrundsatz, weil die einzelnen Daten für einen zum Zeitpunkt der Erhebung unbestimmten Zweck erhoben wurden. An solchen Daten, die wegen ihrer Zusammenstellung zu Profilen typischerweise auch nicht mehr allgemein zugänglich sind, hat die verantwortliche Stelle regelmäßig kein berechtigtes Interesse.

6.2.7 Überprüfung der inhaltlichen Richtigkeit der Social Media Daten

Die inhaltliche Richtigkeit erhobener Daten im Einzelfall ist bei der Erhebung aus allgemein zugänglichen Quellen immer dann zu überprüfen, wenn die Nutzung rechtliche oder tatsächliche Folgen für den Be-

troffenen haben kann. Aus der Privilegierung nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG folgt allerdings zunächst, dass die verantwortliche Stelle nicht jedes im Wege des Monitoring erhobene Datum inhaltlich prüfen muss. Werden hingegen Entscheidungen auf Basis dieser Daten gefällt, müssen diese auf zutreffender sachlicher Grundlage erfolgen, anderenfalls hat die verantwortliche Stelle hieran kein berechtigtes Interesse.

6.2.8 Social Media als Kommunikationsmittel

Wegen der grundsätzlichen Gefahr des Identitätsdiebstahls auf sozialen Medien muss Kundenservice soweit möglich auf einem sicheren Kommunikationsweg stattfinden. Das betrifft insbesondere Fälle, die Abfragen aus dem CRM betreffen, da dabei nicht allgemein zugängliche Daten verarbeitet werden. Der öffentliche Teil von sozialen Netzwerken ist kein sicherer Kommunikationsweg. Hiervon sind einfache, sachbezogene Auskünfte ausgenommen.

Soweit der Betroffene seinen Account gegenüber der verantwortlichen Stelle für die Abwicklung von Servicefällen geöffnet hat, kann dieser regelmäßig hierfür genutzt werden. Die Gefahr des Identitätsdiebstahls ist insoweit nicht größer als bei der Nutzung eines beliebigen anderen nichtsignierten Fernkommunikationsmittels. Allerdings ist die verantwortliche Stelle immer gehalten, dem Verdacht eines Identitätsdiebstahls nachzugehen. Es ist grundsätzlich der nichtöffentliche Weg, etwa durch ein plattformeigenes Nachrichtensystem, zu wählen.

Bestehen Zweifel über das Einverständnis des Betroffenen zur öffentlichen Antwort, ist die darin liegende Übermittlung personenbezogener Daten (auch) an unbestimmte Dritte regelmäßig nicht gerechtfertigt. Dies gilt zunächst allgemein und auch dann, wenn der Accountinhaber als mit dem tatsächlichen Namensträger identisch bekannt ist, wenn sich das Einverständnis des Betroffenen zu dieser Vorgehensweise nicht manifestiert hat. Wenn unsicher ist, ob der Accountinhaber mit dem tatsächlichen Kunden identisch ist, muss ausgeschlossen werden, dass der Fragende sich eine verdeckte Auskunft durch Bestätigung einer konkreten Anfrage erschleichen kann. Vor diesem Hintergrund ist auch die bloße Bestätigungen über die Richtigkeit personenbezogener Daten als rechtfertigungsbedürftige Verarbeitung von Daten zu beurteilen.

