Nicole Tornow

Beurteilung des Datenschutzes anhand ausgewählter Kriterien

Guideline zum Umgang mit Datenschutzrichtlinien

Die Handhabbarkeit von Datenschutz ist ein leidiges Thema, das jeden von uns betrifft, denn oftmals scheitert unsere Motivation schon zu Beginn beim eigentlichen Durchlesen von Datenschutzrichtlinien. Der Aufwand der Einarbeitung ist meist zu abschreckend, um aufmerksam Richtlinien zu bearbeiten oder rechtliche Grundlagen zu verstehen. Aus diesem Grund ist es umso wichtiger, einen umfassenden Überblick und auch Durchblick im Interesse des Schutzes der eigenen personenbezogenen Daten zu gewähren.

Die folgende Auseinandersetzung mit der Handhabbarkeit von Datenschutz umfasste die Einarbeitung in Datenschutzgesetze sowie Datenschutzerklärungen bekannter Unternehmen. Auf dieser Grundlage wurde ein Beurteilungssystem entworfen, welches es dem Einzelnen ermöglichen soll, Datenschutzrichtlinien nach persönlich gewünschtem Schutz zu verstehen, zu bewerten und schließlich mit diesem Wissen über die Einwilligung zu entscheiden. Damit wird gleichzeitig die Frage evaluiert: *Können Datenschutzrichtlinien durch zielgerichtetes Abarbeiten von gewählten Kriterien umfassend beurteilt werden?*

1. Rechtliche und gesetzliche Grundlagen

Datenschutzrichtlinien (nach aktuellem Stand, die EU-DSGVO wird zu Änderungen führen) verweisen oft auf Gesetze, die ohne Fachwissen nicht interpretierbar sind. Nachfolgend werden Auszüge aus dem Bundesdatenschutzgesetz und der Richtlinie 95/46/EG des Europäischen Parlaments erläutert. Das Recht auf Informationelle Selbstbestimmung, im bundesdeutschen Gesetz (jedoch außerhalb des Grundgesetzes) als Datenschutz-Grundrecht verankert, beschreibt das Recht des Einzelnen, über die Freigabe und Verwendung seiner personenbezogenen Daten selbst zu entscheiden[1].

Bundesdatenschutzgesetz (BDSG)

Im Jahr 1990 wurde das *Bundesdatenschutzgesetz* verabschiedet, welches den Schutz des Einzelnen vor der Beeinträchtigung seiner Persönlichkeitsrechte im Umgang mit den eigenen personenbezogenen Daten festlegt (nach § 1 BDSG). Es umfasst dabei die Aspekte der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Besonders die im § 3 BDSG aufgeführten Begriffsbestimmungen sind notwendig, um weitere Gesetzmäßigkeiten zu verstehen. Dazu zählen unter anderem

- *personenbezogene Daten* als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" (§ 3 Abs. 1),
- *Löschen* von Daten, d.h. „Unkenntlichmachen gespeicherter personenbezogener Daten" (§ 3 Abs. 4) und
- *Anonymisieren* personenbezogener Daten, wodurch „Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand [...] einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" (§ 3 Abs. 6).

Andere Paragraphen des BDSG betreffen weitere Aspekte des Datenschutzes und verdeutlichen, auf welche konkreten Eigenschaften im Umgang mit persönlichen Daten zu achten ist. Laut § 4 Abs. 1 sind Datenerhebung, -verarbeitung und -nutzung „nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat". Hierbei gilt im Allgemeinen, dass die personenbezogenen Daten beim Betroffenen erhoben werden müssen. Ausnahmen bilden gegebene Erfordernisse durch eine vorliegende Rechtsvorschrift, eine zu erfüllende Verwaltungsaufgabe oder ein entsprechender Geschäftszweck. Die Einwilligung für Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss nach § 4a immer auf einer freien Entscheidung des Betroffenen beruhen und bedarf der Bereitstellung von ausreichend Information über den Zweck der Datenerhebung.

Werden personenbezogene Daten für eigene Geschäftszwecke erhoben, sind diese Zwecke nach § 28 konkret zu formulieren. Ein Zweck beschreibt eine zur Ausführung bzw. zum Anbieten des Dienstes für den Betroffenen erforderliche Information. § 34 verpflichtet die verantwortliche Stelle, Auskunft über zur eigenen Person gespeicherte Daten, Empfänger, an die entsprechende Daten weitergegeben wurden, und den Zweck der Speicherung zu erteilen. Die Auskunftserteilung kann verweigert werden, wenn damit Geschäftsgeheimnisse gefährdet wären, welche das Informationsinteresse des Betroffenen überwiegen.

