Duale Hochschule Baden-Württemberg
Mannheim

Seminararbeit

Titel

IT-Recht

Studienrichtung Software Engineering

Verfasser:	Sebastian Röhling und Jan Kipka
Kurs:	WWI 14 SEB
Dozent:	BLANK
Studiengangsleiter:	Prof. Dr. Thomas Holey
Bearbeitungszeitraum:	BLANK – BLANK

Kurzfassung

Titel	Titel
Verfasser/in:	Sebastian Röhling und Jan Kipka

Inhaltsverzeichnis

Abbildungsverzeichnis **iv**

Tabellenverzeichnis **v**

Abkürzungsverzeichnis **vi**

1 Einleitung **1**

2 Grundlagen des Bundesdatenschutzgesetzes **2**
2.1 Hintergrund des Gesetzes 2
2.2 Grundlegende Aspekte des Gesetzes 3
2.2.1 Zweck des Gesetzes und Begriffsbestimmungen 3
2.2.2 Zulässigkeit der Datenerhebung 4

3 Grundlagen des Telemediengesetzes bei der Anwendung von sozialen Netzwerken **5**
3.1 Begriffsbestimmungen und Pflichten 5
3.2 Speicherung von Bestands- und Nutzungsdaten 6
3.3 Die Gesetze zum Datenschutz im Kontext sozialer Netzwerke 6

4 Umgang mit personenbezogenen Daten anhand von Praxisbeispielen **8**
4.1 WhatsApp 8
4.2 Facebook 9
4.3 Twitter 9

5 Internationale Datenschutzregelungen **11**
5.1 Anwendbares Recht 11
5.2 Prüfungsstufen zur Datenübermittlung ins Ausland 11
5.2.1 Prüfungsstufe 1: Zulässigkeit der Datenübermittlung 12
5.2.2 Prüfungsstufe 2: Prüfung des Datenschutzniveaus im Empfängerstaat 12
5.2.3 Fall 4: Sonstige Drittstaaten 14

6 Fazit **16**

Literatur **17**

A Anhang **18**

Abbildungsverzeichnis

Abbildung A.1 Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im Januar 2017 (in Millionen) 19

Tabellenverzeichnis

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
EU	Europäische Union
BDSG	Bundesdatenschutzgesetz
TMG	Telemediengesetz

1 Einleitung

Im Zeitalter des Internets gehören soziale Netzwerke wie *Facebook* oder *Twitter* zum Alltag. Um diese Netzwerke nutzen zu können, müssen die Anwender mit den Datenschutzbestimmungen der Diensteanbieter einverstanden sein. Dies schließt die Datenspeicherung der personenbezogener Daten der Benutzer ein, in vielen Fällen sogar die Weitergabe der Daten an Dritte. Das Bundesdatenschutzgesetz und das Telemediengesetz regeln dabei die Persönlichkeitsrechte beim Umgang mit personenbezogenen Daten und bilden den Rahmen für die Erhebung, Verarbeitung und Nutzung dieser. Die wichtigsten Aspekte der beiden Gesetze werden in dieser Arbeit erläutert.

Im ersten Teil der Arbeit werden die Grundlagen des Bundesdatenschutzgesetzes dargelegt. Dabei wird u.a. auf den Hintergrund des Gesetzes, den Zweck und die Regelungen der Zulässigkeit der Datenerhebung. Anschließend folgt die Erläuterung der wichtigsten Aspekte des Telemediengesetzes, um anschließend die deutschen Gesetzesregelungen auf internationale Datenschutzregelungen zu beziehen. Die Arbeit schließt mit einem Fazit.

2 Grundlagen des Bundesdatenschutzgesetzes

Im nachfolgenden Kapitel werden die Grundlagen des Bundesdatenschutzgesetzes vermittelt, welche zum allgemeinen Verständnis dieser Arbeit notwendig sind. Im ersten Teil wird der Hintergrund des Gesetzes näher erläutert, um im zweiten Teil auf die wichtigsten Aspekte einzugehen.

2.1 Hintergrund des Gesetzes

Die amtliche Anmerkung zum Bundesdatenschutzgesetz (BDSG) beschreibt den allgemeinen Hintergrund des Gesetzes wie folgt:

> „Dieses Gesetz dient der Umsetzung der 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).“[1]

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 beordert den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Gründe für das Verfassen der Richtlinie sind u.a. einerseits die Notwendigkeit der Übermittlung von personenbezogenen Daten von einem Mitgliedsstaat der Europäischen Union (EU) in einen anderen zur Errichtung eines funktionierenden Binnenmarktes. Bei dieser Übermittlung sind jedoch die Grundrechte der Personen zu wahren. Andererseits gelten in den Mitgliedsstaaten unterschiedliche Schutzniveaus der Personenfreiheiten und -rechte bei der Verarbeitung personenbezogener Daten, was die Übermittlung dieser Daten zwischen den verschiedenen Staaten verhindern kann. So könnten zahlreiche gemeinsame Wirtschaftsaktivitäten gehemmt oder der Wettbewerb verfälscht werden. Aus diesem Grund ist ein gleichwertiges Schutzniveau zur Beseitigung der Hemmnisse unerlässlich. In der Gemeinschaft der EU ist die Angleichung der Rechtsvorschriften erforderlich.[2]

[1] dejure.org 2017.
[2] vgl. European Union 1995.

