Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Orientierungshilfe „Soziale Netzwerke“

Stand:	*14.03.2013*
Version:	*1.1*
Redaktion:	*Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*

1 Einführung

1.1 Thematische Ausrichtung

Die vorliegende Orientierungshilfe reflektiert das gemeinsame Verständnis der Datenschutzbeauftragten und Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich über die Wahrung des Datenschutzes bei der Verwendung sozialer Medien, insbesondere sozialer Netzwerke, zur Erfüllung eigener Aufgaben oder Geschäftszwecke. Ziel ist es, neben der Konkretisierung der gesetzlichen Mindeststandards auch Best-Practice-Ansätze aufzuzeigen, soweit der gesetzliche Normierungsrahmen Lücken hinsichtlich eines ausreichenden Schutzes des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufweist. Die Darstellung zielt auf die datenschutzrechtliche Bewertung der verschiedenen „Schichten" sozialer Netzwerke. Diese Schichten setzen sich aus den Inhaltsdaten, Bestandsdaten und Nutzungsdaten zusammen. Die Bewertung basiert auf den bestehenden gesetzlichen Grundlagen, den einschlägigen Beschlüssen und Entschließungen der nationalen und internationalen Gremien, insbesondere der Artikel-29-Datenschutzgruppe.

Auf eine Trennung zwischen der Darstellung „technischer" und „rechtlicher" Anforderungen wird in der Orientierungshilfe bewusst verzichtet. Vielmehr wurden als Leitlinie die Schutzziele der Datensicherheit und des Datenschutzes, Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit, Transparenz und Nichtverkettbarkeit (Zweckbindung) herangezogen. In diesen Schutzzielen lassen sich sämtliche Anforderungen am besten vereinen.

1.2 Zielgruppen

Die Orientierungshilfe richtet sich an Betreiber sozialer Netzwerke. Sie richtet sich auch an Behörden und Unternehmen, die mit sozialen Netzwerken ihre Aufgaben erfüllen (wollen) oder ihre Geschäftszwecke verfolgen. Außerhalb des Fokus liegen die privaten Nutzer sozialer Netzwerke. Die Orientierungshilfe ist insofern keine Anleitung für den datenschutzgerechten Gebrauch solcher Netzwerke. Hinweise und Anleitungen für Nutzer[1] derartiger Dienste werden von verschiedenen Datenschutzbehörden und anderen Einrichtungen zur Verfügung gestellt.

1.3 Schutzziele

Diese Orientierungshilfe verwendet neben den „klassischen" Schutzzielen Vertraulichkeit (Kapitel 7), Verfügbarkeit (Kapitel 8) und Integrität (Kapitel 6) als Maßstab auch die modernen

[1] Mit der geschlechtsneutralen Form werden Frauen wie Männer gleichermaßen umfasst.

Datenschutzziele Nichtverkettbarkeit (Kapitel 4), Transparenz (Kapitel 5) und Intervenierbarkeit (Kapitel 9)[2].

Diese ergänzenden Ziele sind teilweise bereits in Datenschutzgesetzen oder anderen Normen explizit verankert (so z. B. in § 10 Abs. 2 Nr. 6 DSG NRW), lassen sich aber auch aus den anderen Regelungen ableiten, die die Aufrechterhaltung des technisch-organisatorischen Datenschutzes zum Inhalt haben.

1.4 Begriffsdefinitionen

Die in dieser Orientierungshilfe verwendeten Begriffe von zentraler Bedeutung werden im Folgenden erläutert.

Soziales Netzwerk: Gesamtheit aus technischer und organisatorischer Infrastruktur mit Soft- und Hardware, Betreiber(n) und Nutzern dieser Infrastruktur sowie der darin vorhandenen Daten.

Betreiber* oder *Anbieter: Eine Organisation, in der Regel juristische Person, die die wesentlichen organisatorischen und technischen Bestandteile eines sozialen Netzwerks bereitstellt und den Dienst damit ermöglicht und darüber den Umfang und die Bedingungen der Nutzung festlegt.

Mitglied: In Bezug auf ein bestimmtes soziales Netzwerk bei diesem registrierte Person[3].

Nutzer: Person, die Dienste eines sozialen Netzwerks nutzt, sei es als registriertes Mitglied oder als nicht-registrierter Externer.

Dritter: Jede andere natürliche oder juristische Person, die nicht Betreiber oder Nutzer in Bezug auf ein bestimmtes soziales Netzwerk ist.

1.5 Allgemeine datenschutzrechtliche Anforderungen

Die Datenschutzbeauftragten des Bundes und der Länder und die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben sich mittlerweile mehrfach in Form von Beschlüssen und Entschließungen zum Datenschutz in sozialen Netzwerken geäußert. Sie haben bei den Betreibern die Beachtung verschiedener Anforderungen angemahnt.

- Information
  Es müssen leicht zugängliche und verständliche Informationen darüber existieren, welche Daten für welche Zwecke erhoben und verarbeitet werden. Nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung (siehe 5.1).

[2] Siehe z. B. Rost/Pfitzmann „Datenschutz-Schutzziele – revisited“, in DuD 6/2009.
[3] Dies kann eine natürliche Person, d. h. ein privater Nutzer oder eine juristische Person als professioneller Nutzer sein.

- Standard-Einstellungen
  Sämtliche Voreinstellungen für die Verwendung personenbezogener Daten des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, entspricht nicht den gesetzlichen Vorgaben (siehe 5.2). Voreinstellungen sind so zu wählen, dass Risiken für die Privatsphäre der Nutzer minimiert werden und dem Prinzip der Erforderlichkeit Rechnung getragen wird.

- Betroffenenrechte
  Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können (siehe 9.3).

- Biometrische Daten
  Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig (siehe 2.2 und 10.2).

- Pseudonyme Nutzung und Löschverpflichtungen
  Das Telemediengesetz (TMG) schreibt die Eröffnung pseudonymer Nutzungsmöglichkeiten in sozialen Netzwerken vor, soweit dies technisch möglich und zumutbar ist. Nutzer müssen die Möglichkeit haben, in dem sozialen Netzwerk unter Pseudonym oder mehreren Pseudonymen zu handeln. Dies dient der Wahrung des informationellen Grundrecht bei der Nutzung des Internet. Das TMG enthält im Hinblick auf Nutzungsdaten – soweit keine Einwilligung vorliegt – ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen (siehe 4).

- Social Plug-ins
  Das direkte Einbinden von Social Plug-ins in Websites deutscher Anbieter ist unzulässig, wenn dadurch eine Datenübertragung an den jeweiligen Anbieter des Social Plug-ins ausgelöst wird, ohne dass die Internetnutzer hinreichend informiert werden und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden (siehe 5.1).

- Datensicherheit
  Die großen Mengen an teils sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben (siehe 2.5).

- Minderjährigenschutz
  Daten von Minderjährigen sind besonders zu schützen. Insofern kommt datenschutzfreundlichen Standardeinstellungen eine wichtige Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und für diese leicht verständlich und beherrschbar sein.

- Kontaktpersonen
  Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

2 Technische Grundlagen – Datensicherheit

Aus einem informationstechnischen Blickwinkel bestehen soziale Netzwerke typischerweise aus folgenden Komponenten:

- Client (Internet-Browser oder Smartphone-App),
- Übertragungsnetz (Internet),
- Server-Infrastruktur,
- Datenhaltungs-Infrastruktur (sog. Content Delivery Networks).

Diese Komponenten haben jeweils ihre eigenen Datensicherheitsanforderungen, die unterschiedliche Sicherheitsmaßnahmen erforderlich machen. Die Maßnahmen dienen der Datensicherheit und damit grundsätzlich dem Datenschutz (etwa die Verschlüsselung). Mitunter existieren auch widerstreitende Interessen, z.B. wenn durch Beobachtung des Nutzerverhaltens Angriffe auf das Netzwerk verhindert werden sollen und dabei zusätzliche, das Recht auf informationelle Selbstbestimmung gefährdende Datenverarbeitung stattfindet.

In diesem Kapitel werden verschiedene Aspekte der Technik sozialer Netzwerke beleuchtet und im Hinblick auf ihre Datensicherheitsanforderungen diskutiert. Die getroffene Auswahl ist nicht abschließend, sondern stellt eine Fokussierung auf diejenigen Bereiche dar, die in der Datenschutzdiskussion von besonderer und aktueller Bedeutung sind.

2.1 Datenhaltung

Betreiber (zentralisierter) sozialer Netzwerke verwalten typischerweise große Datenmengen[4]. Die zum performanten Betrieb solcher Datenmengen genutzten Techniken und Architekturen sind

[4] Die von großen Anbietern wie Facebook oder Google betriebenen Datenbanken gehören zu den größten der Welt. Facebook hatte Mitte 2010 ein Datenvolumen von 15 Petabytes (PB, dies sind

vergleichsweise neu und entwickeln sich noch immer rasch weiter. Die wichtigsten Anforderungen an diese Systeme sind:

- Die Systeme sollten über ausreichende Sicherheitsoptionen wie Zugriffschutz und Authentisierung verfügen, da die entsprechenden Anforderungen nicht von Beginn an in die Entwicklung der Systeme eingegangen sind.

- Die Daten sollten auf logische und räumlich einheitliche Speicherorte verteilt werden, um die Löschung und Beauskunftung von Nutzerdaten nicht zu erschweren.

- Das Löschen von Daten sollte nicht über das Entfernen der Indexeinträge, die zum Auffinden der eigentlichen Daten genutzt werden, erfolgen. Vielmehr sind die Daten tatsächlich zu löschen.

2.2 Biometrische Techniken

Biometrie stellt zunächst keine typische Technik sozialer Netzwerke dar, da biometrische Merkmale wie Fingerabdrücke oder Gesichtsgeometrien nicht erhoben werden.

Allerdings hat die biometrische Erkennung von Gesichtern auf den Fotos der Nutzer mittlerweile Einzug in verschiedene Netzwerke gehalten. Dies ist offenbar auch auf Fotos geringerer Qualität mit einigem Erfolg möglich, zumindest wenn sich die Erkennung nur auf die relativ überschaubare Menge der Freunde eines Nutzers beschränkt. In der Regel handelt es sich dabei um lernende Systeme, die eine anfängliche und fortlaufende „Mitarbeit“ derjenigen Nutzer erfordern, die Personen auf Fotos manuell markieren.

Der Umstand, dass hierbei – aus Sicht des Betreibers eines sozialen Netzwerkes – ohne aufwändige zusätzliche Erhebungen eine massentaugliche biometrische Datenbasis geschaffen wird, birgt datenschutzrechtliche Risiken. Details hierzu werden in Abschnitt 10.2 erörtert.

2.3 Tracking

Obwohl kein exklusives Thema sozialer Netzwerke, ist das Tracking von Nutzern ein wichtiges Element in der Gesamtfunktionalität vieler Netzwerke. Als Instrument zur Steuerung und Analyse von Werbeeinblendungen trägt das Tracking entscheidend dazu bei, die Einnahmen der unentgeltlich angebotenen Netzwerke zu sichern. Dabei haben soziale Netzwerke gegenüber anderen Angeboten im Internet einen entscheidenden Vorteil: Sie kennen ihre Nutzer[5]. Es ist

---

15.000.000 Gigabytes) bei einem Anstieg von 60 TB pro Tag; siehe Thusoo et al: „Data warehousing and analytics infrastructure at facebook“, in Proceedings of the 2010 international conference on Management of data, http://borthakur.com/ftp/sigmodwarehouse2010.pdf. Aktuell werden mehr als 100 PB angegeben, http://www.facebook.com/notes/facebook-engineering/under-the-hood-hadoop-distributed-filesystem-reliability-with-namenode-and-avata/10150888759153920.

[5] Jedenfalls soweit es sich um ihre Mitglieder handelt und die Anmeldung nicht unter Pseudonym erfolgt ist. Nichtmitglieder können Soziale Netzwerke zwar auch aufrufen, sind in ihren Möglichkeiten in der Regel aber sehr beschränkt.

ihnen daher immer möglich, die Aktivitäten nutzerspezifisch zu verfolgen. Der Nutzer kann sich dem nicht durch Browsereinstellungen o. Ä. entziehen, ohne seinen Anmeldestatus zu verlieren.