Ist die weitere Speicherung erhobener Daten nicht mehr zulässig oder werden diese für den erforderlichen Zweck nicht mehr benötigt, sind sie nach § 35 zu löschen bzw. zu sperren, wenn der Löschung „gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen".

Die genannten Paragraphen sind keineswegs vollständig wiedergegeben, noch decken sie alle zu beachtenden Gesetze ab. Die Formulierungen wurden gezielt auf die behandelte Thematik zugeschnitten. Für eine umfangreichere Einarbeitung sind daher ebenso § 6 (Rechte des Betroffenen), § 28b (Scoring) sowie § 29 (Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung) zu beachten.

Europäische Richtlinie 95/46/EG

Die *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates*[2] wurde am 24. Oktober 1995 erlassen. Sie bezieht sich auf den Schutz personenbezogener Daten in Europa, genauer: in allen Mitgliedsstaaten des *Europäischen Wirtschaftsraumes* (EWR)[3], der die Staaten der EU sowie die EFTA-Staaten Island, Liechtenstein und Norwegen umfasst. Auch auf europäischer Ebene werden ähnliche Regelungen wie im BDSG festgelegt. So ähnelt die Gesetzgebung der Einwilligung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten der des BDSG sehr.[4]

Da die Europäische Union ein Zusammenschluss von Staaten ist, wird vor allem die Übermittlung von personenbezogenen Daten geregelt. Die Übermittlung ist unter bestimmten Bedingungen bzw. Voraussetzungen generell zulässig. Gründe dafür sind u.a. die rechtmäßige Erfüllung betroffener, im öffentlichen Interesse liegender Aufgaben (Übermittlung an Dritte) oder eine zweckmäßige Begründung und Beurteilung durch die Europäische Kommission (Übermittlung außerhalb der EU).[5]

Eine weitere Festlegung gilt der allgemeinen Speicherung von Daten und ist vor allem bzgl. Datenclouds für den Betroffenen wichtig. Cloudspeicherdienste legen Nutzerdaten nicht zwingend an einem Standort und darüber hinaus im Wohnsitzstaat des Nutzers ab. Problematisch ist, dass jegliche Speicherung von Daten außerhalb Deutschlands, respektive der EU, einem anderen Datenschutzgesetz und damit auch einem anderen Datenschutzniveau unterliegt. Die Risiken betreffen dabei nicht nur den grundlegenden Schutz vor Datenmissbrauch, sondern vor allem die Auseinandersetzung mit Datenschutzgesetzen des jeweiligen Staats. Meist werden in Verträgen der Anbieter Vereinbarungen zu Erhebung, Verarbeitung und Nutzung der Daten getroffen, die bindend für beide Vertragsseiten sind.[6]

Vom Safe-Harbor-Abkommen zum Privacy Shield Framework

Das Safe-Harbor-Abkommen war eine Vereinbarung zwischen der EU und dem Handelsministerium der USA, welches in der Zeit von 6.7.2000 bis 6.10.2015 bestand.[7] Das Abkommen regelte die Speicherung und Verarbeitung personenbezogener Daten von EU-Bürgern in den USA. Am 6.10.2015 wurde diese Vereinbarung vom Europäischen Gerichtshof für ungültig erklärt, mit der Begründung, dass im Hinblick auf die Angemessenheit des Schutzes von personenbezogenen Daten ein unzureichendes Schutzniveau vorhanden ist.[8]

Im Juli 2016 wurde von der Europäischen Kommission, dem Handelsministerium der USA und der Schweizer Verwaltung das EU-U.S. und Swiss-U.S. *Privacy Shield Framework*[9] ins Leben gerufen, welches als „Nachfolger" für das Safe-Harbor-Abkommen den Schutz personenbezogener Daten zwischen der EU resp. Schweiz und den USA regelt. Unternehmen können sich für das Framework selbst zertifizieren,[10] was bedeutet, dass die Verwendung des Frameworks auf einer freiwilligen Basis beruht und sicherstellt, dass die im Privacy Shield festgelegten Prinzipien eingehalten werden[11].