2.2 Grundlegende Aspekte des Gesetzes

2.2.1 Zweck des Gesetzes und Begriffsbestimmungen

Die Umsetzung der Angleichung ist das BDSG, welches laut §1 Abs. 1 BDSG den Einzelnen davor schützt, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. §1 Abs. 2 BDSG definiert die gültigen Stellen, die personenbezogene Daten für die Erhebung, Verarbeitung und Nutzung erheben:

1. Öffentliche Stellen des Bundes,
2. Öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. Nicht-öffentliche Stellen (u.a. soziale Netzwerke), soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Weiterhin grenzt das BDSG den Begriff der personenbezogenen Daten ab. Laut §3 Abs. 1 BDSG „sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“ §3 Abs. 4 BDSG definiert das Verfahren des Speicherns. Das Speichern ist im Einzelnen das „Erfassen, Aufnehmen oder Aufbewahren von personenbezogenen Daten.“ Diese Daten werden auf einem Datenträger zum Zweck einer Weiterverarbeitung und Nutzung gesichert. Das Übermitteln wird laut §3 Abs. 4 BDSG als Bekanntgeben der gespeicherten personenbezogenen Daten an einen Dritten verstanden, wobei die Daten entweder direkt an einen Dritten weitergegeben werden oder dieser die Daten einsieht oder abruft. Werden die gespeicherten Daten letztendlich in jeglicher Weise verwendet, handelt es sich um das Nutzen der Daten.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten steht allgemein unter dem Prinzip der Datensparsamkeit, laut §3a TMG. Dies bedeutet, dass die Speicherung der Daten und die Gestaltung der Datenverarbeitungssysteme an dem Ziel ausgerichtet werden, so wenig Daten wie möglich zu erheben, verarbeiten und

zu nutzen. Weiterhin sind die Daten zu anonymisieren oder zu pseudonymisieren, sofern dies je nach Verwendungszweck möglich und nicht mit einem erhöhten Aufwand verbunden ist.

2.2.2 Zulässigkeit der Datenerhebung

Zum Abschluss dieses Unterkapitels wird auf einen weiteren grundlegenden Teil des BDSGs eingegangen. Nachdem nun der Zweck des Gesetzes und kontextuelle Begriffe abgegrenzt worden sind, wird nun die Zulässigkeit der Datenerhebung, -verbreitung und -nutzung anhand §4 BDSG erläutert.

§4 Abs. 1 BDSG zur Folge ist die „Erhebung, Verarbeitung und Nutzung personenbezogener Daten (...) nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dieses erlaubt oder anordnet oder der Betroffene eingewilligt hat." Dies bedeutet, dass die Erhebung, Verarbeitung und Nutzung grundsätzlich verboten ist, jedoch zulässig wird, wenn entweder eine klare Rechtsgrundlage gegeben ist oder der Nutzer die Erhebung, Verarbeitung und Nutzung der Daten ausdrücklich erlaubt.

Laut §4 Abs. 2 BDSG sind personenbezogene Daten beim Betroffenen zu erheben. Dies ist ohne seine Mitwirkung nur zulässig, wenn entweder eine Rechtsvorschrift die Erhebung vorsieht oder eine zu erfüllende Verwaltungsaufgabe oder ein Geschäftszweck diese erforderlich macht. Weiterhin ist sie ebenfalls zulässig, wenn „die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde". Generell stehen beide Fälle unter der Bedingung, dass keine Anhaltspunkte für eine Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen existieren.

§4 Abs. 3 BDSG erklärt die Unterrichtungspflicht der Datenerhebung durch die verantwortliche Stelle gegenüber dem Betroffenen. Die Unterrichtung schließt die Identität der verantwortlichen Stelle und den Zweck der Erhebung, Verarbeitung und Nutzung ein. Außerdem sind die Kategorien von Empfängern dem Betroffenen nur mitzuteilen, wenn dieser nicht mit der Übermittlung an diese zu rechnen hat. Werden personenbezogene Daten durch die Anordnung einer Rechtsvorschrift erhoben, die zu einer Auskunft verpflichtet, ist der Betroffene hierauf hinzuweisen.

Nachdem nun die Grundlagen des BDSGs erläutert worden sind, folgt im nachfolgenden Kapitel die Beschreibung der Grundsätze des Telemediengesetzes, welches die Vorschriften des BDSGs auf die Erhebung personenbezogener Daten bei der Benutzung des Internets und folglich sozialer Netzwerke anwendet.

3 Grundlagen des Telemediengesetzes bei der Anwendung von sozialen Netzwerken

Das BDSG regelt den Datenschutz bei der allgemeinen Erhebung von personenbezogenen Daten, jedoch nicht explizit für die Datenerhebung bei der Benutzung des Internets und folglich sozialer Netzwerke. Für diesen Zweck ist 2007 das Telemediengesetz (TMG) in Kraft getreten, welches den Datenschutz im Internet regelt.[3][4] In diesem Kapitel werden die Grundlagen des TMGs vermittelt und im Kontext der Anwendung von sozialen Netzwerken behandelt.