In technischer Hinsicht stehen sozialen Netzwerken die typischen Methoden für das Tracking zur Verfügung: Cookies, Flash-Cookies bzw. LSO (Local Shared Objects) oder HTML5 Client-Side Storage. Meist wird eine Kombination dieser Techniken eingesetzt (mehr zum Nutzertracking und zur Reichweitenanalyse in 10.4).

2.4 Werbung

Insbesondere für diejenigen sozialen Netzwerke, die ihre Mitgliedschaft kostenlos anbieten, bilden Werbeeinnahmen die bei weitem größte Einnahmequelle. Entsprechend wird auf die Möglichkeiten Wert gelegt, die Werbung möglichst zielgenau und damit erfolgversprechend und gewinnbringend platzieren zu können.

Den sozialen Netzwerken ist es oft möglich, sowohl die Angaben soziographischer Natur ihrer Nutzer (Alter, Geschlecht, Wohnort etc.) als auch deren aktuelle Aktivitäten bei der Werbeeinblendung zu berücksichtigen. Besonders interessant ist dies, wenn sich die Beobachtung der Nutzer über die Grenzen des eigenen Netzwerks hinaus auf das gesamte Web erstreckt. Dies ist mit Hilfe sog. Social Plug-ins möglich, die Webseitenanbieter in ihre Seiten integrieren.

Statt bzw. ergänzend zu der Finanzierung durch Werbung bestehen andere Möglichkeiten der Kostendeckung, etwa Nutzungsentgelte.

2.5 Technische und organisatorische Maßnahmen zur Datensicherheit

Soziale Netzwerke sind verpflichtet, Maßnahmen zur Gewährleistung der Datensicherheit zu ergreifen. Sie verwalten die persönlichen Daten, Beziehungen, Fotos, Meinungen, Interessen und Gewohnheiten von Millionen, nicht selten minderjährigen Menschen.

2.5.1 Verhinderung systematischer Massendownloads von Profildaten aus dem sozialen Netzwerk

Anbieter sozialer Netzwerke müssen sicherstellen, dass die Nutzer ihrer Angebote die Profildaten und Kommunikationsinhalte anderer Nutzer nicht ohne ausdrückliche Einwilligung der Betroffenen automatisiert von Dritten ausgelesen werden können.

Folgende Maßnahmen gegen den automatisierten und systematischen Abruf (z.B. durch crawler) von Profildaten und Kommunikationsinhalten sollten getroffen werden:

- Der Zugriff von Suchmaschinen oder anderen Indexierern auf die Profile der Nutzer sollte von diesen im Rahmen der Datenschutzeinstellungen festgelegt werden können und in den Standardeinstellungen deaktiviert sein.

- Betreiber von sozialen Netzwerken sollten Maßnahmen ergreifen, die eine Massenkopie von Daten aus dem Netzwerk verhindern. Zu solchen Maßnahmen zählen z. B. die Beobachtung von auffälligen Aktivitäten im Netzwerk (Unterscheidung zwischen manuellen und maschinellen Zugriffen) oder die externe Auditierung der eigenen Infrastruktur.

2.5.2 Angriffe auf den sozialen Graphen

Vereinfacht lassen sich soziale Netzwerke als Graphen betrachten, die Knoten (Nutzerprofile) und Kanten (Freundschaftsbeziehungen) verbinden. Ziel vieler Betreiber von Netzwerken ist es, diesen Graphen möglichst groß und engmaschig zu machen. Insbesondere soll er nicht in voneinander unabhängige Bereiche zerfallen. Diese aus Netzwerksicht wünschenswerte Eigenschaft macht soziale Netzwerke (und auch andere zusammenhängende Netzwerke) anfällig für sich von Knoten zu Knoten fortpflanzende Missbräuche.

Eine einmal gefundene Schwachstelle (z. B. zum Auslesen oder Verändern von Daten) kann ausgehend von einem Nutzer (z. B. dem Account eines Angreifers) rasch in dem gesamten Netzwerk ausgenutzt werden und damit die Infrastruktur in ihrer Gesamtheit gefährden. Einige aktuellere Beispiele hierfür sind Koobface[6], Ramnit[7] oder LilyJade[8]; das Problem reicht bis in die Anfangszeiten sozialer Netzwerke zurück (z. B. 2005 der Spacehero-Wurm auf MySpace[9]).

Betreiber sozialer Netzwerke müssen sämtliche nach dem Stand der Technik als erforderlich anzusehenden Maßnahmen ergreifen, damit solche Angriffe unterbunden werden oder zumindest so rechtzeitig erkannt werden, dass Gegenmaßnahmen getroffen werden können. Hierzu sollten u. a. folgende Vorkehrungen getroffen werden:

- Einführung von CAPTCHAs[10], um Programme (sog. Social Bots) zu behindern,

- Plausibilitätsprüfungen von Nutzeraccounts, um insbesondere automatisiert betriebene Accounts zu erkennen,

- Beobachtung der Aktivitäten im Netzwerk auf Auffälligkeiten (z. B. besonders hohe Zugriffszahlen) und entsprechende Gegenmaßnahmen (z. B. zeitliche oder zahlenmäßige Begrenzung abfragbarer oder herunterladbarer Profile),

---

[6] http://en.wikipedia.org/wiki/Koobface
[7] http://www.spiegel.de/netzwelt/web/zehntausende-opfer-mehrzweck-wurm-kapert-facebook-konten-a-807521.html
[8] http://www.securelist.com/en/blog/706/Worm_2_0_or_LilyJade_in_action
[9] http://namb.la/popular/
[10] Completely Automated Public Turing test to tell Computers and Humans Apart, siehe http://de.wikipedia.org/wiki/CAPTCHA.

- Meldungen anderer Nutzer.

Diese Vorkehrungen[11] können systematische Massendownloads von Profildaten erschweren, sind jedoch nicht lückenlos[12] und erfordern ein permanentes Nachsteuern. Datensicherheit ist als Prozess zu begreifen, der zyklisch immer wieder durchlaufen werden muss. Die Betreiber sozialer Netzwerke müssen die Nutzer über bestehende Restrisiken informieren.

3 Verantwortlichkeit

Nach Art. 2 d) der RL 95/46/EG (EG-Datenschutzrichtlinie[13]) ist für die Verarbeitung Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hiervon zu unterscheiden ist der Auftragsdatenverarbeiter im Sinne von Art. 2 e) der RL 95/46/EG als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Bei der Beurteilung wird auf die konkrete Funktion bei der Durchführung der Datenverarbeitung abgestellt. Die jeweilige Stelle kann für gewisse Datenverarbeitungen als verantwortliche Stelle, für andere Verarbeitungen auch als Auftragsdatenverarbeiter tätig werden. Je nach eingenommener Rolle können sich somit unterschiedliche Funktionen für Anbieter und Betreiber, aber auch die Nutzer eines sozialen Netzwerks ergeben.

3.1 Verantwortungsverteilung bei sozialen Netzwerken

3.1.1 Betreiber von sozialen Netzwerken

Betreiber von sozialen Netzwerken, die Online-Kommunikationsplattformen zur Nutzung bereitstellen, sind regelmäßig als verantwortliche Stelle nach Art. 2 d) der RL 95/46/EG bzw. § 3 Abs. 7 BDSG anzusehen.[14] Sie bestimmen über die Zwecke und Mittel der Datenverarbeitung. Die Fähigkeit, die Verarbeitungszwecke zu bestimmen, ist bereits feststellbar, wenn mit den im Rahmen der Nutzung der Dienste erhobenen Daten zum Beispiel Werbe- oder Marketingzwecke verfolgt werden. Hierbei werden Nutzungsdaten (z. B. IP-Adresse, Browsertyp, Cookies) und Inhaltsdaten (eingestellte Fotos, eingestellte Beiträge) verarbeitet. Eine entsprechende

[11] Z. B. Facebook Immune System, http://allfacebook.de/wp-content/uploads/2011/10/FacebookImmuneSystem.pdf, oder Everything you ever wanted to know about Facebook Security, http://www.scribd.com/doc/70451272/Facebook-Security-Infographic.
[12] Z. B. The Socialbot Network: When Bots Socialize for Fame and Money, http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1.
[13] 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 (ABl. EG Nr. L 281 S. 31).
[14] Art. 29-Datenschutzgruppe, WP 163 vom 12.07.2009, S. 6.

Zwecksetzung ergibt sich nicht selten aus den Allgemeinen Geschäftsbedingungen des Betreibers des sozialen Netzwerks. Die Entscheidung über die Mittel der Datenverarbeitung, d. h. die zum Einsatz kommende Soft- und Hardware, wie auch die Entscheidung über die Verarbeitung selbst, z. B. über die Speicherdauer, liegt im Regelfall ebenfalls bei den Betreibern von sozialen Netzwerken. Die Bezeichnung als „verantwortliche Stelle“ oder als „Auftragsdatenverarbeiter“ (auch in schriftlichen Vereinbarungen oder Verträgen) ist nicht maßgebend für die Bewertung. Es kommt auf die tatsächliche Aufgabenverteilung an, also welcher Stelle die jeweilige Funktion bzw. Rolle bei der Datenverarbeitung zukommt.

3.1.2 Professionelle Nutzer

Denkbar ist, dass mehrere verantwortliche Stellen gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Dies führt dazu, dass alle Stellen die Adressaten für die Einhaltung der Datenschutzvorschriften und insbesondere für die Erfüllung der Betroffenenrechte (Auskunft, Löschung, Sperrung, Berichtigung etc.) sind. Die Artikel-29-Datenschutzgruppe hat festgestellt, dass bezüglich der Akteure in einem sozialen Netzwerk sowohl die Konstellation denkbar ist, dass zwei oder mehrere Verantwortliche gemeinsam die vollständige Kontrolle über die Zwecke und Mittel ausüben, als auch der Fall, dass zwei oder mehrere Verantwortliche nur bezüglich eines Teils der Datenverarbeitung gemeinsam eine solche Kontrollfunktion besitzen.[15] Die Verfolgung gleicher Ziele und der Einsatz gleicher Mittel können auf verschiedene gemeinsam für die Datenverarbeitung Verantwortliche verteilt sein. Bei komplexen Verarbeitungsformen macht dies eine klare Zuweisung von Verantwortlichkeiten notwendig.[16] Unklarheiten dürfen sich nicht zu Lasten der Nutzer des sozialen Netzwerks auswirken. Diese müssen ihre Rechte auf Benachrichtigung, Löschung, Sperrung, Berichtigung und Widerspruch richtig adressieren können.

Webseitenbetreiber sind für die Datenverarbeitung Verantwortliche, wenn sie mittels Einbindung von Inhalten und von Diensten sozialer Netzwerkebetreiber (z. B. Social Plug-ins) zur Ausgestaltung ihres eigenen Dienstes die Datenverarbeitung der Anbieter des sozialen Netzwerks technisch ermöglichen.[17]

Die Verantwortlichkeit der Verwender der Dienste sozialer Netzwerke wird vor allem dann begründet, wenn diese zur Ausgestaltung ihres eigenen Angebotes die Dienste der Netzwerkanbieter nutzen und dabei eigene Geschäftszwecke verfolgen, z. B. durch die Inanspruchnahme von vom Betreiber zur Verfügung gestellten Statistiken. Derartige

---

[15] Art. 29-Datenschutzgruppe, WP 169 vom 16.02.2010, S. 26.
[16] Vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Wer ist datenschutzrechtlich verantwortlich für Facebook-Fanpages und Social-Plugins?, www.datenschutzzentrum.de/facebook/facebook-verantwortlichkeit.html.
[17] Ernst, Social Plugins: Der „Like-Button“ als datenschutzrechtliches Problem, NJOZ 2010, 1917, 1918.

Nutzungsstatistiken werden auf der Grundlage von personenbezogenen Nutzerdaten der Nutzer erstellt.