2. Festlegung der Kriterien

Auf Basis der gegebenen Gesetzesgrundlage wurden ausgewählte Datenschutzrichtlinien betrachtet, aus denen einzelne Faktoren zur Beurteilung des Schutzes personenbezogener Daten abgeleitet wurden. Anhand von Facebook[12], Amazon[13], Valve[14] und DropBox[15] ergaben sich folgende Kriterien:

Auskunftsanforderung – Das Auskunftsrecht wird in § 34 BDSG festgehalten. Die Auskunft informiert den Nutzer nicht nur über persönlich angegebene, sondern auch automatisiert gesammelte Daten. Als Kriterium wird die Erwähnung und Wahrnehmbarkeit dieses Rechts geprüft.

Die **Datenfreigabe** gilt primär dem Schutz und der Verwaltung personenbezogener Daten. Dieses Kriterium bestimmt, wie und in welcher Form die Freigabe personenbezogener Daten vom jeweiligen Dienst oder Nutzer bestimmt werden kann. Diese Vorgehensweise ist stark vom Unternehmen und dessen Geschäftsinhalt abhängig. Es gibt keine gesetzliche Vorgabe, die dieses Kriterium bestimmt. Ein ausführliches Beispiel gibt die Datenschutzrichtlinie von Facebook[12] unter dem Punkt „Wie werden diese Informationen geteilt?" vor.

Die **Einwilligung** ist in § 4a BDSG sowie Richtlinie 95/46/EG[4] verankert. Als Kriterium wird damit vor allem der Zeitpunkt und die explizite Aufforderung zur Einwilligung betrachtet.

Die **Gültigkeit der rechtlichen Grundlage** bezieht sich vor allem auf die Ereignisse des Safe-Harbor-Abkommens. Nachdem das Abkommen für ungültig erklärt wurde, war es stets Bestandteil vieler Datenschutzrichtlinien. Bis zum Zustandekommen des Privacy Shield Frameworks befanden sich daher in einem Zeitraum von acht Monaten sowohl die Betroffenen als auch die Unternehmen im Unklaren und waren aufgrund fehlender Alternativen in ihrem Handlungsspielraum eingeschränkt.

Jugendschutz – Der Schutz personenbezogener Daten von Minderjährigen besitzt eine Sonderstellung bei Erhebung, Verarbeitung und Nutzung von Daten. In den Richtlinien von Valve wird ausdrücklich erwähnt, dass „Valve […] nicht wissentlich personenbezogene Daten von Personen im Alter von 13 Jahren und darunter […]"[14] erhebt, auch Amazon gibt an, „keine Produkte zum Kauf durch Minderjährige an[zubieten]. […] [Kunden, die] das 18. Lebensjahr noch nicht vollendet haben, dürfen […] nur zusammen mit einem Elternteil oder Vormund […]"[13] Produkte erwerben. Aus rechtlicher Sicht werden jedoch innerhalb des BDSG keine Regelungen getroffen. Hierbei sind die Nutzer auf Vorgaben der Datenschutzrichtlinien zur Erhebung, Verarbeitung und Nutzung des jeweiligen Dienstanbieters angewiesen. Etwaige Maßnahmen, die im Bürgerlichen Gesetzbuch (BGB) festgehalten werden und in solchen Situationen Anwendung finden, werden hier nicht betrachtet.

Das **Löschen** personenbezogener Daten wird erforderlich, sobald eine Speicherung bzw. Ablage in irgendeiner Form erfolgt. Sowohl im BDSG als auch in den meisten Richtlinien wird dieses Kriterium thematisiert.

Sprache – Viele der heutigen Dienstleistungen werden international angeboten, daher ist eine Datenschutzrichtlinie in der eigenen Landessprache nicht selbstverständlich oder gesetzlich verankert. Die verwendete Sprache kann zum Nachteil werden, wenn eine Übersetzung nicht aktuell oder inkorrekt ist. Ein charakteristisches Beispiel dafür liefert DropBox; das Unternehmen schreibt ausdrücklich in seiner Datenschutzrichtlinie: „Diese Übersetzung wird nur zu Informationszwecken bereitgestellt. Bei Unstimmigkeiten gilt der englische Ausgangstext."[15]

Die **Transparenz** von Datenschutzrichtlinien begründet sich in einer verständlichen Erläuterung der verwendeten Methoden zur Datenerhebung, -verarbeitung und -speicherung. Im BDSG werden hierbei § 6c (Mobile personenbezogene Speicher- und Verarbeitungsmedien) im Speziellen erfasst, ebenso wird in § 28b das Verfahren des Scorings beschrieben, welches einen

„[…] Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen […]“ (§ 28b Abs. 1) ermittelt. In beiden Paragraphen werden sehr spezifische Themen bestimmt. Eine allgemeine Regel für die Auskunft über den Einsatz bestimmter Cookies o.ä. wird nicht festgehalten.