3.1 Begriffsbestimmungen und Pflichten

Laut §2 TMG ist ein Diensteanbieter „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt (...)." Weiterhin ist ein Nutzer laut §2 TMG jede natürlich oder juristische Person, die Telemedien nutzt, um insbesondere Informationen zu erhalten. Abschließend werden Telemedien als Verteildienste bezeichnet, welche laut §2 TMG „im Wege einer Übertragung von Daten ohne individuelle Anforderung gleichzeitig für eine unbegrenzte Anzahl von Nutzern erbracht werden." Dazu gehören nahezu alle Angebote im Internet, wie Shopping-Portale, Online-Dienste (wie z.B. Wetter- oder Nachrichtenauskünfte) oder Suchmaschinen.[5]

Wann und unter welchen Bedingungen personenbezogene Daten nun aber tatsächlich erhoben werden dürfen, regeln §§12, 13 TMG. §12 Abs. 1 TMG besagt, dass Diensteanbieter personenbezogene Daten nur erheben und verwenden dürfen, wenn das TMG oder eine andere Telemedien-bezügliche Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat. Gleiches gilt für die Verwendung der Daten für andere Zwecke. Zu Beginn des Nutzungsvorgangs hat der Diensteanbieter den Betroffenen über

[3] vgl. klicksafe.de 2017a.
[4] vgl. Surfer-haben-rechte.de 2014.
[5] vgl. Surfer-haben-rechte.de 2014.

die Erhebung und Verwendung der Daten laut §13 Abs. 1 TMG zu unterrichten. Die Einwilligung des Nutzers kann dabei elektronisch eingeholt werden, sofern der Diensteanbieter sicherstellt, dass die Einwilligung bewusst und eindeutig erteilt wird, die Einwilligung protokolliert wird, der Inhalt der Einwilligung jederzeit abrufbar ist und der Nutzer die Einwilligung jederzeit widerrufen kann (§13 Abs. 2 TMG).

3.2 Speicherung von Bestands- und Nutzungsdaten

§14 Abs. 1 TMG spezifiziert eine Art der Daten, welche von den Diensteanbietern erhoben und verwendet werden dürfen: die Bestandsdaten. Bestandsdaten gelten als Daten, welche „für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten).“ Wenn eine zuständige Stelle eine Auskunft über Bestandsdaten anordnet, sofern dies staatliche Zwecke, wie z.B. der Strafverfolgung, notwendig ist, dürfen Diensteanbieter diese Auskunft erteilen.

Neben den Bestandsdaten sieht das TMG ebenfalls die Erhebung und Nutzung von Nutzungsdaten vor. Laut §15 Abs. 1 TMG sind Nutzungsdaten erforderlich, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Dabei sind Nutzungsdaten insbesondere Merkmale zur Identifikation des Nutzers, Angaben zum Beginn und Ende sowie zum Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer ins Anspruch genommenen Telemedien. §15 Abs. 3 erlaubt den Diensteanbietern die Nutzung der Daten zur Erstellung von Nutzungsprofilen für Zwecke der Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien führen, wenn der Nutzer dem nicht widerspricht. Weiterhin darf der Diensteanbieter die Daten auch nach dem Ende des Nutzungsvorgangs für Zwecke der Abrechnung verwenden und diese für demselben Zweck an andere Dienstanbieter und Dritte weitergeben. Zur Marktforschung anderer Diensteanbieter dürfen die Daten anonymisiert übermittelt werden (§15 Abs. 4,5 TMG).

3.3 Die Gesetze zum Datenschutz im Kontext sozialer Netzwerke

In der Praxis sind die Diensteanbieter von sozialen Netzwerken darauf angewiesen, mit ihrem Angebot Profit zu erzielen. Dabei werden die verwendeten Daten, wie weiter oben erläutert, häufig anonymisiert an Dritte verkauft und weitergegeben, um die grundsätzliche kostenlose Nutzung ihrer Dienste auszugleichen. Der Verkauf der Daten

wird über die Allgemeinen Geschäftsbedingungen (AGB) abgesichert, welche vor der Nutzung vom Benutzer durchgelesen werden sollten und bestätigt werden. Somit ist die Unterrichtungspflicht der Diensteanbieter gegenüber den Nutzern erfüllt. Jedoch ist nicht alles, was die Anbieter in den AGB vermerken, automatisch rechtskräftig. Aus diesem Grund geht der Bundesverband der Verbraucherzentralen gegen einzelne, für Nutzer besonders nachteilige Klauseln vor.[6]

Im Jahr 2015 beispielsweise hat der Verbraucherschutz *Facebook* abgemahnt, nachdem der Anbieter des sozialen Netzwerks seine AGBs aktualisiert hat und diese aus Sicht des Verbands gegen 19 Klauseln des deutschen Rechts verstoßen. Das Geschäftsmodell von Facebook basiert auf dem Motto *Facebook ist und bleibt kostenlos*, jedoch wurden mit der Einführung der aktualisierten AGB personenbezogene Nutzerdaten an werbetreibende Unternehmen weiterverkauft. Die Verbraucherzentrale argumentiert, dass Facebook sein Geschäftsmodell verharmlosen und Transparenz verhindern würde. Trotz Mahnung der der Verbraucherzentrale konnte noch keine Einigung mit Facebook erzielt werden, sodass den Nutzern aktuell (Stand April 2017) nichts anderes übrig bleibt, als das soziale Netzwerk zu verlassen.[7][8]