3.2 Nutzer als verantwortliche Stelle

Nutzer von sozialen Netzwerken sind im Regelfall als Betroffene im Sinne von Art. 2 a) der RL 95/46/EG, § 3 Abs. 1 BDSG und nicht als für die Datenverarbeitung Verantwortliche. Allerdings ist nicht ausgeschlossen, dass sie selbst über die Zwecke und Mittel der Datenverarbeitung entscheiden bzw. mitentscheiden. Im Zusammenhang mit dem Freunde-Finder-Verfahren sozialer Netzwerke wurde etwa angenommen, dass die Nutzer und der Betreiber des sozialen Netzwerks bewusst und gewollt zusammenwirken, indem die Nutzer die erforderlichen Adressdaten bereitstellen und der Netzwerkbetreiber die Erstellung von Einladungs-E-Mails und deren Versand übernimmt.[18]

Nutzer sind datenschutzrechtlich für die Verarbeitung personenbezogener Daten anderer Personen verantwortlich, wenn sie diese in ihren Nutzerprofilen oder auf den Plattformen in sozialen Netzwerken veröffentlichen. Nur wenn der Nutzer in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten tätig wird, kommen die Datenschutzvorschriften nicht zur Anwendung (vgl. Art. 3 Abs. 2 der EG-Datenschutzrichtlinie, § 1 Abs. 2 Nr. 3 BDSG).[19] Die Annahme einer ausschließlich persönlichen oder familiären Datenverarbeitung ist bei der Verwendung fremder personenbezogener Daten jedoch zumeist nicht gegeben; dies gilt insbesondere, wenn die personenbezogenen Informationen für jedermann sichtbar sind. Selbst wenn die Sichtbarkeit auf bestimmte Kreise bzw. Listen beschränkt ist, wird der persönliche und familiäre Bereich verlassen, wenn sich Netzwerkbetreiber eigene Nutzungs- und Verarbeitungsrechte an den eingestellten Informationen einräumen. Ausgeschlossen ist eine familiäre und persönliche Nutzung sozialer Netzwerke außerdem, wenn der Nutzer das Profil ganz oder teilweise zu beruflichen oder geschäftlichen Zwecken verwendet.

Von einer rein familiären und persönlichen Nutzung eines sozialen Netzwerkes kann ausgegangen werden, wenn die Zugriffsmöglichkeiten auf Informationen anderer Betroffener in dem Profil des jeweiligen Nutzers auf die von ihm selbst ausgewählte Kontakte beschränkt ist und eine Nutzung dieser Daten durch den Netzwerkbetreiber ausgeschlossen wird, d. h. die verwendeten Informationen ausschließlich zur privaten Kommunikation und Interaktion verwendet werden.

[18] LG Berlin, Urteil vom 06.03.2012, 16 O 551/10 (nicht rechtskräftig).
[19] Vgl. Art. 3 Abs. 2 der EG-Datenschutzrichtlinie, § 1 Abs. 2 Nr. 3 BDSG, sowie Art. 29-Datenschutzgruppe, WP 163 vom 12.07.2009, S. 6.

4 Rechtliche Grundlagen – Zulässigkeit

Die europäische und deutsche Rechtsordnung verpflichten Betreiber sozialer Netzwerke, beim Erheben, Verarbeiten und Nutzen personenbezogener Daten die datenschutzrechtlichen Vorgaben einzuhalten, Art. 7 RL 95/46/EG und § 4 Abs. 1 BDSG.

4.1 Anwendbares Recht

Für die Bestimmung, welche Rechtsordnung Anwendung findet, ist der Sitz des Dienstanbieters maßgeblich. Das für soziale Netzwerke einschlägige Telemedienrecht verweist zur Bestimmung des anzuwendenden Rechts auf die allgemeinen Regeln des BDSG, § 3 Abs. 3 Nr. 4 TMG. Anwendbar sind somit die Regelung des § 1 Abs. 5 BDSG bzw. zu dessen europarechtskonformen Auslegung Art. 4 RL 95/46/EG.

Danach ist die Anwendung deutschen Datenschutzrechts ausgeschlossen, wenn der Betreiber des Netzwerkes seinen Sitz in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat. In diesen Fällen kommt das jeweilige nationalstaatliche Recht des Sitzlandes zur Anwendung.

Deutsches Datenschutzrecht findet bei Betreibern sozialer Netzwerke Anwendung, die ihren Sitz **nicht** in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum innehaben und im Inland Daten erheben, verarbeiten oder nutzen. Dies ist der Fall, wenn der Betreiber zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind. Die Artikel-29-Datenschutzgruppe legt den Begriff „Mittel“ weit aus. Unter diesen Begriff fallen demnach auch Anlagen von Auftragsdatenverarbeitern[20], die im Auftrag der Betreiber Daten im Inland erheben oder verarbeiten. Ein Bezug zum Inland wird auch dann hergestellt, wenn Cookies oder Javascript auf den Endgeräten der Nutzer zur Durchführung der Datenverarbeitung durch den Betreiber gespeichert oder ausgeführt werden.[21]

Dieser stark technisch orientierte Ansatz wird durch einen normativen Ansatz ergänzt. Zweck der Regelung des Art. 4 RL 95/46/EG ist es, das datenschutzrechtliche Schutzniveau nicht dadurch zu gefährden, dass außereuropäische Anbieter in den Markt drängen, ohne sich den auf diesem Markt geltenden Regeln unterwerfen zu müssen. Zugleich sollen zu heterogene Regelungsanforderungen an die Betreiber vermieden werden.

Die stark auf die objektiven Merkmale abstellende Bestimmung der Erhebung, Verarbeitung und Nutzung von Daten im Inland, wird durch die Zweckbestimmung des Betreibers ergänzt. Unter

[20] A. A. VG Schleswig, Beschl. v. 14.02.2013; https://www.datenschutzzentrum.de/presse/20130215-verwaltungsgericht-facebook.htm.
[21] Art.-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht v. 16. Dezember 2010, WP 179 0836-02/10/DE, S. 25f.

das Datenschutzrecht des jeweiligen Ziellandes fallen Betreiber nur, wenn auch der Wille zur Datenverarbeitung von personenbezogenen Daten im jeweiligen Land zum Ausdruck kommt. Die durch das Internet hervorgerufene Vernetzung erlaubt aus technischer Sicht, jeden Dienst von jedem Ort der Welt aus abzurufen. Daher soll nationales Datenschutzrecht für Angebote gelten, die sich explizit oder implizit an die Betroffenen in dem jeweiligen Land richten. Indizien für eine derartige Ausrichtung des Angebotes könnten die Spracheinstellungen, Domainendungen oder die direkte inhaltliche Ansprache sein.

Deutsches Datenschutzrecht findet daher auf Betreiber mit Sitz im außereuropäischen Ausland Anwendung, die im Inland Daten erheben, verarbeiten und nutzen und deren Angebot sich an in Deutschland lebende Personen richtet.

Wenn der nichteuropäische Betreiber eine Niederlassung in einem Mitgliedstaat der Europäischen Union betreibt, findet das jeweilige Landesrecht des europäischen Sitzstaates Anwendung. Voraussetzung ist jedoch, dass es sich bei der Niederlassung um eine datenschutzrechtlich relevante Niederlassung handelt. Die Niederlassung muss für das jeweils in Frage stehende Verfahren die datenschutzrechtliche Verantwortung, d. h. die tatsächliche Entscheidungsbefugnis über Art und Umfang der Datenverarbeitung innehaben.

Öffentliche Stellen des Bundes und der Länder als Betreiber sozialer Netzwerke unterliegen den nationalen datenschutzrechtlichen Anforderungen aus dem BDSG bzw. den jeweiligen Landesdatenschutzgesetzen bzw. dem Bundesdatenschutzgesetz und dem Telemedienrecht. Die Anwendung des datenschutzrechtlichen Teils des Telemediengesetzes gilt gemäß § 11 Abs. 1 TMG nicht für soziale Netzwerke, soweit die Bereitstellung solcher Dienste im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von oder zwischen nicht-öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von internen Arbeits- oder Geschäftsprozessen erfolgt.

4.2 Gesetzliche Grundlagen im Bundesdatenschutz- und Telemediengesetz

Das deutsche Datenschutzrecht legt für Betreiber sozialer Netzwerke Anforderungen fest. Maßgelblich ist der Zweck der Erhebung und der Verarbeitung und die technische Natur des Datums. Somit kann ein „technisches Datum“ unterschiedlichen rechtlichen Regelungsregimen unterfallen. Der Name eines Betroffenen kann insoweit ein Bestands-, Nutzungs-, Abrechnungs- und Inhaltsdatum sein; dessen Verarbeitung kann im TMG oder im BDSG bzw. LDSG geregelt sein.

4.2.1 Inhaltsdaten

Zu den Inhaltsdaten zählen Informationen der Betroffenen, die Gegenstand der Leistungserbringung durch den Betreiber des sozialen Netzwerkes sind und den „Inhalt“ des

Dienstes ausmachen. Dazu gehören die Profilinformationen eines persönlichen Profils und die Inhalte der Kommunikation. Derartige Informationen unterfallen entweder bereichsspezifischen Gesetzen oder den allgemeinen Regeln des BDSG oder LDSG.

4.2.2 Bestandsdaten

Bestandsdaten unterliegen den Regeln des § 14 Abs. 1 TMG. Bestandsdaten sind Angaben, die für die Begründung, Durchführung und Beendigung eines Nutzungsverhältnisses notwendig sind. Welche konkreten Daten das sind, wird durch den jeweiligen Nutzungsvertrag bestimmt. Dazu zählen identifizierende Nutzerangaben (Name, Anschrift, E-Mail), Zugangsdaten (Nutzername, ID, Kennwort) oder weitere vertragsrelevante Informationen (Tarife, Nutzungszeiten etc.).

4.2.3 Nutzungsdaten

In den Anwendungsbereich des TMG fallen auch sämtliche Daten, die erforderlich sind, um die Inanspruchnahme des sozialen Netzwerkes zu ermöglichen und abzurechnen. Die Erhebung, Verarbeitung und Nutzung derartiger Nutzungsdaten ist in § 15 TMG umfassend geregelt. Zu den Nutzungsdaten zählen Merkmale zur Identifikation des Nutzers (IP-Adresse, Cookies, Nutzerkennung), Angaben über Beginn und Ende der Nutzung und Angaben über die in Anspruch genommenen Dienste. Soweit die Nutzungsdaten für die Abrechnung kostenpflichtiger Angebote des sozialen Netzwerkbetreibers verwendet werden, handelt es sich um Abrechnungsdaten, deren Verwendung durch § 15 Abs. 4 TMG geregelt wird.

4.3 Rechtsnatur der Mitgliedschaft in einem sozialen Netzwerk

Soziale Netzwerke sind ein relativ neues Phänomen der Entwicklung des Internets, deren rechtliche Einordnung, die entscheidend für die datenschutzrechtliche Bewertung ist, nicht einfach ist. Eine einheitliche, allgemein anerkannte Auffassung zu ihrer Rechtsnatur hat sich daher bislang noch nicht herausgebildet.

4.3.1 Vertragliche Ausgestaltung

Der Vorteil einer vertraglichen Ausgestaltung ist es für Betreiber sozialer Netzwerke, dass in Deutschland der Abschluss von Nutzungsverträgen grundsätzlich formfrei möglich ist. Es gilt der Grundsatz der Privatautonomie: Jeder kann mit jedem einen Vertrag über einen individuell gewünschten Inhalt abschließen. Dabei darf nicht außer Acht gelassen werden, dass über verbraucherschützende Vorschriften wie die §§ 305 ff. BGB zivilrechtlich eine Inhaltskontrolle möglich ist.