Das **Übermitteln** (Weitergabe der Daten) an Dritte ist sowohl in § 29 BDSG als auch in der Richtlinie 95/46/EG[5] verankert. Das Kriterium soll darauf aufmerksam machen, in welcher Form und aus welchen Gründen Daten weitergegeben werden (dürfen).

Verständnis – Das Verstehen der Datenschutzrichtlinie bezieht sich auf die angestrebten Nutzergruppen, Struktur und Aufbau des Textes, Eindeutigkeit sowie Erläuterungen von Fachbegriffen. Das Kriterium *Verständnis* ist jedoch schwer rechtlich festzuhalten, da eine genaue Definition von Verständnis vom jeweiligen Vorwissen abhängig ist. Es werden indirekte Angaben zur Verständlichkeit gegeben, bspw. „[…] nachvollziehbar in allgemein verständlicher Form“ (§ 34 Abs. 2 BDSG). Facebook nutzt beispielsweise eine persönliche Anrede und verwendet eine übersichtliche Struktur, die vor allem jüngeren Nutzern zu Gute kommt.[12]

Warnhinweise sind zwar kein Bestandteil von Datenschutzrichtlinien oder Datenschutzregelungen, jedoch sehr hilfreich für Nutzer mit wenig oder gar keinem informations- oder medientechnischen Vorwissen. Sie sollen die Sensibilisierung im Umgang mit personenbezogenen Daten fördern.

Zweckbindung – Der Zweck begründet die Erhebung, Verarbeitung und Nutzung von Daten und muss daher vor jeder Einwilligung bekannt sein (§ 28 BDSG). Anhand der Zweckbindung wird sichtbar, aus welchem Grund bestimmte Daten benötigt werden.

Anwendung der Kriterien auf die Datenschutzrichtlinie von Facebook

Facebook ist ein Gigant der sozialen Netzwerke. Die Datenschutzrichtlinie wird anhand der Kriterien *Löschen*, *Datenfreigabe*, *Einwilligung* und *Auskunftsanforderung* untersucht. Alle verwendeten Informationen sind, sofern nicht anders angegeben, der Facebook-Datenschutzrichtlinie[12] entnommen.

Löschen – Facebook ermöglicht jederzeit das Löschen des eigenen Kontos. Dazu gehören alle Inhalte, die mit diesem Konto verbunden sind. Jedoch können jegliche Informationen, die mit anderen Nutzern geteilt wurden, nicht immer direkt gelöscht werden. Personenbezogene Daten, die von anderen Nutzern zur Person bereitgestellt wurden, sind nicht mit dem Konto verbunden und fallen daher nicht darunter.

Datenfreigabe – Die Verwaltung der eigenen Daten wird in Facebook stark durch das Teilen von Informationen mit anderen gesteuert. Einige Informationen sind öffentliche Inhalte, die auch mit Hilfe von Suchmaschinen eingesehen werden können. Dazu gehören alle Inhalte, die mit der öffentlichen Zielgruppe geteilt werden, das *Facebook Forum* und das öffentliche Profil eines Nutzers (beinhaltet u. a. Nutzername, Altersgruppe, Geschlecht). Geteilte Informationen können durch den Nutzer, mit dem sie geteilt wurden, ebenso weiter geteilt werden. Der Nutzer selbst kann dementsprechend keinen direkten weiteren Einfluss darauf nehmen.

Einwilligung – Aufgrund meiner Recherchen habe ich die Webseite der Datenschutzrichtlinie von Facebook mehrfach verwendet. Nach mehrmaligen Aufrufen der Seite wurde ich mit der folgenden Information konfrontiert: „Cookies helfen uns dabei, Facebook-Dienste anzubieten, zu schützen und zu verbessern. Wenn du unsere Webseite weiterhin verwendest, stimmst du unserer Richtlinie zu Cookies zu.“ Damit erhebt das Unternehmen ohne meine explizite Einwilligung oder die Verwendung eines Facebook-Kontos bereits Daten.