6.2.9 Zwecktrennung bei Zuspeicherung in Kundendatenbank

Die verantwortliche Stelle darf außerhalb des Listenprivilegs des § 28 Abs. 3 BDSG Daten in ihrer Kundendatenbank nicht dauerhaft mit CRM-Daten anreichern, ohne hierzu eine Einwilligung eingeholt zu haben. Zuspeicherungen in die generelle Kundendatenbank widersprechen regelmäßig dem Grundsatz der Getrenntspeicherung, weil Daten für Werbekampagnen, Statistiken, Beschwerdemanagement und Service vermischt werden. Damit wird auch die Profilbildung möglich, wobei eine Nutzung nach §§ 6a, 28b BDSG nur unter besonderen Bedingungen zulässig ist. Daher hat in solchen Fällen der Betroffene regelmäßig ein Interesse, von derartigen Erhebungen freizubleiben. Eine technische Lösung ist die Anlage mehrerer Datenbanken zu verschiedenen Zwecken, wobei zu beachten ist, dass etwa Details von Servicevorgängen nicht willkürlich über die Geschäftsbeziehung hinaus gespeichert werden dürfen. Am Ausschluss der personenbezogenen Auswertung des CRM nach Anreicherung aus automatisiert erhobenen öffentlichen Profilen ohne Einwilligung hat der Betroffene regelmäßig ein überwiegendes berechtig-

tes Interesse. § 28 Abs. 1 Satz 1 Nr. 3 BDSG findet auf die durch Verkettung entstandenen neuen Daten keine Anwendung.

6.2.10 Profiling auf Grundlage von Social Media Daten

Die automatisierte Einschätzung von Persönlichkeitsmerkmalen eines Betroffenen auf Basis von Social-Media-Daten zur Vorbereitung einer automatisierten Entscheidung ist nur dann zulässig, wenn dem Betroffenen keine unmittelbare Rechtsfolge und kein erheblicher Nachteil drohen. Die Bildung eines Zahlenwerts aus einem Posting kann als Mittel der Pseudonymisierung hingegen zulässig sein. Unter die regelmäßig unzulässigen Praktiken nach § 6a BDSG fällt u.a. die Festlegung dynamischer Preise oder die sonstige finanzielle Einschätzung von Betroffenen auf Grundlage von Social-Media-Daten. Die sog. Tonalitätsanalyse ist dagegen häufig datenschutzrechtlich unbedenklicher als die Speicherung eines gesamten Postings, wenn es der verantwortlichen Stelle nur um die ausgedrückte Stimmung geht und eine Reidentifizierung zur direkten Ansprache nicht geplant ist. Dies gilt insbesondere dann, wenn das originale Posting nach Berechnung eines Scores aus dem System gelöscht wird und dem CRM-Benutzer ausschließlich aggregierte Daten angezeigt werden.

6.2.11 Informationspflichten bei der Nutzung von Social Media Daten

Die Benachrichtigungs- und damit Auskunftspflichten fallen bei der Verarbeitung von Social Media Daten nicht wegen Unzumutbarkeit (§§ 33 Abs. 2 Nr. 7a BDSG, 34 Abs. 7 BDSG) weg.

Dies folgt aus der Tatsache, dass das Monitoring freiwillig ist, die verantwortliche Stelle durch ihre Praxis die logistischen Schwierigkeiten bei der Benachrichtigung somit selbst herbeiführt, ohne dazu geschäftlich im Sinne der Erforderlichkeit gezwungen zu sein, und damit für fehlende Leistungsfähigkeit einstehen muss. Will sie der Benachrichtigungspflicht entgehen, muss sie regelmäßig auf die Speicherung verzichten. Die Benachrichtigungspflicht fällt jedoch weg, soweit ein erhobenes Datum Angaben zu einer Person enthält, die nicht greifbar ist (etwa Äußerungen über einen Dritten auf Twitter), denn die verantwortliche Stelle darf durch die Benachrichtigung nicht mehr Daten erheben, als ihr zulässigerweise aus der Maßnahme selbst erwachsen.