Datenschutzrechtlich gilt, dass Datenerhebungen und –verwendungen, die für den Vertragszweck erforderlich sind, grundsätzlich auf gesetzlicher Grundlage nach § 28 Abs. 1 S. 1 Nr. 1 BDSG bzw. § 14 Abs. 1 TMG zulässig sind. Ähnlich wie bei der Mitgliedschaft in einem

Verein sind jedoch Regelungen, die mit dem Hauptzweck der Mitgliedschaft nichts zu tun haben, aber von hoher datenschutzrechtlicher Relevanz sind, kritisch zu hinterfragen: Ebenso wenig wie ein Sportverein über eine Satzungsregelung, nach der die Mitgliederdaten an Sportartikelhersteller verkauft werden dürfen, diese Datenübermittlung legitimieren kann, kann sich ein Betreiber eines sozialen Netzwerks über seine Nutzungsrichtlinien ausbedingen, die Mitgliederdaten zu einem Zweck zu verwenden, der mit der vereinbarten Nutzung des sozialen Netzwerks unmittelbar nichts zu tun hat. Dies gilt z B. für die oben erwähnte Werbung, es sei denn, der Vertrag ist so deutlich ausgestaltet, dass der Nutzer sich darüber im Klaren ist, dass er auch einen Vertrag über die werbliche Nutzung seiner Daten schließt.

Wenn der Betreiber des sozialen Netzwerks die Nutzungsbedingungen ändert, braucht er jedenfalls bei wesentlichen Änderungen die Zustimmung des Nutzers; ansonsten gelten für diesen die alten Bedingungen fort. Ein kollektives Einverständnis der Nutzer in Form eines fehlenden Widerspruchs durch ein betreiberseitig definiertes Quorum genügt nicht. Anders als beim Verein, bei dem von Gesetzes wegen Satzungsänderungen nur unter der Beteiligung der Mitglieder möglich sind (vgl. § 33 BGB), werden die Nutzungsbedingungen bei sozialen Netzwerken einseitig durch den jeweiligen Betreiber gesetzt. Hieran ändern auch betreiberseitig initiierte Abstimmungen über geplante Änderungen nichts. Es handelt sich letztlich um eine Änderung des Nutzungsvertrags, mit der das einzelne Mitglied einverstanden sein muss.

Allerdings ist es im vertraglichen Bereich denkbar, dass das Mitglied seine Zustimmung durch konkludentes Handeln äußert. Dies kann sogar in einem Unterlassen bestehen, wie sich im Umkehrschluss aus § 308 Nr. 5 BGB ergibt. Voraussetzung ist, dass dies entsprechend vorher vertraglich vereinbart wird und dem Mitglied eine angemessene Frist zur Abgabe einer ausdrücklichen Erklärung eingeräumt wird sowie bei Fristbeginn ein Hinweis auf die vorgesehene Bedeutung seines Verhaltens erfolgt.

Liegt ein wirksamer Vertrag vor, muss der Betreiber eines sozialen Netzwerks im Rahmen seiner Informationspflichten nach § 13 Abs. 1 TMG und § 4 Abs. 3 S. 1 BDSG den Nutzer über die konkreten Datenflüsse unterrichten (sofern sich diese nicht bereits direkt aus der vertraglichen Regelung ergeben). Im Fall von pseudonymer Nutzerdatenanalyse ist der Nutzer ebenfalls darüber zu Unterrichten und auf sein Widerspruchsrecht hinzuweisen, § 15 Abs. 3 TMG.

4.3.2 Einholen einer datenschutzrechtlichen Einwilligung

Das Rechtsinstitut der Einwilligung kommt in denjenigen Konstellationen zum Tragen, in denen die beabsichtigte Datenerhebung und -verwendung nicht mehr von dem (vertraglich vereinbarten) Zweck des Nutzungsverhältnisses gedeckt ist. Dies ist insbesondere dann der Fall, wenn der Zweck in keinem Zusammenhang mit der Nutzung des sozialen Netzwerkes steht. Auch der Umgang mit personenbezogenen Daten zum Zweck der individualisierten Werbung bedarf der Einwilligung. Denn für die unmittelbare Inanspruchnahme des Dienstes ist die Datenverarbeitung zum Zweck der Werbung nicht erforderlich.

In diesen Fällen muss der Nutzer informiert einwilligen, d. h. er muss über Zweck und Umfang der Datenverarbeitung aufgeklärt werden und sein Einverständnis aktiv – beispielsweise durch das Setzen eines Häkchens – bekunden. Wichtig ist – parallel zu den Ausführungen zur vertraglichen Ausgestaltung – dass beim Nutzer ein entsprechender Rechtsbindungswillen vorhanden ist und auch nachgewiesen werden kann. Im Einzelnen sieht das Gesetz in § 13 Abs. 2 und 3 TMG vor, dass der Dienstanbieter bei einer elektronischen Einwilligung sicherstellen muss, dass

- der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann,
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann und
- er auf dieses Widerrufsrecht hingewiesen wird.

Die Einwilligung ist das Mittel der Wahl für Datenerhebungen und -verwendungen, die über den im Rahmen der Mitgliedschaft vereinbarten Vertragszweck hinausgehen.

Aufgrund der Gestaltungsmacht des Netzwerkbetreibers ist dieser in der Lage, den Umfang der geschuldeten vertraglichen Leistung zu bestimmen. Eine einseitige nachträgliche Erweiterung der Pflichten des Nutzers durch das Abverlangen einer Einwilligung unter der Bedingung, nur bei der Erteilung der Einwilligung das Nutzungsverhältnis fortzusetzen, stellt die Freiwilligkeit der Erteilung der Einwilligung in Frage. Soziale Netzwerke sind auf die Pflege der Kommunikationsbeziehungen, die Teil der menschlichen Identität sind, ausgerichtet. Wird die Fortnutzung des Dienstes von der Erteilung der Einwilligung abhängig gemacht, hat der Nutzer nur die Wahl seine Kommunikationsbeziehung abzubrechen oder den Eingriff in seine Persönlichkeitsrechte zu legitimieren. Auch die Nutzung von personenbezogenen Daten Betroffener, die nicht Nutzer des jeweiligen Netzwerkes sind bzw. nicht mit den Betreibern direkt in Kontakt stehen, ist in der Regel nur auf der Grundlage einer entsprechenden Einwilligung der Betroffenen möglich. Nicht auszuschließen sind Fälle, in denen Betreiber ein berechtigtes Interesse darlegen können, personenbezogene Daten zu verarbeiten und auch Personen, die nicht Nutzer des Netzwerkes sind, diesen Eingriff dulden müssen, z. B. Maßnahmen der Datensicherheit gegen Angriffe von außen. Eine derartige Befugnis ist jedoch im jeweiligen Einzelfall plausibel zu begründen und muss die Ausnahme bleiben. Den schutzwürdigen Interessen dieser Betroffenen, die womöglich eine bewusste Entscheidung getroffen haben, einen bestimmten Dienst nicht zu nutzen, sollte Rechnung getragen werden.

4.4 Zweckbindung und Nichtverkettbarkeit

Einige Datenschutzgesetze haben inzwischen die Nichtverkettbarkeit als Schutzziel bzw. als allgemeine Maßnahme zur Datensicherheit aufgenommen. Ziel der Nichtverkettbarkeit ist, dass personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können So fordern §§ 12 Abs. 2 TMG, 28 Abs. 1 S. 2 BDSG, Art. 6 Abs. 1 lit b) RL 95/46/EG, dass bei der Datenverarbeitung gewährleistet sein muss, dass personenbezogene Daten nur dann zu einem anderen Zweck verarbeitet und genutzt werden dürfen, soweit dafür eine gesetzliche Rechtfertigung existiert oder die Betroffenen in die Zweckänderung eingewilligt haben.

Im Rahmen von sozialen Netzwerken geht es somit zum einen um die Frage, welche Inhalts-, Nutzungs- und Bestandsdaten in das Profil eines Nutzers einfließen, aber auch, inwieweit unterschiedliche Profile innerhalb des Netzwerkes, aber auch mit Profilen oder weiteren Inhalts-, Nutzungs- und Bestandsdaten des Nutzers außerhalb des Netzwerkes durch den Anbieter oder Dritte, verbunden werden können. Im Sinne der informationellen Selbstbestimmung muss das Netzwerk dem Nutzer die Möglichkeit bieten, zu entscheiden, wer was wann über ihn weiß und dies auch jederzeit feststellen zu können. Die folgenden Grundsätze sollten zur Förderung der Kontrolle beachtet werden[22]:

- Den Nutzern sollten Möglichkeiten zur Verfügung stehen, mit denen sie Verkettungen bzw. Zweckänderungen ihrer Daten und deren Ausmaß erkennen können.
- Die Nutzer sollten in der Lage sein, die Verkettung ihrer Daten über ein geeignetes Identitätsmanagement zu kontrollieren. Dazu gehört auch die Möglichkeit, in dem sozialen Netzwerk unter verschiedenen Pseudonymen (z. B. zur Trennung beruflicher und privater Nutzung) zu agieren (vgl. dazu unten 4.5).
- Verkettungen müssen rückgängig gemacht werden können, indem z. B. Verknüpfungen von Profilen mit einer App oder einem Profil in einem anderen Netzwerk gelöscht werden können.
- Die Vertrauenswürdigkeit in die Verarbeitung sollte durch geeignete Nachweise gefördert werden (IT-Grundschutz, Audits, Zertifizierung).

4.5 Anonyme und pseudonyme Nutzung

Das TMG fordert in § 13 Abs. 6 von Betreibern sozialer Netzwerke, die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzende ist über diese Möglichkeit zu informieren. Den

[22] Vgl. Studie „Verkettung digitaler Identitäten“ ULD / TU Dresden, https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

Nutzenden muss jedenfalls ermöglicht werden, in dem Sozialen Netzwerk unter Pseudonym zu agieren. Eine Offenlegung der tatsächlichen Identität des Nutzers gegenüber dem Betreiber des Sozialen Netzwerks kann dagegen zur Erschwerung von Missbrauch insbesondere dann hingenommen werden, wenn die Nutzer das Netzwerk nicht nur passiv (Herunterladen von Informationen), sondern auch aktiv (Einstellen von Informationen) nutzen können. Betreiber sozialer Netzwerke für Privatnutzung sollten die Nutzung von Pseudonymen aktiv fördern.

Bei Netzwerken, die im beruflichen Kontext genutzt werden, ist es in der dortigen Zielgruppe zwar eher unüblich, anonym bzw. unter Pseudonym aufzutreten. Trotzdem gilt die Verpflichtung aus § 13 Abs. 6 TMG zur Eröffnung einer optionalen Möglichkeit, in dem Netzwerk unter Pseudonym zu handeln, auch für solche Netzwerke. Bei entsprechenden Vorgaben zur Gestaltung der Pseudonyme muss die Qualität des Netzwerkes nicht leiden, so dass eine Unzumutbarkeit für den Anbieter nicht anzunehmen ist.

4.6 Zweckbindung

Zentrale Intention der Nichtverkettbarkeit ist die Sicherung der Zweckbindung. Das bedeutet, dass personenbezogene Daten nur für den Zweck verarbeitet werden dürfen, den die gesetzliche Vorgabe erlaubt bzw. der im Rahmen der Einwilligung durch den Betreiber des sozialen Netzwerkes vorgegeben worden ist. Nach § 13 Abs. 1 TMG hat der Dienstanbieter den Nutzer vor der Erhebung über den Zweck zu informieren. Soll der Zweck geändert werden, so ist dies nur möglich, wenn entweder hierfür eine gesetzliche Grundlage besteht oder die Einwilligung beim Betroffenen eingeholt wird (vgl. auch § 12 Abs. 2 TMG). Der Zweck muss im Rahmen der Einwilligung so umrissen werden, dass es dem Betroffenen möglich ist einzuschätzen, welche Verkettungsmöglichkeiten sich hieraus ergeben. Pauschale Zweckbestimmungen wie „zur Erbringung des Dienstes“ sind nicht ausreichend.