Auskunftsanforderung – Eine persönliche Auskunftsanforderung wird von Facebook nicht angeboten. Es gibt jedoch eine automatisierte und im Account bereitgestellte Option „Deine Daten herunterladen“, die mit dem Konto verbundene Information als komprimierte Datei zusammenstellt.

Aufgrund dieser Auszüge wirft der Datenschutz bei Facebook vor allem im Bereich der Datenfreigabe und der Einwilligung einige Bedenken auf. Eine explizite Einwilligung erfolgt nicht aus freien Stücken und ist dem Nutzer unter Umständen bereits bei der Informationssammlung ein Hindernis oder Ablehnungsgrund. Des Weiteren weist die Datenfreigabe aufgrund der *Teilen*-Funktion erhebliche Gefahren für den Schutz der eigenen Daten auf. Unbedachtes Teilen einer Aussage oder eines Bildes kann damit ungeahnte Konsequenzen nach sich ziehen.

3. Beurteilungssystem für Datenschutzrichtlinien

Aufbauend auf den Kriterien habe ich ein Beurteilungssystem entwickelt, welches eine dem Nutzer vorliegende Datenschutzrichtlinie anhand von gewichteten Kriterien bewertet. Das System zielt auf eine motivierende Strategie ab, die den Betroffenen dazu anhalten soll, den Schutz seiner personenbezogenen Daten bewusst zu handhaben.

Als Basis für das Beurteilungssystem habe ich nach möglichen vorhandenen Vorgehensweisen oder Systemen recherchiert. Die meisten Ergebnisse lieferten Bewertungen spezifischer Datenschutzrichtlinien, jedoch kein umfassendes oder einheitliches System zur Bewertung einer beliebigen Richtlinie.

Nicole Tornow

Nicole Tornow hat an der Friedrich-Schiller-Universität Jena (FSU) Informatik studiert. Nach einem erfolgreichen Abschluss des Masterstudiums ist sie nun als Software-Entwicklerin im E-Commerce-Bereich tätig.

Aufbau und Arbeitsweise des Beurteilungssystems

Mein Beurteilungssystem ist dreischrittig aufgebaut: Gewichtung der Kriterien, Bewertung der Kriterien anhand einer gegebenen Datenschutzrichtlinie und Auswertung. Die Auswertung ergibt eine prozentuale Angabe, die durch farbliche Abstufung repräsentiert wird, welche die Richtlinie in ihrer Gesamtheit beurteilt.

Gewichtung der Kriterien

Für das Beurteilungssystem verwende ich nur eine kleine Auswahl der genannten Kriterien. In Tabelle 1 ist eine beispielhafte Darstellung einer benutzerdefinierten Gewichtung angegeben.

Kriterium	Gewicht g[i]	Gewichtungsfaktor w[i] = g[i] / g_max
Auskunftsanforderung	6	0,6
Datenfreigabe	10	1,0
Einwilligung	7	0,7
Löschen	9	0,9

Tabelle 1: Berechnung von Gewichtungsfaktoren

Die Gewichtung der Kriterien erfolgt durch den Nutzer nach eigenem Ermessen und Wünschen. Der maximale Wert *g_max* eines Gewichts *g[i]* beträgt 10, der minimale Wert ist 0. Wird ein Kriterium mit dem Wert 0 belegt, so geht es nicht in die Berechnung und damit nicht in die Beurteilung ein. Je höher eine Gewichtung angegeben wird, desto stärker fließt die erreichte Punktezahl der Bewertung in das Endergebnis ein.

Bewertung der Kriterien

Die Bewertung eines Kriteriums gibt an, wie gut die Datenschutzrichtlinie diesen Aspekt behandelt. Es können je Kriterium zwischen 0 und 5 Punkten vergeben werden, wobei p_max = 5 Punkte die höchste und damit beste Wertung p[i] für ein Kriterium darstellt. Tabelle 2 zeigt die Bewertung von Kriterien. Die Abstufung zwischen den Punkteniveaus könnte folgendermaßen beschrieben werden:

Das Kriterium …

0 – … wird in der Datenschutzrichtlinie nicht erwähnt oder besitzt eine gesetzwidrige oder nicht akzeptable Aussage.

1 – … ist nur unzureichend oder indirekt beschrieben. Die resultierende Aussage ist nur unter expliziter Beachtung seitens des Nutzers vertretbar. Viele Fragen bleiben offen.