7. Literaturverzeichnis

Bücher, Kommentare

Auernhammer, Herbert	Bundesdatenschutzgesetz mit TMG, TKG, EnWG und IFG 4. Auflage Köln u.a., 2014
Ambrock, Jens	Die Übermittlung von S.W.I.F.T.-Daten an die Terrorismusaufklärung der USA, Berlin, 2013
Bader, Johann *Ronellenfitsch, Michael*	Beck'scher Onlinekommentar zum VwVfG, 24. Edition, München, 2014
Bamberger, Heinz Georg *Roth, Herbert (Hrsg.)*	Kommentar zum Bürgerlichen Gesetzbuch Band 3, 3. Auflage, München, 2012
Bergmann, Lutz *Möhrle, Roland* *Herb, Armin (Hrsg.)*	Datenschutzrecht, Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz, 47. Ergänzungslieferung, Stuttgart, 2014
Bruhn, Manfred	Kundenorientierung, Bausteine für exzellentes Customer Relationship Management (CRM) 4. Auflage, München, 2012
Däubler, Wolfgang *Klebe, Thomas* *Wedde, Peter* *Weichert, Thilo*	Bundesdatenschutzgesetz 4. Auflage, Frankfurt am Main, 2014
Damm, Renate *Rehbock, Klaus*	Widerruf, Unterlassung und Schadensersatz in den Medien, 3. Auflage, München, 2008
Bonk, Barbara	Technische Möglichkeiten der Datenerhebung und zivilrechtliche Folgen bei Verstoß gegen die datenschutzrechtlichen Informationspflichten, München, 2009
Dörr, Erwin	Neues Bundesdatenschutzgesetz. Handkommentar, 1. Auflage,

Schmidt, Dietmar Frechen, 1997

Ehmann, Eugen (Hrsg.) Lexikon des IT-Rechts 2014/2015, Die wichtigsten 150 Praxisthemen, 5. Auflage, Heidelberg, 2014

Epping, Volker
Hillgruber, Christian Beck'scher Online-Kommentar zum GG, 22. Edition, München, 2014

Erbs, Georg
Kohlhaas, Max (Hrsg.) Strafrechtliche Nebengesetze, 195. Ergänzungslieferung, München, 2013

Eschenbacher, Michael: Datenerhebung im arbeitsrechtlichen Vertragsanbahnungsverhältnis,Frankfurt am Main, 2008

Gierschmann, Sybille
Säugling, Markus Systematischer Praxiskommentar Datenschutzrecht, Köln, 2014

Gola, Peter
Schomerus, Rudolf
(Hrsg.) Bundesdatenschutzgesetz, 12. Auflage, München, 2015

Grabitz, Eberhard
Hilf, Meinhard
Nettesheim, Martin
(Hrsg.) Das Recht der Europäischen Union, 55. Ergänzungslieferung, München, 2015

Grützner, Thomas
Jakob, Alexander (Hrsg.) Compliance von A-Z, 1. Auflage, München, 2010

Hansen, Marit
Meissner, Sebastian
(Hrsg.) Verkettung digitaler Identitäten, Kiel, 2007

Hesse, Konrad Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Auflage, Heidelberg, 1995

Hoeren, Thomas
Sieber, Ulrich
Holznagel, Bernd (Hrsg.)
Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs,
39. Auflage,
München, 2014

Jauernig, Othmar (Hrsg.)
Bürgerliches Gesetzbuch mit Allgemeinem Gleichbehandlungsgesetz,
15. Auflage,
München, 2014

Kilian, Wolfgang
Heussen, Benno (Hrsg)
Computerrechts-Handbuch. Informationstechnologie in der Rechts- und Wirtschaftspraxis,
Stand: 32. Ergänzungslieferung,
München, 2013

Kreutzer, Ralf
Hinz, Jule
Working Paper Möglichkeiten und Grenzen von Social Media Marketing, Working Papers of the Institute of Management Berlin at the Berlin School of Economics and Law (HWR Berlin)
Nr. 58
Berlin 2010

Lackner, Karl (Hrsg.)
Strafgesetzbuch. Kommentar,
28. Auflage,
München, 2014

Lapp, Edgar
Linguistik der Ironie,
2. Auflage,
Tübingen, 1997

Lerch, Kent
Die Sprache des Rechts, Band 3: Recht vermitteln,
Berlin, 2005

Leupold, Andreas
Glossner, Silke (Hrsg.)
Münchener Anwaltshandbuch IT-Recht,
3. Auflage,
München, 2013