Weiterhin gilt ebenfalls für soziale Netzwerke das Prinzip der Datensparsamkeit. Dies bedeutet, dass auch soziale Netzwerke die Datenmenge, die der Nutzer dem Netzwerk übermittelt, auf ein Minimum zu reduzieren hat. Außerdem ist es in einzelnen Fällen für den Nutzer möglich, sich unter einem Pseudonym anzumelden und selektiv mit den Daten umzugehen: „bei den wenigsten Sozialen Netzwerken ist es wirklich notwendig, seinen vollen Namen, die echte Adresse oder die Telefonnummer anzugeben, um den Dienst nutzen zu können. Schließlich kauft man dort (...) in der Regel nicht ein oder erhält Rechnungen, wofür der Anbieter Geschäftsdaten benötigen würde.“[9][10]

An dieser Stelle sind die nötigen Grundlagen zum BDSG und TMG vermittelt. Im folgenden Kapitel werden internationale Datenschutzregelungen im Kontext der Verwendung von sozialen Netzwerken näher beleuchtet.

[6] vgl. klicksafe.de 2017b.
[7] vgl. Spiegel Online GmbH 2015.
[8] vgl. Verbraucherzentrale Bundesverband 2017.
[9] klicksafe.de 2017b.
[10] vgl. klicksafe.de 2017b.

4 Umgang mit personenbezogenen Daten anhand von Praxisbeispielen

Das vorliegende Kapitel befasst sich damit, welche personenbezogenen Daten die drei sozialen Netzwerke WhatsApp, Facebook und Twitter von ihren Nutzern für welche Zwecke speichern, und inwiefern der Nutzer Zugang und Gewalt über die zu ihm gespeicherten Daten besitzt. Dazu werden Teilaspekte der Nutzungsbedingungen dieser Betreiber genauer durchleuchtet. Wie die Statistik in A.1 auf Seite 19 zeigt, besitzen die ausgewählten Netzwerke eine sehr hohe Reichweite und gehören zu denjenigen sozialen Netzwerken, welche heutzutage am meisten verwendeten werden.

4.1 WhatsApp

In den Nutzungsbestimmungen von WhatsApp steht zu Anfang beschrieben, dass der Nutzer durch das Verwenden der Diente von WhatsApp eine mehr oder weniger allumfassende Lizenz zur „Nutzung, Reproduktion, Verbreitung, Erstellung abgeleiteter Werke, Darstellung und Aufführung der Informationen, die [der Nutzer hochlädt, übermittelt, speichert, sendet oder empfängt]“ gewährt.[11] Zwar beschränkt sich WhatsApp in dieser Hinsicht darauf, diese Lizenz lediglich für die Dienstbetreibung, z.B. für die Nachrichtenübermittlung, zu nutzen. Nichtsdestotrotz wäre es möglich, diese Lizenz auch für weitere Marktforschungszwecke, Trendanalysen o.Ä. verwendet werden, was von WhatsApp jedoch nicht erwähnt wird. Zu den übermittelten Informationen zählen die eigene Handynummer, die Kontakte aus dem Adressbuch, aufgerufene Webseiten aus dem Messenger heraus und die Inhalte, die über die Teilen-Funktion von WhatsApp versendet werden. Darüber hinaus erhält WhatsApp Standorte, die der Nutzer selber teilt, oder die von anderen Nutzern mitgeteilt bekommen. Auch sein Online-Status und Zuletzt-Online-Status wird gespeichert.[12]

Damit WhatsApp seine Dienste bereitstellen und verbessern kann, erhebt es nicht

[11] **WhatsAppInc..2017**.
[12] **WhatsAppInc..2017**.

nur die oben genannten Informationen, sondern teilt sie auch mit der Facebook-Unternehmensgruppe und Drittanbietern.[13]

Der Nutzer hat die Möglichkeit, seinen WhatsApp-Account zu löschen. Dies garantiert jedoch nicht, dass WhatsApp alle gespeicherten personenbezogenen Daten dieses Nutzers tatsächlich löscht, da WhatsApp diejenigen Daten löscht, die nach der Läschung des Accounts nicht mehr zum Betreiben und Bereitstellen seiner Dienste benötigt werden.[14]

4.2 Facebook

Im Grunde speichert Facebook die Daten zu allen Informationen und allen Aktivitäten, die mit einem Nutzer zu tun haben. Dazu gehören erstellte und geteilte Posts, Wohnort, Geburtstag, angeschaute Inhalte, häufige Kontaktpersonen, Gerätestandorte, Namen des Mobilfunk- und Internetdienstanbieter, Besuche von Webseiten, die den „Gefällt-mir“-Button eingebettet haben und vieles mehr.[15]

Facebook nutzt diese gesammelten Informationen um personalisierte Werbung und Seiten- oder Freundesvorschläge anzuzeigen. Auch nutzt es sie um Personen in hochgeladenen Bildern zu erkennen. Auch Facebook gibt gesammelte Informationen an die Facebook-Unternehmensgruppe und an Dritte weiter, um z.B. die Wirksamkeit von Werbeanzeigen und Diensten zu messen.[16]

Im Gegensatz zu WhatsApp hingegen ist die Auskunft über die gesammelten Daten der eigenen Person transparenter gestaltet. Der Nutzer hat nämlich die Möglichkeit über einen speziellen Facebook-Dienst eine Datei herunterzuladen, die Auskunft über alle personenbezogenen Daten gibt, die über den Nutzer gesammelt wurden. Sie enthält z.B. seine Adresse, seine Klicks auf Werbeanzeigen, hinzugefügte Apps über Facebook, aktive Sitzungen, Gefällt-mir“-Angaben, Fotos, Beiträge, gelöschte Freunde, und in Facebook getätigte Suchanfragen.[17]

4.3 Twitter

Das letzte Beispiel stellt das soziale Netzwerk Twitter dar, welches im Vergleich zu den anderen beiden Netzen kein Bestandteil der Facebook-Unternehmensgruppe ist.