2 – … ist direkt beschrieben. Es sind jedoch starke Einschränkungen vorhanden.
Beispiel: Die Datenfreigabe bei Facebook bedarf eines bewussten Vorgehens des Nutzers. Die Teilen-Funktion enthält die Gefahr, dass Daten durch weiteres Teilen öffentlich einsehbar werden und gegebenenfalls nicht vollständig gelöscht werden können.

3 – … ist direkt und ausreichend beschrieben. Es sind Einschränkungen vorhanden.

4 – … ist direkt, ausreichend und akzeptabel beschrieben. Damit verbundene Überprüfungen oder Maßnahmen sind jedoch nicht vollständig aufgezeigt. Kleinere Einschränkungen sind vorhanden.
Beispiel: Der Jugendschutz wird bei Amazon eindeutig in der Richtlinie beschrieben. Maßnahmen zur Überprüfung sind jedoch nur indirekt oder gar nicht genannt.

5 – … ist in der Datenschutzrichtlinie vollständig mit zugehörigen Maßnahmen und Regelungen beschrieben.
Beispiel: Die Auskunftsanforderung der Otto GmbH[16] ist eindeutig auf ihrer Datenschutz-Webseite sichtbar und referenziert entsprechende Paragraphen des BDSG.

Berechnung und Aussage der Bewertung

Tabelle 2 beschreibt beispielhaft die Zusammenführung der Gewichtung der Kriterien mit den für die Kriterien erreichten Punkten. Verwendet werden die Gewichtungen aus Tabelle 1. Die Farbkodierung (Färbung) richtet sich nach Tabelle 3.

Kriterium	Punkte p[i]	Gewicht w[i]	Ergebnisse p[i] × w[i]
Auskunftsanforderung	4	0,6	2,4
Datenfreigabe	2	1,0	2,0
Einwilligung	1	0,7	0,7
Löschen	3	0,9	2,7
Erreichte Punkte S = $\sum$ p[i] × w[i]			7,8
Maximal erreichbar S_max = p_max × $\sum$ w[i]			16,0
Relatives Ergebnis Q = 100 × S / S_max			48,75 %
Färbung			**ausreichend**

Tabelle 2: Gesamtauswertung

4. Bewertung der Datenschutzrichtlinie von Facebook anhand des Beurteilungssystems

Nun bewerte ich die Datenschutzrichtlinie von Facebook im vorgestellten Beurteilungssystem anhand der ausgewählten vier Kriterien. Die Gewichtung der Kriterien wurde in Tabelle 1 bereits dargestellt, die Bewertung der Kriterien in Tabelle 2 begründe ich wie folgt:

Auskunftsanforderung: 4 – Die Auskunftsanforderung wird relativ einfach für den Nutzer innerhalb dessen Accounts gelöst. Der Betroffene kann sich eine Datei mit den Daten, die mit seinem Konto verbunden sind, herunterladen. Inwiefern diese Funktion vollständig ist bzw. welche Resultate geliefert werden, kann hier nicht beurteilt werden.

Datenfreigabe: 2 – Die Datenfreigabe bei Facebook wird vor allem durch die *Teilen*-Funktion sehr unübersichtlich. Facebook beschreibt in seiner Datenschutzrichtlinie ausführlich, in welcher Form und mit welcher Auswirkung das Teilen die Handhabbarkeit der eigenen Daten beeinflusst. Der Nutzer sollte hier keinesfalls gedankenlos Informationen weitergeben.

Einwilligung: 1 – Der Besuch einer Webseite des Unternehmens aktiviert nach bestimmter Zeit Cookies, die automatisch Daten erheben, unabhängig davon, ob der Nutzer ein Facebook-Konto besitzt. Zwar werden Hinweise darauf gegeben, dass bei weiterem Nutzen der Facebook-Seite die Cookies aktiviert werden, jedoch gibt es keine explizite Einwilligung oder Ablehnung.

Löschen: 3 – Facebook ermöglicht jederzeit das Löschen des eigenen Accounts und damit verbundener Daten. Jedoch ist es nicht möglich, alle Daten zur eigenen Person vollständig zu entfernen.

Die erreichte Bewertung der Facebook-Datenschutzrichtlinie beträgt 48,75 % und ist damit im dunkelgrauen Bereich. Das bedeutet in diesem Fall, dass die Datenschutzrichtlinie zwar gut bis sehr gut aufgebaut und geschrieben ist, sich jedoch Einschränkungen für die personenbezogen Daten ergeben, die sehr gravierend sind. Insbesondere die Kriterien der Datenfreigabe und der Einwilligung zeigen aufgrund ihrer hohen Gewichtung und niedrigen Bewertung einen deutlichen Einfluss in der Berechnung.