Marnau, Ninja
Schlehahn, Eva
TClouds, Cloud Computing – Legal Analysis,
Kiel, 2011

Maunz, Theodor
Dürig, Günter (Hrsg.)
Grundgesetz,
71. Ergänzungslieferung,
München, 2014

Müller-Broich, Jan — Telemediengesetz, Baden-Baden, 2012

Müller-Glöge, Rudi; Preis, Ulrich; Schmidt, Ingrid (Hrsg.) — Erfurter Kommentar zum Arbeitsrecht, 15. Auflage, München, 2015

Ohly, Ansgar; Sosnitza, Olaf (Hrsg.) — Gesetz gegen den unlauteren Wettbewerb mit Preisangabenverordnung, 6. Auflage, München, 2014

Palandt, Otto — Bürgerliches Gesetzbuch (BGB), 73. Auflage, München, 2014

Porter, Joshua — Designing for the Social Web, Berkeley, 2008

Rengeling, Hans-Werner; Middeke, Andreas; Gellermann, Martin (Hrsg.) — Handbuch des Rechtsschutzes in der Europäischen Union, 3. Auflage, München, 2014

Rogosch, Patricia Maria: — Die Einwilligung im Datenschutzrecht, Baden-Baden, 2013

Roßnagel, Alexander — Handbuch Datenschutzrecht, die neuen Grundlagen für Wirtschaft und Verwaltung, München, 2003

Säcker, Franz; Rixecker Roland (Hrsg.) — Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 5, 6. Auflage, München, 2013

Schaffland, Hans-Jürgen; Wiltfang, Noeme — Bundesdatenschutzgesetz, Loseblattsammlung, Stand Mai 2014, Berlin, 2014

Schönke, Adolf; Schroeder, Horst (Hrsg.) — Strafgesetzbuch. Kommentar, 29. Auflage, München, 2014

Simitis, Spiros (Hrsg.) Bundesdatenschutzgesetz,
8. Auflage,
Baden-Baden, 2014

Spindler, Gerald
Schmitz, Peter
Geis, Ivo Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz,
München, 2004

Spindler, Gerald
Schuster, Fabian (Hrsg.) Recht der elektronischen Medien,
3. Auflage,
München, 2015

Taeger, Jürgen
Gabel, Detlev Kommentar zum BDSG und Datenschutzvorschriften des TKG und TMG,
2. Auflage,
Frankfurt/M., 2013

Tamm, Marina
Tonner, Klaus Verbraucherrecht,
Baden-Baden, 2012

Thüsing, Gregor (Hrsg.) Beschäftigtendatenschutz und Compliance,
2. Auflage,
München, 2014

Tinnefeld, Marie Theres
Buchner, Benedikt
Petri, Thomas Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht,
4. Auflage,
Oldenburg, 2005

Unabhängiges Landes-zentrum für Datenschutz Schleswig-Holstein/GF Forschungsgruppe (Hrsg.) Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen,
Kiel/München, 2014

Wohlgemuth Hans
Gerloff, Jürgen Datenschutzrecht, Eine Einführung mit praktischen Fällen,
3. Auflage,
München, 2005

Wolff, Heinrich Amadeus
Brink, Stefan (Hrsg.) Beck'scher Online-Kommentar zum Datenschutzrecht,
1. Auflage,
München, 2012