[13] **WhatsAppInc..2017**.
[14] **WhatsAppInc..2017**.
[15] **FacebookInc..2017**.
[16] **FacebookInc..2017**.
[17] **FacebookInc..2017b**.

Twitter speichert auf der einen Seite grundlegende Accountinformationen wie E-Mail-Adresse, Geburtsdatum, Kurzbeschreibung, Bild und Telefonnummer der Nutzers. Auf der anderen Seite Daten zu Tweets erhoben, die der Nutzer verfasst, als „gefällt-mir“ markiert, oder teilt. Zusätzlich kann der Nutzer optional sein Adressbuch hochladen, um Follower-Vorschläge zu erhalten. In diesem Fall werden diese Adressbuchdaten ebenfalls von Twitter gespeichert. Darüber hinaus nimmt sich Twitter das Recht, Standortdaten zu sammeln, wenn diese vom Nutzer geteilt werden.[18]

Twitter benutzt diese Daten zur Bereitstellung, Bewertung und Verbesserung der eigenen Dienste, und um dem Nutzer personenbezogenen und standortabhängige Werbung, Trends, Geschichten und Follower-Vorschläge anzuzeigen.[19]

Nicht-öffentliche, personenbezogene Daten gibt Twitter nur nach konkreten Anweisungen der Nutzer an Dritte weiter, wenn der Nutzer z.B. einer anderen Software den Zugriff auf den eigenen Twitter-Account gewährt. Twitter Nutzungsbedingung sieht auch vor, dass jeder Nutzer die über sich gespeicherten, personenbezogenen Daten ansehen, anpassen oder löschen kann.[20]

[18] **TwitterInc..2017**.
[19] **TwitterInc..2017**.
[20] **TwitterInc..2017**.

5 Internationale Datenschutzregelungen

5.1 Anwendbares Recht

Das deutsche Bundesdatenschutzgesetz (BDSG) wendet grundsätzlich das Territorialprinzip an. Demzufolge müssen ausländische Stellen bzw. ausländische Betreiber von sozialen Netzwerken deutsches Recht berücksichtigen, wenn diese in Deutschland personenbezogene Daten erheben wollen.[21]

Eine Ausnahme existiert für Stellen, die ihren Sitz in einem Mitgliedsstaat der Europäische Union (EU) haben und zusätzlich keinen Sitz in Deutschland haben. Denn dann wird gemäß Art. 25 der EU-Datenschutzrichtlinie 95/46/EG das Sitzlandprinzip angewandt, wenn personenbezogene Daten in Deutschland erhoben werden. Das Sitzlandprinzip besagt, dass das Recht zur Datenerhebung und zum Datentransfer desjenigen Landes anzuwenden ist, in dem die datenerhebende Stelle ihren Sitz hat[22].[23]

5.2 Prüfungsstufen zur Datenübermittlung ins Ausland

Damit eine Stelle bzw. ein soziales Netzwerk, welches Daten in den Deutschland erhebt, diese erhobenen Daten in ein anderes Land transferieren darf, gilt es zwei Prüfungsstufen zu bewältigen, welche in den folgenden Unterkapiteln genauer erläutert werden.

[21] **ICS.2011**.
[22] **ICS.2011**.
[23] **EG.1995**.

5.2.1 Prüfungsstufe 1: Zulässigkeit der Datenübermittlung

In der ersten Prüfungsstufe muss sich die erhebende Stelle bzw. das soziales Netzwerk vergewissern, ob es überhaupt befugt ist, die erhobenen Daten aus Deutschland heraus in ein anderes Land zu transferieren. Diese Befugnis kann entweder auf einem Gesetz oder auf der Einwilligung der betroffenen Person, deren erhobenen Daten ins Ausland übermittelt werden sollen, gemäß §4a BDSG beruhen.[24] Letzteres spielt für soziale Netzwerke eine besondere Rolle. Schließlich müssen Nutzer von sozialen Netzwerken ihren Datenschutzrichtlinien und damit dem Datentransfer ins Ausland bereits bei der Registrierung zustimmen.

Zusätzlich ist die erhebende Stelle den Grundprinzipien der Datenspeicherung verpflichtet, welche in **??** auf Seite ?? gelistet und erläutert sind.[25]

5.2.2 Prüfungsstufe 2: Prüfung des Datenschutzniveaus im Empfängerstaat

Bei der zweiten Prüfungsstufe wird das Datenschutzniveau im Empfängerstaat untersucht. Hierzu wird eine Fallunterscheidung vorgenommen.