4.7 Trennungsprinzip

Um die Nichtverkettbarkeit auch technisch zu unterstützen, gilt im Datenschutzrecht das Trennungsprinzip. Nach § 13 Abs. 4 Nr. 4 TMG hat der Dienstanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können. Außerdem muss sichergestellt sein, dass Nutzungsprofile i. S. d. § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können (§ 13 Abs. 4 Nr. 5 TMG). Für soziale Netzwerke bedeutet das, dass Nutzungsprofile, die zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des sozialen Netzwerks erstellt werden, getrennt von den Nutzerprofilen verarbeitet werden müssen, die aus den Inhaltsdaten eines Nutzers bestehen. Für Nutzungsprofile sind Pseudonyme zu verwenden. Fallen noch bei weiteren Telemedien (z. B. Chat-Dienste, Spiele etc.) personenbezogene Daten

an, so sind auch diese Daten und Profilinformationen von den übrigen Daten so weit wie möglich zu trennen.

5 Transparenz und Kontrolle

5.1 Transparenz

Nach §13 Abs. 1 TMG hat der Dienstanbieter die Nutzer vor der Datenverarbeitung über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der RL 95/46/EG in allgemein verständlicher Form zu unterrichten. Nach § 4 Absatz 3 BDSG sind den Betroffenen von der verantwortlichen Stelle deren Identität, der Zweck der Datenverarbeitung und die Kategorien von Empfängern mitzuteilen. Letzteres gilt jedoch nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

Diese Anforderungen gelten sowohl für die Erhebung von Nutzungs- und Bestandsdaten nach dem TMG als auch für Inhaltsdaten nach dem BDSG. Die Einwilligung nach § 13 TMG bzw. § 4a BDSG ist nur wirksam, solange sie in Kenntnis des vorgesehenen Zwecks der Erhebung, Verarbeitung oder Nutzung erteilt wurde.

Neben der Information über Art, Umfang und Zwecke der Erhebung und Verwendung sind Nutzer über ihre Rechte zu informieren, z. B. über das Recht, der Einwilligung zur Verarbeitung zu widersprechen (§ 13 Abs. 3 TMG) und über die Möglichkeit, das Angebot anonym oder pseudonym zu nutzen (§ 13 Abs. 6 TMG). Zusätzlich muss der Betreiber des sozialen Netzwerks kommerzielle Inhalte sowie die dahinterstehende natürliche oder juristische Person klar als solche kennzeichnen (§ 6 TMG).

Informationen und Nutzungsbedingungen, die Rechte und Pflichten der Nutzer und des Betreibers des sozialen Netzwerks regeln, müssen in einer verständlichen und übersichtlichen, deutschsprachigen, barrierefreien Erklärung, die im gesamten Angebot leicht zugänglich ist, bereitgestellt werden (Datenschutzerklärung und Nutzungsbestimmungen). Die Informationen müssen umfassend sein, also z. B. auch Informationen zu personenbezogenen Daten enthalten, die mit Hilfe von Cookies erhoben werden. Die Verwendung der Daten ist strukturiert und klar anzugeben, insbesondere die Weitergabe und der Zugriff durch berechtigte Dritte ist eindeutig festzulegen. Die Informationen sind stets zu aktualisieren, insbesondere bei neuen und geänderten Funktionen, und allen Nutzern vor der Einführung zur bestätigenden Kenntnis zu geben.

Nutzer sollten über mögliche Konsequenzen ihres Handelns auch während der Nutzung des Dienstes (z. B. bei der Veränderung von Datenschutz-Einstellungen einer Bildersammlung) informiert werden, z. B. durch eingebaute, kontext-sensitive Funktionen, die angemessene Informationen auf der Basis der jeweiligen Handlungen der Nutzer liefern.

Die Information der Nutzer sollte sich auch auf den Umgang mit Daten von Personen, die nicht Nutzer des Netzwerkes sind, beziehen: Betreiber sozialer Netzwerke sollten auch über Ge- und Verbote im Hinblick darauf informieren, wie die Nutzer diese Daten behandeln dürfen, die in ihren Profilen enthalten sind (z. B. wann die Einwilligung eines Betroffenen vor der Veröffentlichung eingeholt werden muss oder über mögliche Konsequenzen von Regelverstößen). Insbesondere spielen Fotos in Nutzerprofilen, auf denen Personen abgebildet sind, die bei dem Netzwerk nicht angemeldet sind oder von der Veröffentlichung keine Kenntnis haben (in vielen Fällen sogar versehen mit Hinweisen auf den Namen und/oder das Nutzerprofil), in diesem Kontext eine Rolle. Die derzeit weit verbreiteten Praktiken stehen in vielen Fällen nicht in Einklang mit den bestehenden Regelungen des Schutzes des Rechts am eigenen Bild gemäß dem Kunsturhebergesetz.

Die verantwortliche Stelle ist mit einfach zugänglicher Kontaktmöglichkeit anzugeben; bei ausländischen Anbietern sollte auch eine Kontaktmöglichkeit in dem Land, auf dessen Markt das Angebot ausgerichtet ist, angegeben sein. Ferner ist zu empfehlen, die Nutzer über den Regulierungsrahmen zu informieren, dem der Betreiber des sozialen Netzwerks unterliegt. Für den Fall der Insolvenz oder des Verkaufs sind Nutzer darüber zu informieren, wie mit ihren personenbezogenen Daten umgegangen wird.

Gibt es verschiedene Nutzergruppen, sind sowohl die Datenschutzbestimmungen als auch die Nutzungsbedingungen nach Nutzergruppen zu untergliedern, sodass – falls Regelungen nur bestimmte Nutzergruppen betreffen sollten – jeder Nutzer eindeutig erkennen kann, welche Bestimmungen für ihn gelten. Dies kann der Fall sein, wenn das soziale Netzwerk neben den Nutzern mit persönlichem Profil z. B. auch professionelle Nutzer oder Drittanbieter und Entwickler im Netzwerk zulässt.

Insbesondere über den Zugriff und die Verarbeitung durch Dritte (z. B. Anbieter von Anwendungen innerhalb des Netzwerks, Kooperations- und Werbepartner oder auch Sicherheitsbehörden) sind die Nutzer zu informieren. Dies gilt auch, wenn z. B. für die Anzeige von Werbeeinblendungen in dem Browser-Fenster eines Nutzers die IP-Adresse dieses Nutzers an einen anderen Dienstanbieter weitergegeben wird, der den Inhalt der Werbung liefert.

Bietet das soziale Netzwerk Schnittstellen für Drittanbieter an, sind der Umfang und die Weiterverwendung der Daten genau zu definieren und zu benennen.

Informationen sollten auch über verbleibende Sicherheitsrisiken gegeben werden und über andere mögliche Konsequenzen der Veröffentlichung personenbezogener Daten in einem Profil, wie auch über mögliche Zugriffe durch Dritte (einschließlich Strafverfolgungsbehörden und Geheimdiensten).

5.2 Kontrolle durch den Nutzer

Das Recht auf informationelle Selbstbestimmung setzt Kontrollbefugnisse für den Nutzer voraus. Der Anspruch, selbst zu bestimmen, wer wann was über die eigene Person weiß, soll dem Nutzer sowohl gegenüber dem Betreiber des sozialen Netzwerks als auch gegenüber anderen Nutzern und Drittanbietern eingeräumt werden. Dies schließt nicht nur die selbstgenerierten Daten (z. B. Informationen über die eigene Person), sondern auch fremdgenerierte Daten (z. B. Markierungen auf Fotos durch Dritte) mit ein. Die Kennzeichnung von Fotos (d. h. das Hinzufügen von Links auf existierende Nutzerprofile oder des Namens der abgebildeten Person/en) sollte an die vorherige Einwilligung der Betroffenen gebunden sein.

Die Konfigurations- und Einstellungsmöglichkeiten sollten also zulassen, dass Informationen gruppen- oder personenbezogen sichtbar sind. Eine Weitergabe an Dritte (Nutzer des Netzwerks, Entwickler, Werbepartner) ohne explizite Einwilligung des Betroffenen ist unzulässig. Verständliche und übersichtliche Hilfestellungen zu den Einstellungsmöglichkeiten inklusive klarer Angaben über die möglichen Auswirkungen, ggf. ergänzt durch FAQs, sowie die höchstmögliche Schutzeinstellung zum Zeitpunkt der Registrierung (datenschutzfreundliche Standardeinstellungen, die der Nutzer auf eigenen Wunsch verändern kann) erlauben dem Nutzer, selbstbestimmt mit seinen Informationen umzugehen. Informationen, die auf Grund schwacher Schutzeinstellungen (möglicherweise sogar ohne das Wissen der Nutzer) offen für Dritte innerhalb und außerhalb des Netzwerks abrufbar sind und ggf. durch Suchmaschinen erfasst werden, unterliegen nicht mehr der Kontrolle der Nutzer und widersprechen dem Grundsatz der informationellen Selbstbestimmung. Die Kontrolle des Nutzers über die eigenen Daten muss auch gewährleistet werden, wenn er diese bewusst an Dritte weitergibt. Eine Weitergabe der Daten durch diese Dritten ohne Einwilligung des Betroffenen ist grundsätzlich nicht zulässig.

Werden Daten durch den Nutzer gelöscht, sollten Anbieter sicherstellen, dass die Löschung auch für etwaige Kopien, die Dritten zur Verfügung gestellt wurden umgesetzt wird, es sei denn, der Nutzer hat in die weitere Nutzung eingewilligt.

Um kontrollieren zu können, welche Daten der Betreiber über die betroffene Person gespeichert hat, muss die Umsetzung des Auskunftsanspruchs nach § 34 Abs. 1 BDSG durch den Betreiber des sozialen Netzwerks gesichert sein. Dies kann über ein Online-Abrufverfahren erfolgen, muss aber alle vom Betreiber gespeicherten Daten (Inhalts-, Bestands- und Nutzungsdaten) beinhalten. Es bedarf in diesem Fall eines bestmöglichen Schutzes vor Missbrauch.

Bei international ausgerichteten Netzwerken ist darauf zu achten, dass die Nutzerkontrolle nicht durch Sprachbarrieren gefährdet ist.

5.3 Interne Kontrolle

Die Einhaltung der Datenschutzbestimmungen muss in internen Datenschutzrichtlinien und Konzepten festgelegt sowie ggf. durch einen internen Datenschutzbeauftragten kontrolliert werden.[23] Hierbei muss sichergestellt sein, dass dieser in seiner Funktion weisungsfrei, der Unternehmensleitung direkt unterstellt, ausreichend geschult und qualifiziert ist. Dieser muss hinreichend unterstützt und rechtzeitig über datenschutzrelevante Änderungen informiert werden. Neue oder geänderte Funktionen sind in der Regel durch eine Vorabkontrolle auf Datenschutzverstöße zu kontrollieren (insbesondere bei Risiken für die Rechte und Freiheiten der Betroffenen wie z. B. bei der Verarbeitung besonderer Datenkategorien wie politische Meinung, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben).[24]

Datenschutzkonzepte (inklusive Rechte- und Rollenkonzepte) und technische Dokumentationen sind vor dem Produktivbetrieb zu erstellen und legen – neben der Dokumentation der Systeme und ihrer Funktionen – insbesondere den Umgang und die Verwendung (Zweckbindung) der zu verarbeitenden Daten, den Schutzbedarf der Daten sowie die technischen und organisatorischen Maßnahmen fest, die vom Betreiber des sozialen Netzwerks zu ergreifen sind. Die Datenschutzkonzepte sind zu aktualisieren, sobald Änderungen oder Neuerungen entwickelt werden.

Technische und organisatorische Maßnahmen sind insbesondere zu ergreifen, um zu gewährleisten, dass die Vertraulichkeit und Integrität der Daten gesichert ist. Die Verknüpfung verschiedener Daten bzw. die Zweckentfremdung der Daten ist zu verhindern. Hierfür ist eine revisionssichere Protokollierung zu installieren, die die Zugriffe auf die Anwendung und auf das System protokolliert („wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?“ und „wer hatte von wann bis wann welche Zugriffsrechte?“). Zusätzlich kontrolliert ein Monitoring die Verfügbarkeit der Systeme und informiert rechtzeitig über Unregelmäßigkeiten. Die Informationen der Systeme sind über festgelegte Mitarbeiter bei Bedarf auszuwerten und ggf. in geeignete Maßnahmen zu überführen.