5. Schlussfolgerung und Ausblick

Rückblickend wird deutlich, dass sowohl die Datenschutzrichtlinien als auch die Datenschutzgesetze unterschiedliche Kriterien hervorgebracht haben. Es gab auf beiden Seiten Übereinstimmungen wie die Auskunftsanforderung und das Löschen von Daten. Jedoch wurden auch Kriterien gefunden, wie der Jugendschutz, die in den Datenschutzgesetzen keine Rückendeckung erhalten. Durch die gesetzliche Vorgabe wurde deutlich, wie wichtig die Einwilligung und Zweckbindung in Bezug auf die Erhebung, Verarbeitung und Nutzung von Daten ist.

Die zu Beginn gestellte Frage kann daher nur hinsichtlich der Wiedergabe der Datenschutzrichtlinie durch den Filter der Kriterien beurteilt werden. Mit den vorgestellten Kriterien können die wichtigsten und datenschutzrechtlich relevanten Aspekte betrachtet werden. Änderungen an der Datenschutzrichtlinie können mit diesem Vorgehen nur durch ein erneutes Abarbeiten der Kriterien erfasst werden (sofern keine eindeutigen Kennzeichnungen über die Änderungen vorgenommen wurden). Zusammenfassend bilden die Kriterien eine gute Abdeckung der betrachteten Datenschutzrichtlinien, müssen jedoch im Einzelfall durch weitere Faktoren erweitert werden.

Letztendlich ermöglicht diese Vorgehensweise, den Berg an heutigen Datenschutzrichtlinien zu bewältigen. Der damit verbundene Aufwand ist für den Betroffenen dennoch sehr hoch. Die gegebenen Bewertungen der Kriterien bedürfen der Erarbeitung eines Vorwissens zumindest in datenschutzrechtlicher Sicht. Die Erfahrung und Expertise im Hinblick auf Datenschutzrichtlinien kann mit der Bearbeitung und damit aktiven Auseinandersetzung der Thematik gewonnen werden. Damit bleibt dennoch das Problem: Die Informationslast bleibt beim Betroffenen.

Das vorgestellte Beurteilungssystem stellt eine mögliche Herangehensweise zur Beurteilung von Datenschutzrichtlinien dar. Das Fokussieren auf einzelne Kriterien kann hierbei den Blick für das Wesentliche erleichtern. Die Wahl und Erweiterung der Kriterien kann sich darüber hinaus speziell an den Eigenschaften des Dienstleisters (bspw. Soziale Netzwerke, Online-Shops) orientieren und somit eine zielgerichtete Beurteilung ermöglichen.

Die Bewertung der Kriterien ist dabei der kritische Aspekt des Systems. Hierbei stellt sich die Herausforderung, entsprechende Textanalysewerkzeuge zur automatischen Beurteilung zu entwickeln. Die Idee basiert hierbei darauf, dem Nutzer möglichst viel der angesprochenen Informationslast abzunehmen und darüber hinaus für den Schutz der eigenen personenbezogenen Daten zu motivieren.

Ein Einsatz des Beurteilungssystems liegt vor allem im App-Anwendungsbereich oder als Browser-Plugin. Mithilfe einer Farbkodierung könnten damit visuelle Empfehlungen in Abhängigkeit der benutzerdefinierten Gewichtung gegeben werden.

Referenzen

1 *Datenschutz-Wiki (2016) Informationelle Selbstbestimmung. 28.4.2016, https://www.datenschutz-wiki.de/Informationelle_Selbstbestimmung*

2 *Europäische Gemeinschaften (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. Abl. L 281, 23.11.1995, S. 31, http://eur-lex.europa.eu/eli/dir/1995/46/oj*

3 *Europäische Gemeinschaften (1999) Beschluss des Gemeinsamen EWR-Ausschusses Nr. 83/1999 vom 25. Juni 1999 zur Änderung des Protokolls 37 und des Anhangs XI (Telekommunikationsdienste) zum EWR-Abkommen. ABl. L 296, 23.11.2000, S. 41, http://eur-lex.europa.eu/eli/dec/1999/83(2)/oj*