Fall 1: Transfer innerhalb der EU

Da gemäß §4b Abs. 1 BDSG ein hohes Datenschutzniveau in allen Mitgliedstaat der Europäische Union vorliegt, kann die Datenübermittlung zu einer Empfängerstelle innerhalb der Europäische Union ohne weitere Vorkehrungen direkt folgen. Neben den Mitgliedsstaaten der EU wird auch Island, Norwegen und Liechtenstein ein hohes Datenschutzniveau zugeschrieben, weshalb der Datentransfer in diese Länder ebenfalls unproblematisch ist.[26]

Fall 2: Transfer in Drittstaaten mit Angemessenheitsentscheidung

Als „Drittstaaten“ oder „Drittländer“ werden nach Art. 25 der EU-Datenschutzrichtlinie 95/46/EG Empfängerstaaten bezeichnet, welche ihren Sitz[27].[28]

[24] **LDI.2017**.
[25] **LDI.2017**.
[26] **LDI.2017**.
[27] **LDI.2017**.
[28] **EG.1995**.

Manche dieser Drittstaaten haben im Sinne der EU ein angemessenes Datenschutzniveau, weshalb diesen Drittstaaten gemäß Art. 25 Abs. 6 der EU-Datenschutzrichtlinie 95/46/EG eine sogenannte Angemessenheitsentscheidung ausgesprochen wurde. Stand September 2016 trifft dies für die folgenden Staaten zu: Andorra, Argentinien, Kanada, Schweiz, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay. Liegt die Empfängerstelle, zu der der Betreiber des sozialen Netzwerkes von Deutschland senden will, in einem dieser Länder, so kann dies ohne Weiteres getan werden[29].[30]

Fall 3: Transfer in die USA

Ehemalig regelte die 2000 getroffene Übereinkunft, das sogenannte „Safe Habor"-Abkommen, den Datentransfer von Deutschland nach USA. Es besagte, dass Unternehmen in den USA ein angemessenes Datenschutzniveau im Sinne des Artikel 25 Absatz 6 der Datenschutzrichtlinie 95/46 gewährleisten, wenn sie sich den Prinzipien des Safe Habor-Abkommen per Selbstzertifizierung verpflichten.[31] Diese Prinzipien sind die „sieben "Grundsätze des ‚sicheren Hafens' zum Datenschutz"(Informationspflicht, Wahlmöglichkeit, Weitergabe, Sicherheit, Datenintegrität, Auskunftsrecht und Durchsetzung)".[32] Mit dem Urteil zur Rechtssache C-362/14, welches auch das „Schrems-Urteil" genannt wird, wurde das „Safe Habor"-Abkommen am 06.10.2015 für ungültig erklärt.[33] Zu dem besagten Schrems-Urteil kam der europäische Gerichtshof, da der österreichische Jurist Maximilian Schrems darüber empört war, was das soziale Netzwerk Facebook alles über ihn gespeichert hatte und deshalb gegen Facebook vorgegangen ist. Denn unter anderen hatte Facebook Daten von ihm gespeichert, die Schrems für gelöscht gehalten hatte.[34] Trotz der Aufhebung des Urteils wird vom US-Handelsministerium weiterhin eine Liste mit den Safe Habor-zertifizierten Unternehmen geführt, da die Prinzipien für die Daten, die von den Unternehmen unter der dem Safe Habor-Abkommmen gespeichert wurden, gelten bis sie gelöscht werden.[35]

Als Nachfolger von Safe Habor gibt es seit 12.07.2016 das „Privacy Shield"-Abkommen zwischen der EU und USA. Dieses Abkommen definiert Regelungen, die für ein angemessenes Datenschutzniveau einzuhalten sind. Amerikanische Unternehmen haben die Möglichkeit, sich zur Einhaltung der Privacy Shield-Regelungen zu verpflichten, was die Datenübermittlung von Deutschland nach USA erlaubt.[36] Das weitverbrei-

[29] **LDI.2017**.
[30] **EG.1995**.
[31] **BDFI.2017**.
[32] **BDFI.2017**.
[33] **BDFI.2017**.
[34] **Welt.2015**.
[35] **BDFI.2017**.
[36] **LDI.2017**.

tete soziale Netzwerk Twitter hat laut ihren Datenschutzrichtlinien den Regelungen des Privacy Shield-Abkommen verpflichtet, was Twitter den Transfer von deutschen Daten in die USA ermöglicht.[37]

5.2.3 Fall 4: Sonstige Drittstaaten

Will ein soziales Netzwerk personenbezogene Daten von Deutschland in ein Drittland übermitteln, welches sich keinem der drei zuvor gelisteten Fälle zuordnen lässt, dann muss die übermittelnde Stelle, also der Betreiber des sozialen Netzwerkes, gemäß §4b Abs. 3 und 5 BDSG überprüfen, ob ein angemessenes Datenschutzniveau in bei der Empfängerstelle vorliegt.[38] Ist diese Überprüfung erfolgreich, so ist die Datenübermittlung legitim. Wenn nicht, dann ist ein Transfer zur Empfängerstelle nur dann möglich, wenn einer der sechs in §4c BDSG beschriebenen Tatbestände eintritt. Der erste Tatbestand in §4c Abs. 1 Nr. 1 BDSG ist derjenige, der als einziger für Betreiber von sozialen Netzwerken greifen kann. Dieser Tatbestand besagt nämlich, dass ein Datentransfer zu einer Empfängerstelle ohne angemessenem Datenschutzniveau dann stattfinden darf, wenn die betroffene Person dazu eingewilligt hat. Damit diese Einwilligung gültig ist, muss die betroffene Person davor ausdrücklich darüber informiert werden, dass ihre Daten ohne angemessenen Datenschutz außerhalb Deutschlands gespeichert oder verarbeitet werden.[39] Der Kurznachrichtendienst WhatsApp ist ein soziales Netzwerk, deren Datenexport auf dieser Einwilligung beruht. In ihren Datenschutzrichtlinien, die jeder Nutzer akzeptieren muss, heißt es:

> „Du akzeptierst unsere Informationspraktiken, (...) sowie die Übertragung und Verarbeitung deiner Informationen in die/den USA und andere/n Länder/n weltweit, (...) und zwar unabhängig davon, wo du unsere Dienste nutzt. Du erkennst an, dass die Gesetze, Vorschriften und Standards des Landes, in dem deine Informationen gespeichert oder verarbeitet werden, von denen deines eigenen Landes abweichen können.“[40]

Greift keiner der in §4c BDSG beschriebenen Tatbestände, dann gibt es drei letzte Optionen, die ein Datentransfer zu einer Empfängerstelle in einem Drittstaat ohne angemessenen Datenschutzniveau legitim ist:

1. Die Empfängerstelle kann einen EU-Standardvertrag unterzeichnen, welcher die Empfängerstelle dazu verpflichtet die Persönlichkeitsrechte der betroffenen Personen zu wahren.[41] Facebook, eines der bekanntesten sozialen Netzwerken, ist ein

[37] **TwitterInc..2017**.
[38] **LDI.2017**.
[39] **LDI.2017**.
[40] **WhatsAppInc..2017**.
[41] **LDI.2017**.

Unternehmen, welches in ihren Datenschutzrichtlinien vorgibt, EU-Standardverträge für den Datentransfer aus Europa heraus abgeschlossen zu haben.[42]

2. Die Empfängerstelle kann einen Individualvertrag aufsetzen, welcher ebenfalls die Wahrung der Persönlichkeitsrechte der betroffenen garantiert.[43]

3. Gehört die Empfängerstelle zu einem Konzern, so kann sich dieser Konzern einer verbindlichen Konzernregelung zum Datenschutz verpflichten, welche die Persönlichkeitsrechte der betroffenen Personen wahren. Dies ist besonders für global-aktiven Konzernen interessant, da solche verbindlichen Konzernregelung den Datentransfer zur allen Empfängerstellen des Konzern erlauben, unabhängig davon, in welchem Land sie ansässig sind.[44]

[42] **FacebookInc..2017**.
[43] **LDI.2017**.
[44] **LDI.2017**.

6 Fazit

Für soziale Netzwerke sind insbesondere die deutschen und internationalen rechtlichen Regelungen zur Erhebung, Verarbeitung und Weiterleitung von personenbezogenen Daten ausschlaggebend. In Deutschland wird dies durch das Bundesdatenschutzgesetz geregelt. Es schützt laut §1 Abs. 1 BDSG den Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Betreiber von sozialen Netzwerken sind in Deutschland dazu verpflichtet, Erhebung, Verarbeitung und Nutzung personenbezogener Daten dem Prinzip der Datensparsamkeit zu unterstellen. Das heißt, dass sie so wenig Daten wie möglich speichern sollen. Des Weiteren sind sie gemäß der Unterrichtungspflicht aus §4 Abs. 3 BDSG dazu verpflichtet den Betroffen genauestens darüber zu informieren, welche Daten von ihm erhoben werden.

Aber auch der rasche Wandel von Regelungen, Richtlinien, Abkommen und Gesetze im Kontext des Datenschutzes für Betreiber eines sozialen Netzwerkes zu berücksichtigen. Das jüngste Beispiel hierfür liefert das Schrems-Urteil vom 06.10.2015, in dem das Safe Habor-Abkommen zwischen den USA und Deutschland zum sicheren Datentransfer kurzerhand für ungültig erklärt wurde.

Darüber hinaus spielt aber auch der Nutzer eine wichtige Rolle. Er möchte die Angebote eines sozialen Netzwerkes nutzen, kann mit diesem aber keine individuellen Nutzungsbedingungen aushandeln. Durch dieses strukturelle Ungleichgewicht kann ein Betreiber eines sozialen Netzwerkes im Rahmen des BDSG diktieren, welche Daten er erhebt und was er damit macht. Das Musterbeispiel stellt das Netzwerk Facebook dar, welches soviel personenbezogene Daten erhebt, wie nur möglich. Aus diesem Grund sollte sich jeder Nutzer immer zwei Mal überlegen, welche Informationen er von sich preisgibt. Denn sie werden mit hoher Wahrscheinlich eine bleibende Spur im sozialen Netzwerk hinterlassen.

Literatur

dejure.org (2017). *Bundesdatenschutzgesetz*. URL: https://dejure.org/gesetze/BDSG (besucht am 22. 06. 2017).

European Union (1995). *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*. URL: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=DE (besucht am 25. 06. 2017).

klicksafe.de (2017a). *Welche gesetzlichen Grundlagen regeln den Datenschutz im WWW?* URL: http://www.klicksafe.de/themen/datenschutz/privatsphaere/welche-gesetzlichen-grundlagen-regeln-den-datenschutz-im-www/ (besucht am 25. 06. 2017).

klicksafe.de (2017b). *Welche gesetzlichen Grundlagen regeln den Datenschutz im WWW?* URL: http://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/datenschutz-in-sozialen-netzwerken/ (besucht am 25. 06. 2017).