5.4 Externe Kontrolle

Die externe Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen obliegt den Aufsichtsbehörden für den Datenschutz, die entsprechend der gesetzlichen Vorgaben deutsches Datenschutzrecht (vgl. 4.1) oder das Datenschutzrecht des jeweiligen Sitzstaates anzuwenden haben. Die Zuständigkeit der deutschen Aufsichtsbehörden ergibt sich aus § 38 Abs. 1 S. 1 BDSG.

[23] Vgl. § 4f BDSG.
[24] Vgl. § 4d Abs. 5 BDSG.

Die sachliche Zuständigkeit der Aufsichtsbehörde ergibt sich aus dem jeweiligen Landesdatenschutzgesetz bzw. dem Bundesdatenschutzgesetz. Die örtliche Zuständigkeit knüpft an den (deutschen) Sitz der verantwortlichen Stelle an.

Um die ergriffenen technisch-organisatorischen Maßnahmen zu verbessern, können verantwortliche Stellen ihre Verfahren und Anwendungen auch durch einen unabhängigen Auditor prüfen und bewerten lassen.

6 Integrität und Authentizität

Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[25] Dieses Recht schließt die Gewährleistung der Unversehrtheit und der korrekten Funktionsweise von Systemen mit ein. Die Integrität der Daten ist gegeben, wenn die Daten vollständig und unverändert sind.[26]

Nutzer müssen sich also darauf verlassen können, dass die Informationen – ihre eigenen, aber auch die der anderen Nutzer – vollständig und richtig, d. h. nicht durch Dritte verändert, sind, es sei denn, dies ist eindeutig erkennbar. Nach der Anlage zu § 9 Satz 1 BDSG ist durch technische und organisatorische Maßnahmen sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht verändert werden können. Zusätzlich muss durch die verantwortliche Stelle sichergestellt sein, dass die Systeme und Anwendungen korrekt funktionieren. Werden Sicherheitslücken oder bereits eingetretene Schadensfälle entdeckt, sind sofort Gegenmaßnahmen zu ergreifen und betroffene Nutzer umgehend darüber und über die ergriffenen Maßnahmen zu informieren. Der Umfang an personenbezogenen Daten in sozialen Netzwerken und deren teilweise hoher Schutzbedarf erfordern hohe Standards bei der IT-Sicherheit, um die Daten vor Missbrauch wie z. B. Identitätsdiebstahl zu schützen.

Eng verbunden mit dem Begriff der Integrität ist die Authentizität der Nutzer sowie der technischen Systeme. Personen oder Organisationen, die in die eigene Kontaktliste aufgenommen werden, haben oft einen weiter reichenden Zugriff auf die persönlichen Informationen. Ein Nutzer muss also erkennen können, wer hinter dem Profil steht. Private Nutzer haben das Recht, Telemedien anonym oder pseudonym zu nutzen, jedoch muss das Vortäuschen einer falschen Identität (Identitätsdiebstahl) ausgeschlossen werden. Hierfür muss die verantwortliche Stelle Maßnahmen ergreifen, um so gut wie möglich sicherzustellen, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Dies beinhaltet einerseits

[25] 1 BvR 370/07, 1 BvR 595/07
http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.
[26] https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

Sicherheitsmaßnahmen, um den Zugriff auf die Konten der Nutzer zu schützen (z. B. Zugriff nur über gesicherte Verbindungen, Passwortmindestanforderungen), aber auch Überwachungssysteme, um z. B. Missbrauch durch virtuelle Profile (sog. Social bots[27]) schnell zu erkennen und zu verhindern.

Lässt ein soziales Netzwerk zu, dass Organisationen, öffentliche Stellen oder Unternehmen Seiten im Netzwerk betreiben, sollte dies nur vertretungsberechtigten Personen erlaubt sein. Gibt ein Nutzer vor, im Namen von Organisationen, öffentlichen Stellen oder Unternehmen zu handeln, kann so das Vertrauen der Nutzer erschlichen werden, die der Organisation, der öffentlichen Stelle oder dem Unternehmen ggf. weiter reichenden Zugriff auf Informationen geben.

7 Vertraulichkeit

Soziale Netzwerke werden zu unterschiedlichen Zwecken von öffentlichen Stellen, insbesondere von Sicherheitsbehörden, genutzt. Informationen aus sozialen Netzwerken können für öffentliche Stellen etwa erforderlich sein, um Straftaten aufzuklären oder um Gefahren für die öffentliche Sicherheit zu erkennen und abzuwehren. Inwieweit ein Zugriff auf die Daten in sozialen Netzwerken zulässig ist, müssen die öffentlichen Stellen nach den für sie geltenden Rechtsvorschriften in eigener Verantwortung bewerten.

Betreiber sozialer Netzwerke sind nach deutschem Recht z. B. verpflichtet, beschlagnahmte Unterlagen nach § 98 StPO an Strafverfolgungsbehörden herauszugeben oder, soweit sie Telekommunikationsdienste anbieten, nach § 100g StPO Auskunft über Verkehrsdaten zu erteilen.

Behörden erlangen Informationen nicht nur über Auskunftsersuchen an die Betreiber, sondern häufig durch eigene Recherchen in sozialen Netzwerken.

Es bestehen erhebliche datenschutzrechtliche Bedenken gegen eine Anwendung der Ermittlungsgeneralklauseln als Rechtsgrundlage für verdeckte Recherchen in nicht öffentlich zugänglichen Bereichen sozialer Netzwerke.

8 Verfügbarkeit

Die verantwortliche Stelle hat sicherzustellen, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Dies bedeutet für Betreiber sozialer Netzwerke zunächst, dass die Daten gegen zufällige oder absichtliche Zerstörung und Verlust durch das Ergreifen von technischen und organisatorischen Maßnahmen geschützt

[27] http://www.heise.de/security/meldung/Studie-Viele-Facebook-Nutzer-sind-sorglos-1370431.html

werden müssen.[28] Weiter muss sichergestellt sein, dass Nutzer nicht nur jederzeit auf ihre personenbezogenen Daten zugreifen können, sondern auch die Verfügungsgewalt hierüber haben. Eine dritte Ebene betrifft die öffentliche Verfügbarkeit der Daten.

Zur Sicherstellung der technischen Verfügbarkeit muss die Infrastruktur durch den Betreiber so abgesichert sein, dass z. B. externe Einflüsse wie Feuer oder Wasser bestmöglich abgewehrt werden können, eine dauerhafte Stromversorgung gewährleistet ist und die Daten durch Backup-Konzepte vor Verlust geschützt sind.

Die Verfügbarkeit der Daten für Nutzer beinhaltet zunächst den Zugriff auf ihre personenbezogenen Daten in dem sozialen Netzwerk. Dies steht in direktem Zusammenhang mit der o. g. technischen Verfügbarkeit sowie mit den Zugriffsrechten auf die eigenen Daten. Inhaltsdaten müssen unter der direkten Kontrolle der Nutzer stehen, d. h. die Daten sind zur Bearbeitung und Löschung durch den Nutzer selbst verfügbar zu halten. Kündigt ein Nutzer sein Konto in dem sozialen Netzwerk, sollte die Möglichkeit bestehen, die dort gespeicherten (Inhalts-) Daten vor der Löschung zu exportieren (diese Möglichkeit kann auch ohne das Löschbegehren zu jedem Zeitpunkt zur Verfügung gestellt werden). Dies schließt neben Texten auch die Fotos und weitere Medien ein. Die exportierten Daten sollten in gängigen, wiederverwendbaren Formaten zur Verfügung gestellt werden.[29]

Die öffentliche Verfügbarkeit von Profilen, d. h. die Sichtbarkeit von personenbezogenen Daten wie Profilname, Foto oder Geschlecht, erleichtert zwar das Auffinden der Person in dem sozialen Netzwerk, darf aber nicht außerhalb der Verfügungsgewalt der betroffenen Person stehen. Öffentlich zugängliche Daten – sowohl innerhalb des Netzwerks für registrierte Nutzer als auch außerhalb des Netzwerks, z. B. durch die Indexierung durch Suchmaschinen – erhöhen das Risiko eines Identitätsdiebstahls, so dass Nutzer zur Ausübung ihres Rechts auf informationelle Selbstbestimmung die Möglichkeit haben müssen, die Verfügbarkeit ihrer Daten gegenüber Dritten einzuschränken. Dabei ist angezeigt, dass die jeweils datenschutzfreundlichste Variante bereits seitens des Anbieters voreingestellt ist.

[28] Vgl. BDSG, Anlage zu § 9 Satz 1: Es sind „(…) sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, (…) zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)."

[29] Geeignet wären etwa PDF oder XML.

9 Intervenierbarkeit (Betroffenenrechte)

9.1 Änderungen des Funktionsumfangs sozialer Netzwerke

Soziale Netzwerke sind komplexe Gebilde, welche einer stetigen Änderung unterworfen sind. Durch die Einführung neuer Funktionen können – möglicherweise unbeabsichtigt – Änderungen erfolgen, die sich enorm auf die Rechtevergabe auswirken.

Die Einhaltung der Prinzipien „Privacy by Design“ und davon abgeleitet „Privacy by Default“ wird daher von Daten- wie auch Verbraucherschützern beständig gefordert. „Privacy by Design“ setzt eine auf Datenschutzbelange Rücksicht nehmende Entwicklung von Produkten voraus. „Privacy by Default“ bedeutet in der Anwendung auf soziale Netzwerke, dass neue Nutzer beim Beitritt und bestehende Nutzer bei der Einführung neuer Funktionen eine selbstbestimmte Entscheidung treffen können, für wen welche Daten sichtbar oder gesperrt sind. Dies sollte zunächst nur der Nutzer selbst sein, welcher dann schrittweise sein Profil für weitere Personen oder Gruppen öffnen kann. Die dabei geltenden Regeln und Abläufe müssen transparent sein und sollten auf evtl. unbeabsichtigte Änderungen verständlich hinweisen. Die Nutzergruppen, welche Zugriff auf die Daten des Netzwerkes haben können, müssen klar benannt werden (z. B. Freunde, Freunde von Freunden, Nicht-Mitglieder, Suchmaschinen), um dem Nutzer einfache Entscheidungen zu ermöglichen. Werden die Nutzungsregeln für ein soziales Netzwerk geändert, muss dies transparent erfolgen und muss mit einer angemessenen Übergangsfrist bekanntgegeben werden. Weiterhin ist Nutzern die Möglichkeit einzuräumen, Änderungen abzulehnen (siehe hierzu auch Kapitel 4.3.1).

Neue Funktionen dürfen niemals ohne aktive Änderungen der Einstelllungen durch den Nutzer zu einer Ausweitung des Umfangs der veröffentlichten Daten oder deren Sichtbarkeit innerhalb und außerhalb des Netzwerks führen.

9.2 Löschen

9.2.1 Löschen von Inhalten der Nutzer

Betreiber sozialer Netzwerke sind grundsätzlich verpflichtet, Löschungsbegehren der Nutzer in Bezug auf deren eigene personenbezogene Daten unverzüglich umzusetzen.

Das Löschen als technischer Prozess ist bei digitalen Verfahren ein mehrstufiger Prozess, der in der Regel für den Nutzer intransparent bleibt. Verteilte Dateisysteme führen teilweise zu Problemen, erteilte Löschbefehle physisch auszuführen, da die Daten an mehreren Orten physisch vorgehalten werden und einzelne Objekte mehrfach vorhanden sein können. Zudem können sich logische und rechtliche Grenzen bei solchen Daten ergeben, die zum Bestandteil der Profile anderer Nutzer geworden sind (z. B. durch Zitieren, Verweisen, „Liken“).

Zwar kann es im Interesse der Nutzer sein, die Daten für eine Wiederherstellung versehentlich gelöschter Daten noch kurzfristig vorzuhalten (vergleichbar mit einem Papierkorb); die sich daran anschließende Löschung muss jedoch sicher und endgültig erfolgen. Insbesondere muss ein Netzwerkbetreiber zuverlässige und überprüfbare Aussagen darüber treffen, wann zur Löschung vorgesehene Daten endgültig vernichtet sind.