Andere Publikationen

Alich, Stefan/Voigt, Paul	Mitteilsame Browser - Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints, CR 2012, S. 344
Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Orientierungshilfe – Cloud Computing, Düsseldorf, 2011
Bauer, Jobst-Hubertus *Günther, Jens*	Kündigung wegen beleidigender Äußerungen auf Facebook, Vertrauliche Kommunikation unter Freunden? NZA 2013, S. 67
Bäumler, Helmut	Das TDDSG aus der Sicht eines Datenschutzbeauftragten, DuD 1999, S.258
Becker, Florian	E-Volution des Rechts- und Verwaltungssystems, in: Hill/Schliesky (Hrsg.), Verfassungswandel durch staatliche Innovation, S. 57 Kiel 2010
Becker, Florian *Ambrock, Jens*	Datenschutz in den Polizeigesetzen, JA 2011, S. 651
Bock, Kirsten *Meissner, Sebastian*	Datenschutz-Schutzziele im Recht, Zum normativen Gehalt der Datenschutz-Schutzziele, DuD 2012, S. 425
Boehme-Neßler, Volker	Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, NVwZ 2014, S. 825
Breinlinger, Astrid *Scheuing, Sachik*	Der Vorschlag für eine EU-Datenschutzverordnung und die Folgen für Verarbeitung und Nutzung für werbliche Zwecke, RDV 2012, S. 64
Breyer, Patrick	Personenbezug von IP-Adressen, Internetnutzung und Datenschutz, ZD 2014, S. 400
Brummund, Fabian	Das Gesetz über den Rechtsschutz bei überlangen Gerichtsverfahren und strafrechtlichen Ermittlungsverfahren, JA 2012, S. 213
Bull, Hans-Peter	Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, NVwZ 2011, S. 257

Caspar, Johannes — Geoinformation und Datenschutz am Beispiel des Internetdienstes Google Street View, DÖV 2009, S. 965

Danckert, Burkhard
Mayer, Frank Joachim — Die vorherrschende Meinungsmacht von Google, Bedrohung durch einen Informationsmonopolisten? MMR 2010, S. 219

Drewes, Stefan
Siegert, Michael — Die konkludente Einwilligung in das Telefonmarketing und das Ende des Dogmas von der datenschutzrechtlichen Schriftform, RDV 2006, S. 139

Draheim, Yvonne
Lehmann, Philipp — Facebook & Co.: Aktuelle rechtliche Entwicklungen im Bereich Social Media – Marken- und Lauterkeitsrecht, GRUR-Prax 2014, S. 401

Eck von Eck, Klaus — „Mehr Vertrauen in Medizinprodukte durch verständliche und kontinuierliche Kommunikation" – MedTech-Kommunikationskonferenz des BVMed in Berlin, MPR 2013, S. 106

Erd, Reiner — Datenschutzrechtliche Probleme sozialer Netzwerke, NVwZ 2011, S. 19.

Ernst, Stefan — Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, S. 1917

Ernst, Stefan — Social Networks und Arbeitnehmer-Datenschutz, NJOZ 2011, S. 953

Federrath, Hannes
Pfitzmann, Andreas — Gliederung und Systematisierung von Schutzzielen in IT-Systemen, DuD 2000, S. 704

Forst, Gerrit — Bewerberauswahl über soziale Netzwerke im Internet? NZA 2010, S. 427

Gabriel, Ulrich
Cornels, Lars C. — Webtracking und Datenschutz - ein "hidden problem", MMR 11/2008, XIV

Gerhartinger, Hartmut — Google ändert Datenschutzbestimmungen, ZD-Aktuell 2012, S. 2780

Grentzenberg, Verena
Schreibauer, Marcus
Schuppert, Stefan
Die Datenschutznovelle (Teil II),
K&R 2009, S. 535

Hansen, Marit
Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter,
DuD 2012, S. 407

Heidrich, Joerg
Wegener, Christoph
Sichere Datenwolken, Cloud Computing und Datenschutz,
MMR 2010, S. 803

Hoeren, Thomas
Giurgiu, Andra
Der Datenschutz in Europa nach der neuen Datenschutz-Grundverordnung,
NWB 2012, S. 1599

Holtorf, Marc
Cloud Computing – Ein Überblick (Teil 2),
MPR 2013, S.196

Iraschko-Luscher, Stephanie
Kiekenbeck, Pia
Internetbewertungen von Dienstleistern - praktisch oder kritisch?
ZD 2012, S. 261