Spiegel Online GmbH (2015). *Verbraucherschützer mahnen Facebook ab*. URL: http://www.spiegel.de/netzwelt/netzpolitik/facebook-agb-verbraucherschutz-gegen-nutzungsbedingungen-a-1020584.html (besucht am 25. 06. 2017).

Surfer-haben-rechte.de (2014). *Datenschutz: Bundesdatenschutzgesetz und Telemediengesetz*. URL: https://www.surfer-haben-rechte.de/content/datenschutz-bundesdatenschutzgesetz-und-telemediengesetz (besucht am 25. 06. 2017).

Verbraucherzentrale Bundesverband (2017). *Facebooks Nutzungsbedingungen: Böses Erwachen für die Nutzer*. URL: https://www.verbraucherzentrale.de/facebook-2015 (besucht am 25. 06. 2017).

A Anhang

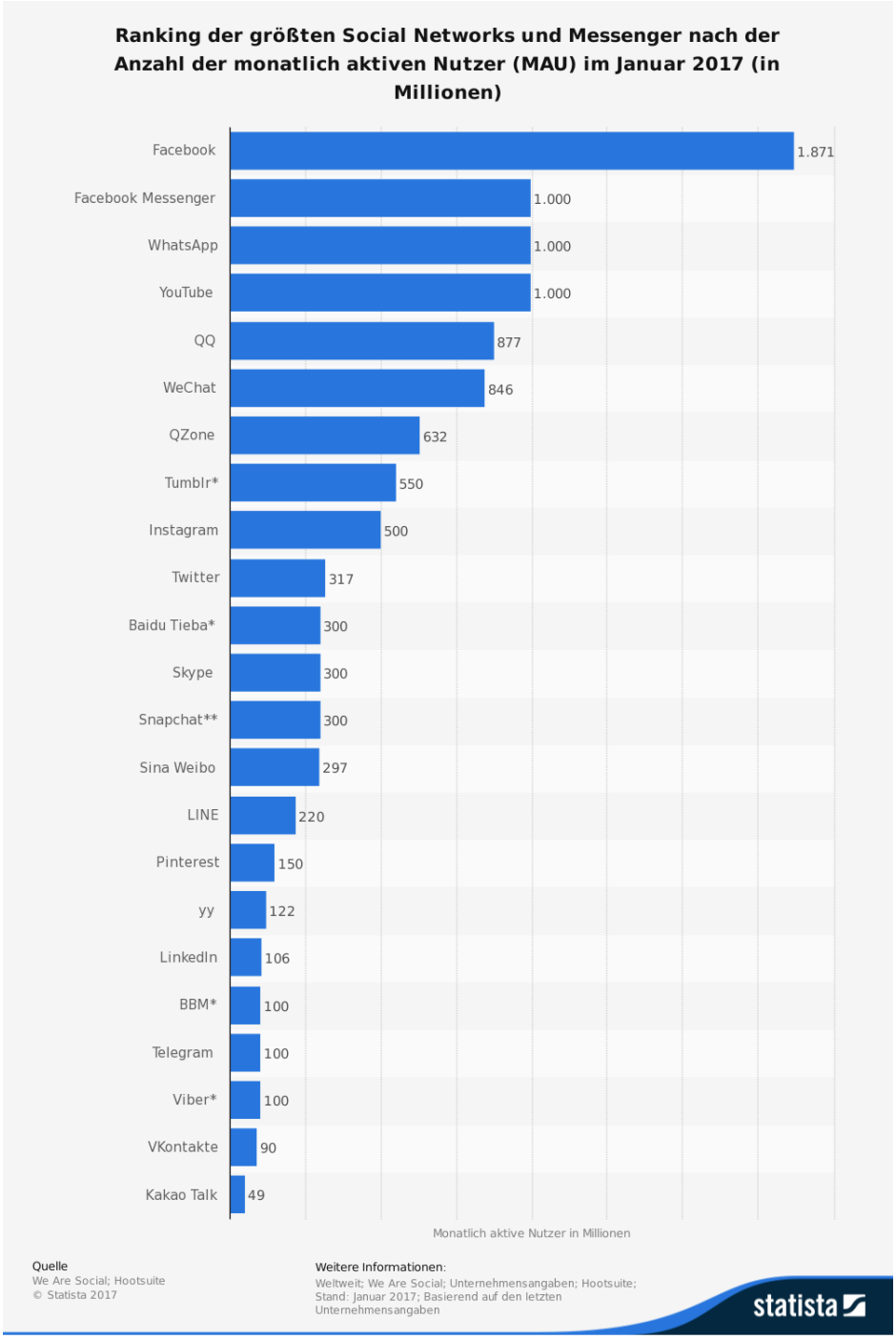

Abbildung A.1: Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im Januar 2017 (in Millionen) (enthalten in **WeAreSocial.2017**)

Ehrenwörtliche Erklärung

Wir erklären hiermit ehrenwörtlich:

- dass wir die vorliegende Arbeit mit dem Titel *Titel* selbständig verfasst und
- keine anderen als die angegebenen Quellen und Hilfsmittel benutzt haben.
- Wir versichern zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Wir sind uns bewusst, dass eine falsche Erklärung rechtliche Folgen haben wird.

Ort, Datum Sebastian Röhling und Jan Kipka