Netzwerkbetreiber sollten außerdem die Möglichkeit vorsehen, personenbezogene Daten, die zum Gegenstand der Profile anderer Nutzer geworden sind, zu entfernen. Betreiber können jedoch die Löschung begrenzen, wenn dadurch die Wahrnehmung berechtigter und gesetzlich anerkannter Interessen, z. B. die Wahrnehmung der Meinungsfreiheit, der jeweiligen Profilinhaber beeinträchtigt werden. Die Grenzen der Löschung sind gegenüber den Nutzern transparent zu machen.

9.2.2 Verfallsdaten von Inhalten der Nutzer

Bereits längere Zeit wird über das „Gedächtnis des Internets“ und die Wiederauffindbarkeit von Informationen, die zum Teil schon lange zurückliegen, diskutiert. Die derzeitige Generation der Nutzer sozialer Netzwerke wird im Alter ein mehr oder weniger vollständiges digitales Abbild ihrer selbst im Netz vorfinden.[30] Vor dem Hintergrund der stetig voranschreitenden technischen und analytischen Möglichkeiten ruft dies nachvollziehbare Ängste hervor.

Die Frage nach Verfallsdaten, automatischen Löschroutinen und Sperrungen stellt sich insbesondere im Kontext der sozialen Netzwerke. Es gibt erste technische Ansätze zur automatisierten Löschung von Daten[31], die sich jedoch bisher auch noch nicht genug praxistauglich erwiesen haben.[32]

In erster Linie sind die Betreiber gefordert, entsprechende Funktionen einzuführen und nutzerfreundlich zu gestalten. Hierbei sind verschiedene Modelle denkbar, angefangen von Standardfragen bei der Veröffentlichung von Beiträgen nach deren vorgesehener Gültigkeitsdauer bis hin zu einfach zu bedienenden Löschroutinen. Denkbar ist auch, die öffentliche Zugänglichkeit von Profildaten zeitlich zu begrenzen.

---

[30] Vgl. BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Studie Soziale Netzwerke – zweite, erweiterte Studie, http://www.bitkom.org/files/documents/BITKOM_Publikation_Soziale_Netzwerke_zweite_Befragung.pdf.

[31] Vgl. Saarland University - Information Security and Cryptography Group - Prof. Dr. Michael Backes, X-pire! - Wie man dem Internet das "Vergessen" beibringt, http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/.

[32] Vgl. Universität Regensburg, Lehrstuhl Wirtschaftsinformatik 4 - Management der Informationssicherheit, Fakultät für Wirtschaftswissenschaften, Prof. Dr. Hannes Federrath, Digitaler Radiergummi und seine Folgen, http://www-sec.uni-regensburg.de/research/streusand/.

Weiterhin ist angesichts neuerer technischer Entwicklungen, z. B. auf Basis von HTML5[33] oder IPv6[34], zu prüfen, inwieweit damit mehr Selbstkontrolle über Nutzerdaten bzw. eine Aufweichung der bestehenden Kunden-Contentprovider-Strukturen möglich ist.

9.2.3 Abmeldung von einem sozialen Netzwerk

Die Abmeldung aus einem sozialen Netzwerk muss einfach und endgültig möglich sein. Die von einzelnen Netzwerken geübte Praxis, Profile in einen „Ruhezustand“ zu versetzen, um dem Nutzer eine spätere Rückkehr zu ermöglichen, ist unzureichend. Der Nutzer muss eine vollständige Kontrolle über seine Daten erlangen und selbst bestimmen können, wie mit seinen Daten verfahren wird. Dabei kann grob zwischen endgültiger Abmeldung (und damit einhergehender Löschung), Ruhezustand (und Nichtsichtbarkeit für Dritte) und einer Mitnahme der Daten (mit anschließender Löschung beim Betreiber) unterschieden werden. In diesen Fällen sind folgende Anforderungen zu erfüllen:

- Der Nutzer sollte eine explizite Löschbestätigung anfordern können, indem der Betreiber eine Löschung in Textform zusichert.
- Die Effektivität der Löschroutinen oder anlassbezogenen Löschungen sollten durch den Betreiber mittels entsprechender allgemein zugänglicher Dokumentation nachgewiesen werden.
- Die Betreiber haben transparent über die Aufbewahrungsfristen für inaktive Accounts zu informieren.

9.3 Auskunft an Betroffene

Betreiber sozialer Netzwerke sind zur (vollständigen) Auskunft nach § 34 BDSG bzw. 13 Abs. 7 TMG verpflichtet.

Für Auskunftsersuchen hat der Betreiber eine einfach zu erreichende Kontaktmöglichkeit innerhalb des Netzwerks einzurichten. Um Missbrauch zu verhindern, müssen Auskunftsersuchen angemessen sicher autorisiert werden, z. B. durch eine Bestätigungsmail an die für das Nutzerprofil registrierte E-Mail-Adresse. Der Nutzer muss die Form der Auskunft (in Textform/elektronisch) wählen können.

Eine Auskunft muss Inhalts-, Bestands- und Nutzungsdaten vollständig umfassen. Inhalts- und Bestandsdaten sind dabei die im Netzwerk hinterlegten persönlichen Daten, Kommunikationen, Bilder und Videos. Nutzungsdaten umfassen das Logging des Nutzers, also welche Seiten des sozialen Netzwerks oder externer Quellen, die über Social Plug-ins mit dem Netzwerk verbunden

[33] Vgl. Konrad Lischka, Hier liest Facebook nicht mit, SPIEGEL ONLINE, http://www.spiegel.de/netzwelt/web/0,1518,825950,00.html.
[34] Vgl. Lutz Donnerhacke, Kommentar: IPv6 und der Datenschutz, heise online, http://www.heise.de/netze/artikel/Kommentar-IPv6-und-der-Datenschutz-1375692.html.

sind, er besucht hat, wann und wie er sich ein- oder ausgeloggt hat oder welche Anfragen ihn innerhalb des Netzwerks erreicht haben. Ebenfalls vom Auskunftsrecht umfasst sind Nutzungsdaten, durch die der Nutzer auch nach dem Ausloggen für das Netzwerk identifizierbar bleibt, z. B. über ein Cookie oder das Browserprofil. Weiterhin sollten einfache Möglichkeiten des Downloads von eigenen Profilen etabliert werden. Der Entwurf der neuen EU-Datenschutzgrundverordnung sieht ein solches Prinzip der Datenportabilität als Recht der informationellen Selbstbestimmung der Nutzer vor.

Auch Nicht-Nutzern ist ein Recht auf Auskunft zu den über sie gespeicherten personenbezogenen Daten einzuräumen. Dafür müssen Betreiber sozialer Netzwerke transparent darstellen, in welcher Weise Daten von Nicht-Nutzern erhoben und verarbeitet werden, z. B. durch den Abgleich von Adressbüchern von Mitgliedern, welche auch Daten von Nicht-Mitgliedern enthalten können.

10 Einzelthemen

10.1 Zugriff auf Adressen

Häufig werden von den Betreibern Funktionen angeboten, die es dem Nutzer ermöglichen, ein auf dem Gerät (PC, Smartphone) gespeichertes oder bei einem E-Mail-Provider geführtes Adressbuch dem sozialen Netzwerk vollständig zur Verfügung zu stellen (sog. Friend-Finding).

Hierbei ist neben der expliziten Einwilligung des Nutzers eine Möglichkeit zur Vorabprüfung der Adressen und zur Sperrung von Einzeladressen durch den Nutzer vor der Übertragung notwendig. Eine automatische Übertragung aller Adressen eines Nutzers an ein soziales Netzwerk ist nicht zulässig. Der Nutzer hat die Verantwortung für die Daten der betroffenen Dritten. Er muss erkennen können, welche Adressen übertragen wurden und muss diese bei Bedarf löschen können.

Besondere Risiken bestehen beim Hochladen beruflich erlangter Kontaktdaten in ein Profil eines Sozialen Netzwerks, z. B. wenn Ärzte oder Psychotherapeuten Kontaktdaten ihrer Patienten bzw. Klienten dafür freigeben und diese dann auf einmal z. B. Freundschaftsanfragen an ihre dortigen Profile übermittelt bekommen. Auf diese Risiken sollten Betreiber Sozialer Netzwerke hinweisen.

Eine Nutzung der Adressdaten durch den Betreiber eines Sozialen Netzwerks für eigene Zwecke im Rahmen der Werbung für den Beitritt zum eigenen Netzwerk (Friend-Finding) ist nur mit Einwilligung der Betroffenen zulässig.

10.2 Biometrie

Der Einsatz biometrischer Verfahren im Rahmen sozialer Netzwerke erfordert besondere Rahmenbedingungen. Von praktischer Bedeutung ist dabei vor allem das Verfahren der

Gesichtserkennung, welches die automatische Markierung von Personen auf in das soziale Netzwerk hochgeladenen Bildern erlaubt.

Die Erstellung, Speicherung und weitere Verwendung biometrischer Daten erfordert die vorherige, explizite Einwilligung der Betroffenen. Diese Einwilligung kann nur auf der Basis einer umfassenden Information der Betroffenen über die Art und Weise der Verwendung der entsprechenden persönlichen Daten in diesem Zusammenhang erfolgen (informierte Einwilligung).

Betreiber eines sozialen Netzwerks dürfen lediglich die Daten registrierter Nutzer, deren entsprechende Einwilligung vorliegt, verarbeiten. „No matches“, also personenbeziehbare biometrische Daten, die keinem Nutzer des sozialen Netzwerkes zuzuordnen sind, müssen unverzüglich und irreversibel gelöscht werden. Neue, nachträgliche Erkennungs- bzw. Zuordnungsvorgänge („Matchingläufe“), etwa über den Bestand nicht identifizierter Personen, sind nicht zulässig. Ein biometrischer Abgleich eines neuen Mitglieds (oder nach der Einwilligung eines Mitglieds) mit dem bisherigen, kompletten Datenbestand des sozialen Netzwerkes darf nicht erfolgen.

Nur unter den soeben genannten Bedingungen ist die Einholung einer Einwilligung zur Erstellung temporärer biometrischer Daten entbehrlich. Nach Erstellung des temporären Templates muss durch den Betreiber geprüft werden, ob eine Einwilligung in die dauerhafte Speicherung des Templates vorliegt. Ist dies nicht der Fall, muss nach den beschriebenen Bedingungen eine Löschung vorgenommen werden. Die Erfüllung dieser Anforderung ist durch eine entsprechende Dokumentation nachzuweisen.

Die Möglichkeit zur jederzeitigen Rücknahme der Einwilligung ist sicherzustellen; die sich daraus ergebenen Konsequenzen müssen technisch umgesetzt werden. Das Referenztemplate muss gelöscht und dessen Verknüpfung bzw. Zuordnung über den gesamten Datenbestand des sozialen Netzwerkes aufgelöst werden.

Für die Übermittlung biometrischer Daten durch den Betreiber des sozialen Netzwerkes an Dritte oder die Nutzung für andere Dienste ist eine entsprechende weitergehende Einwilligung beim Betroffenen erforderlich (informierte Einwilligung).

Es ist technisch und organisatorisch sicherzustellen, dass die biometrischen Daten ausschließlich für die Zwecke genutzt werden, für die sie auch erhoben wurden und denen die Betroffenen im Rahmen ihrer Einwilligung zugestimmt haben.

Bei der Aufnahme und der Übertragung der Bilder (Upload) sind verschlüsselte Kommunikationswege zu nutzen. Dies gilt insbesondere dann, wenn die biometrischen

Algorithmen im Endgerät der Nutzer ablaufen und die Ergebnisse dieser Verfahren mit zentralen Datenbanken abgeglichen werden.[35]

10.3 Werbung

Im Hinblick auf Bestandsdaten (zum Begriff siehe 4.2.2) sieht das einschlägige TMG keine andere gesetzliche Grundlage für eine Verwendung zum Zweck der Werbung als die Einwilligung der Nutzenden vor. Gleiches gilt für die Nutzungsdaten (zum Begriff siehe 4.2.3), jedenfalls wenn diese nicht lediglich unter einem Pseudonym zusammengeführt werden (siehe unten 10.4 Reichweitenanalyse). Im Hinblick auf die nach dem BDSG zu beurteilenden Inhaltsdaten ist insbesondere für Werbung auf der Basis von Profildaten nach § 3 Abs. 9 BDSG – dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben – eine informierte Einwilligung der Betroffenen erforderlich.