Jandt, Silke
Roßnagel, Alexander
Social Networks für Kinder und Jugendliche, Besteht ein ausreichender Datenschutz?
MMR 2011, S. 637

Kopp, Ferdinand
Das EG-Richtlinienvorhaben zum Datenschutz, Geänderter Vorschlag der EG-Kommission für "eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"
RDV 1993 (8), S. 1

Krasemann, Henry
Informelle E-Mail-Anfragen - Ein Fall für die Datenschutz-Mailabfuhr?
MMR 2004, XI

Krüger, Stefan
Maucher, Svenja-Ariane
Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis,
MMR 2011, S. 433

Kühling, Jürgen
Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz,
EuZW 2014, S. 527

Kühling, Jürgen
Gauß, Nicolas
Expansionslust von Google als Herausforderung für das Kartellrecht,
MMR 2007, S. 751

Kühling, Jürgen
Klar, Manuel
Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität,
NJW 2013, S. 3611

Masing, Johannes
Herausforderungen des Datenschutzes,
NJW 2012, S. 2305

Meltzian, Daniel
Die Neugestaltung des Listenprivilegs, Datenschutzrechtliche Vorschriften zum Umgang mit personenbezogenen Daten für Zwecke der Werbung,
DB 2009, S. 2643

Meyerdierks, Per
Personenbeziehbarkeit statischer IP-Adressen Datenschutzrechtliche Einordnung der Verarbeitung durch Betreiber von Webseiten,
MMR 2013, S.705

Moser-Knierim, Antonie
"Facebook-Login" - datenschutzkonformer Einsatz möglich?
ZD 2013, S. 263

Müller, Klaus
Das Geschäft für den, den es angeht,
JZ 1982, S.777

Nolte, Norbert
Zum Recht auf Vergessen im Internet, Von digitalen Radiergummis und anderen Instrumenten,
ZRP 2011, S. 236

Nussbaum, Caroline von
Krienke, Konstantin
Telefonwerbung gegenüber Verbrauchern nach dem Payback-Urteil,
MMR 2009, S. 372

Oberwetter, Christian
Bewerberprofilerstellung durch das Internet - Verstoß gegen das Datenschutzrecht?
BB 2008, S. 1562

Pfeifer, Markus
Neue Regeln für die Datennutzung zu Werbezwecken,
MMR 2010, S. 524

Pflüger, Almut
Datenschutz in der Markt- und Meinungsforschung,
RDV 2010, S. 101

Pießkalla, Michael
Zur Reichweite der Impressumspflicht in sozialen Netzwerken,
ZUM 2014, S. 368

Reinemann, Susanne
Remmertz, Frank
Urheberrechte an User-generated Content,
ZUM 2012, S. 216

Rolf, Christian
Rötting, Michael
Google, Facebook & Co als Bewerberdatenbank für Arbeitgeber?
RDV 2009, S. 263

Rost, Martin
Pfitzmann, Andreas
Datenschutz-Schutzziele – revisited,
DuD 2009. S. 353

Rost, Martin
Die Schutzziele des Datenschutzes, in Schmidt, Jan-Hinrik/Weichert, Thilo (Hrsg.), Datenschutz, S. 353ff.,
1. Auflage
Berlin, 2012

Roßnagel, Alexander
Datenschutz in globalen Netzen,
DuD 1999, S. 253

Das neue Recht elektronischer Signaturen zur Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO,
NJW 2001, S. 1817

Fahrzeugdaten – wer darf über sie entscheiden?
SVR 2014, S. 281

Sachs, Andreas
Meder, Miriam
Datenschutzrechtliche Anforderungen an App-Anbieter, Prüfungen am Beispiel von Android-Apps,
ZD 2013, S. 303

Schaar, Peter
Datenschutzrechtliche Einwilligung im Internet,
MMR 2001, S. 644

Schapper, Claus Henning
Dauer, Peter
Die Entwicklung der Datenschutzaufsicht im nicht-öffentlichen Bereich,(1),
RDV 1987, S. 169

Schäfer-Newiger, Ulrich
Die strikte Trennung von Direktmarketing und Marktforschung,
WRP 2001, S. 782

Schefzig, Jens
Big Data = Personal Data?, Der Personenbezug von Daten bei Big Data-Analysen,
K&R 2014, S. 772

Schlehahn, Eva
SurPRISE, Citizen Summits on Privacy, Security and Surveillance: Country report Germany,
Kiel, 2014
abrufbar unter: http://surprise-project.eu/wp-content/uploads/2014/10/D6.3_Country_report_Germany_final_30.9.pdf

Schweda, Sebastian — EU: Google Spain-Urteil beschäftigt Datenschützer im Rat und in der Art. 29-Datenschutzgruppe,
ZD-Aktuell 2014, 04371

Seidel, Martin — Die Direkt- oder Drittwirkung von Richtlinien des Gemeinschaftsrechts,
NJW 1985, S. 517

Solmecke, Christian
Wahlers, Jakob — Rechtliche Situation von Social Media Monitoring- Diensten. Rechtskonforme Lösungen nach dem Datenschutz- und dem Urheberrecht,
ZD 2012, S. 550

Steidle, Roland
Pordesch, Ulrich — Im Netz von Google. Web-Tracking und Datenschutz,
DuD 2008, S. 324

Tiedemann, Klaus — Datenübermittlung als Straftatbestand,
NJW 1981, S. 945

Tskhovrebov, Zelim — An Unfolding Case of a Genocide: Chechnya, World Order and the „Right to Be Left Alone",
NoJIL 64 (1995), S. 501

Venzke-Caprarese, Sven — Social Media Monitoring - Analyse und Profiling ohne klare Grenzen,
DuD 2013, S. 775

Vierhues, Wolfram — Art. 29-Datenschutzgruppe: Hilfestellung zum Cookie-Gebrauch,
ZD-Aktuell 2012, 02996

Voigt, Paul — Weltweiter Datenzugriff durch US-Behörden - Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten,
MMR 2014, S. 158

Voigt, Paul
Alich, Stefan — Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber,
NJW 2011, S. 3541

Wäßle, Florian
Heinemann, Oliver — Scoring im Spannungsfeld von Datenschutz und Informationsfreiheit, Rechtliche Rahmenbedingungen für den Einsatz von Scoringverfahren nach der Novellierung des Bundesdatenschutzgesetzes,
CR 2010, S. 410

Weichert, Thilo

Datenschutzrechtliche Probleme beim Adressenhandel,
WRP 1996, S. 522

Verbraucher-Scoring meets Datenschutz,
DuD 2006, S. 399

BDSG-Novelle zum Schutz von Internet-Inhaltsdaten,
DuD 2009, S. 7

Cloud Computing und Datenschutz,
DuD 2010, S. 679

Big Data und Datenschutz,
ZD 2013, S. 251

Datenschutz im Auto – Das Kfz als großes Smartphone auf Rädern,
SVR 2014, S. 241

Scoring in Zeiten von Big Data,
ZRP 2014, S. 168

Internet-TV und Datenschutz – ein Annäherungsversuch,
Kiel, 2014,
abrufbar unter https://www.datenschutzzentrum.de/vortraege/20140516-weichert-internet-tv.html

Wuermeling, Ulrich

Umsetzung der Europäischen Datenschutzrichtlinie,
DB 1996, S. 663

Zech, Herbert

Durchsetzung von Datenschutz mittels Wettbewerbsrecht?
WRP 2013, S. 1434

Zeidler, Simon-Alexander
Brüggemann, Sebastian

Die Zukunft personalisierter Werbung im Internet,
CR 2014, S. 248

Zscherpe, Kerstin

Anforderungen an die datenschutzrechtliche Einwilligung im Internet,
MMR 2004, S. 723