10.4 Reichweitenanalyse

Betreiber sozialer Netzwerke, vor allem diejenigen, die eine Finanzierung des Angebotes über Werbeeinnahmen durchführen, betreiben Reichweitenanalysen, mittels derer die Art und Weise der Nutzung des Dienstes sowie die Interessen und Vorlieben der Nutzer festgestellt, analysiert und ausgewertet werden können.

Durch eine derartige Reichweitenanalyse werden umfangreiche und sehr detaillierte Aussagen über die Nutzerinnen und Nutzer durch die Betreiber erhoben, die umfangreiche und sehr detaillierte Aussagen über die Nutzer erlauben, die über die willentlich und bewusst angegebenen Informationen hinausgehen. Die Nutzer sollten grundsätzlich selbst in die Lage versetzt werden, die Datenverarbeitung in ihren Geräten zu steuern. Letzteres ist z. B. durch den Einsatz von Browser-Plug-ins realisierbar. Dadurch kann z. B. das Speichern von Cookies oder Ausführen von JavaScript-Programmen unterbunden werden.

Der Umfang und die Art der Daten der Reichweitenanalyse kann von der Verarbeitung rein technischer Angaben, wie z. B. des genutzten Betriebssystems bis hin zu einer detaillierten Erfassung der Mouse-Aktivitäten eines einzelnen Nutzers reichen. Auch der Fokus der Analyse kann unterschiedlich sein. Einige Anbieter können durch den Einsatz von Social Plug-ins nicht nur die Nutzung des eigenen Dienstes analysieren. Auch die Nutzung anderer Angebote des Internets durch die in dem jeweiligen Netzwerk angemeldeten Nutzer wird analysiert.

Unabhängig von der technischen Art und Weise der eingesetzten Reichweitenanalyse ist diese nur zulässig, wenn sie auf einer entsprechenden rechtlichen Grundlage beruht. Als gesetzliche

[35] Vgl. auch Working Paper 192 der Art. 29-Gruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, vom 22. März 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf.

Rechtsgrundlage kommt § 15 Abs. 3 TMG zur Anwendung. Danach ist die Analyse der Nutzung des angebotenen Dienstes oder darüber hinaus zur

- Werbung,
- Marktforschung oder
- bedarfsgerechten Gestaltung des eigenen Dienstes

zulässig. Die Wahrung dieser Voraussetzung ist durch den Betreiber des Netzwerkes nachzuweisen. Dies gilt insbesondere in den Fällen, in denen die Analyse des Nutzungsverhaltens über das eigene Angebot hinausreicht. Eine anbieterübergreifende Reichweitenanalyse kann nicht auf § 15 Abs. 3 TMG gestützt werden und bedarf regelmäßig der Einwilligung der Nutzenden.

Die Reichweitenanalyse muss den Nutzern kenntlich gemacht werden. Ihnen ist außerdem gemäß § 15 Abs. 3 TMG die Möglichkeit einzuräumen, der Erhebung, Verarbeitung und Nutzung der Informationen über die Nutzung des Dienstes oder anderer Angebote des Internets widersprechen zu können. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen.

Die Erstellung der Nutzungsprofile ist nur bei Verwendung von Pseudonymen zulässig. Die IP-Adresse ist kein Pseudonym i. S. d. § 15 Abs. 3 TMG.[36] Betreiber haben daher sicherzustellen, dass die Pseudonyme nicht aus leicht reidentifzierbaren Daten bestehen.

Gemäß Art. 5 Abs. 3 der E-Privacy-Richtlinie muss der Nutzer bei Cookies, die nicht zur Erbringung eines Dienstes erforderlich sind, vor deren Speicherung seine Einwilligung erteilt haben. Diese Regel ist bei Cookies, die zur Reichweitenanalyse genutzt werden, anwendbar.

Betreiber sozialer Netzwerke sind, anders als andere Anbieter von anmeldefreien Internetdiensten, zumeist sehr einfach in der Lage, die unter Pseudonym erstellten Nutzungsprofile einzelnen Nutzern zuzuordnen. Eine derartige Verknüpfung zwischen den von den Nutzern erstellten Profilen und den durch den Betreiber erstellten Nutzungsprofilen ist nur zulässig, wenn die Betroffenen vorher eingewilligt haben. Die Einwilligung muss den Anforderungen des § 4a BDSG bzw. § 13 Abs. 2 TMG entsprechen.

Eine Zusammenführung dieser Angaben ohne die Einwilligung der Nutzer ist unzulässig und stellt einen Bußgeldtatbestand dar.

Für Themennetzwerke, die für besondere Nutzergruppen eingerichtet wurden, können Beschränkungen hinsichtlich der grundsätzlichen Zulässigkeit der Nutzungsanalyse bestehen. So unterliegen aufgrund des hohen Schutzbedarfes besonderer personenbezogener Daten (§ 3 Abs. 9 BDSG) soziale Netzwerke zu den Themen Gesundheit, sexuelle Orientierung, politische

[36] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 in Stralsund, http://www.informationsfreiheit-mv.de/dschutz/beschlue/Analyse.pdf.

oder religiöse Anschauungen etc., gesonderten und besonderen Rechtfertigungsanforderungen hinsichtlich der Durchführung der Reichweitenanalyse. Die Erforschung und Auswertung des Nutzerverhaltens ist nur auf der Grundlage einer Einwilligung zulässig. Gleiches gilt für soziale Netzwerke ohne unmittelbaren thematischen Bezug zu besonderen personenbezogenen Date,n bei denen derartige Daten zum Zweck der Reichweitenanalyse genutzt werden. Auch hier ist eine gesonderte Einwilligung erforderlich.

10.5 Nutzung auf mobilen Endgeräten

Die Verwendung eines sozialen Netzwerks auf einem mobilen Gerät unterscheidet sich in einigen Punkten wesentlich von der Verwendung mit einem Webbrowser, wenn spezielle Apps oder eine Integration von (mehreren) sozialen Netzwerken in das Betriebssystem des mobilen Gerätes zum Einsatz kommen. Die grundsätzlichen Funktionalitäten wie Kontakte knüpfen und pflegen, Nachrichten austauschen und Bilder und Fotos teilen, sind auf mobilen Geräten wie Smartphones oder Tablets ebenfalls vorhanden. Darüber hinaus sind Lokalisierungsdaten über den eigenen Aufenthaltsort sowie ggf. die Standorte anderer Teilnehmer des sozialen Netzwerks verfügbar.

10.5.1 Umgang mit Lokalisierungsdaten

Mobile Endgeräte verfügen üblicherweise über Ortungsdienste, welche mit GPS sowie durch Informationen aus WLAN-Hotspots und Mobilfunkmasten realisiert werden. Sollen diese standortbezogenen Daten an ein soziales Netzwerk übertragen werden, wird eine Einwilligung des Nutzers benötigt, soweit dies nicht für die Erbringung der jeweiligen Dienstleistung erforderlich ist. Die Voreinstellung dieser Datenübertragung sollte derart sein, dass keine Daten übertragen werden. Sollen die Standortdaten allen Personen eines sozialen Netzwerks zugänglich gemacht werden, dann ist eine eindrückliche Warnung an den Nutzer erforderlich. Alle Einstellungen zur Lokalisierung sollten über einen leicht auffindbaren Menüpunkt klar erkennbar und jederzeit änderbar sein. Eine Deaktivierung Nutzung und Löschung der Standortdaten muss jederzeit leicht möglich sein; eine Deaktivierung aller Ortungsdienste des Gerätes ist hierfür nicht ausreichend.

Die fortlaufende Speicherung von Aufenthaltsinformationen im Sinne einer Historie ist nur gestattet, solange und soweit dies für die Erbringung einer Dienstleistung erforderlich ist. Nutzer sind über evtl. existierende Datenbestände historischer Aufenthaltsinformationen im Rahmen der Information nach § 13 Abs. 1 TMG zu unterrichten. Sie sollten darüber hinaus jederzeit die Möglichkeit haben, Aufenthaltshistorien zu löschen.

10.5.2 Übertragung

Personenbezogene Daten dürfen nur an den Betreiber des sozialen Netzwerks übertragen werden. Eine Übermittlung dieser Daten an andere Empfänger (wie den Hersteller der App-Software) ist im Allgemeinen nicht erforderlich und damit auch nicht zulässig. Sollten doch

Diagnose- oder Trackingdaten zusätzlich erfasst werden, so muss hierzu die explizite Einwilligung des Nutzers eingeholt oder sämtliche personenbezogenen Daten vor der Übertragung i. S. d. § 3 Abs. 6 BDSG anonymisiert werden.

Eine Übertragung der Daten muss über eine ausreichend verschlüsselte Verbindung (SSL/TLS) erfolgen und gegen unberechtigte Zugriffe (Man-In-The-Middle-Angriffe) geschützt sein.

Literatur

[1] Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282012%294&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864#RelatedDocuments

[2] Selbstbedienungsladen Smartphone: Apps greifen ungeniert persönliche Daten ab, http://www.heise.de/ct/artikel/Selbstbedienungsladen-Smartphone-1464717.html

[3] Data Protection Commissioner of Ireland: Facebook Ireland Ltd Report of Audit, http://dataprotection.ie/documents/Facebook%20Report/Facebookauditreport1.pdf

[4] Data Protection Commissioner of Ireland: Facebook Technical Analysis Report, http://dataprotection.ie/documents/Facebook%20Report/report.pdf/appendices.pdf

[5] Data Protection Commissioner of Ireland: Facebook Ireland Ltd Report of Re-Audit, http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

[6] Tao Stein et al.: Facebook Immune System, http://allfacebook.de/wp-content/uploads/2011/10/FacebookImmuneSystem.pdf

[7] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 08. Dezember 2011): Datenschutz in sozialen Netzwerke, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf?__blob=publicationFile

[8] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden: Datenschutzkonforme Gestaltung sozialer Netzwerke, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/Duesseld

orferKreis/170408DatenschutzkonformeGestaltungSozNetzwerke.pdf?__blob=publicationFile

[9] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke (WP 163), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf

[10] International Working Group on Data Protection in Telecommunications: Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten - ,,Rom Memorandum" - 43. Sitzung, 3.-4. März 2008, http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf

[11] Berliner Beauftragter für Datenschutz und Informationsfreiheit: ICH SUCHE DICH. Wer bist du? Soziale Netzwerke & Datenschutz, Juli 2012, http://www.datenschutz-berlin.de/attachments/894/2012-Broschuere-Soziale-Netzwerke.pdf

[12] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: selbst & bewusst. Tipps für den persönlichen Datenschutz bei Facebook, Januar 2013, http://www.datenschutz-hamburg.de/uploads/media/selbst_bewusst-Datenschutz_bei_Facebook_01.pdf

[13] Datenschutzbeauftragter des Kantons Zürich: Checkliste Privacy Facebook, November 2012, https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/veroeffentlichungen/leitfaeden_und_checklisten/_jcr_content/contentPar/publication_1/publicationitems/titel_wird_aus_dam_e/download.spooler.download.1355402195455.pdf/Checkliste+Privacy+Facebook.pdf

Abkürzungen

AGB	Allgemeine Geschäftsbedingungen
API	Application Programming Interface
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
FAQ	Frequently Asked Questions
GG	Grundgesetz
GPS	Global Positioning System
HDFS	Hadoop Distributed File System
HTML	Hyptertext Markup Language
IP	Internet Protocol
KUG	Kunsturhebergesetz
LDSG	Landesdatenschutzgesetz
LSO	Local Shared Object
RL	Richtlinie
SSL	Secure Sockets Layer
stopp	Strafprozessordnung
TLS	Transport Layer Security
TMG	Telemediengesetz
WLAN	Wireless Local Area Network