Relatives Ergebnis Q	Farbe	Bedeutung
$Q < 40\,\%$	**durchgefallen**	Die Datenschutzrichtlinie weist eindeutige Mängel auf. Von einer Einwilligung wird abgeraten.
$40\,\% \leq Q < 60\,\%$	**ausreichend**	Die Datenschutzrichtlinie ist inhaltlich ausreichend beschrieben und kann unter Beachtung der Einschränkungen akzeptiert werden.
$60\,\% \leq Q < 80\,\%$	**gut**	Die Datenschutzrichtlinie ist inhaltlich gut aufgestellt und kann unter Berücksichtigung kleinerer Einschränkungen akzeptiert werden.
$80\,\% \leq Q$	**sehr gut**	Die Datenschutzrichtlinie ist inhaltlich sehr gut aufgebaut und kann mit bewusstem Umgang akzeptiert werden.

Tabelle 3: Farbkodierung

4 *Der Europäische Datenschutzbeauftragte (2016) Berechtigte Gründe für die Verarbeitung personenbezogener Daten. https://web.archive.org/web/20160621152314/https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Dataprotection/QA/QA6 (27.5.2017)*
5 *Der Europäische Datenschutzbeauftragte (2016) Übermittlung personenbezogener Daten. https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Dataprotection/QA/QA9 (27.5.2017)*
6 *Der Europäische Datenschutzbeauftragte (2016) Cloud-Computing. https://web.archive.org/web/20160621152452/https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Dataprotection/QA/QA10 (27.5.2017)*
7 *Safe Harbor (2017) https://www.datenschutz-wiki.de/Safe_Harbor (27.5.2017)*
8 *Export.gov (2017) U.S.-EU Safe Harbor List. https://safeharbor.export.gov/list.aspx (27.5.2017)*
9 *International Trade Administration (2017) Privacy Shield Overview. https://www.privacyshield.gov/Program-Overview (27.5.2017)*
10 *International Trade Administration (2017) Self-Certification Information. https://www.privacyshield.gov/article?id=Self-Certification-Information (27.5.2017)*
11 *International Trade Administration (2017) Privacy Shield Framework. https://www.privacyshield.gov/EU-US-Framework (27.5.2017)*
12 *Facebook (2017) Datenrichtlinie. https://de-de.facebook.com/privacy/explanation (3.3.2017)*
13 *Amazon.de (2017) Amazon.de-Datenschutzerklärung. http://www.amazon.de/gp/help/customer/display.html?nodeId=3312401 (3.3.2017)*
14 *Valve (2017) Einverständnis zu den Datenschutzrichtlinien. http://store.steampowered.com/privacy_agreement/ (3.3.2017)*
15 *DropBox (2017) Dropbox-Datenschutzrichtlinien. https://www.dropbox.com/privacy (3.3.2017)*
16 *Otto (2017) Datenschutz. https://www.otto.de/shoppages/service/about/datenschutzinformation (4.3.2017)*

Sarah Schott und Claudia Sichting

Roboter im Alltag: Wer trägt Verantwortung bei Schutzbefohlenen?

Roboter, die mit Kindern spielen, im Alltag helfen und auf Gefühle reagieren: das ist doch Science-Fiction! Warum sollten wir uns da schon jetzt mit dem Datenschutz befassen? Die französische Firma Aldebaran[1], eine Tochterfirma von SoftBank Robotics, bietet bereits einen solchen Roboter mit Namen Pepper für Privatpersonen in Japan an und will das Angebot schrittweise auf andere Länder ausdehnen. Somit ist jetzt der gebotene Zeitpunkt, die Fähigkeiten der Roboter auszuloten und bei Bedarf das Datenschutzrecht anzupassen. Wartet man erst, bis sich die Entwicklung auch in Europa durchgesetzt hat, wird zwischenzeitlich oder auf lange Sicht der Schutz der Privatsphäre riskiert.

1. Roboter

Nur 1,20 m bzw. 1,40 m groß, mit Kunststoffgehäuse und comichaftem Gesicht sind die beiden *Aldebaran*-Modelle *Pepper* und *Romeo* deutlich als humanoi… *per* (siehe Abbildung 1) soll, mit… in einem Gespräch, der Unterhal… und in familiärer Umgebung eing… *MEO*-Forschungsprojektes es, einen Roboter zu entwickeln, der Personen mit eingeschränkter Selbstständigkeit im Alltag unterstützt.[4]

Für die Bewältigung ihrer Aufgaben verfügen beide über eine Vielzahl an Sensoren, darunter Mikrophone, diverse Kameras, Ultraschall-, Beschleunigungs-, und Drucksensoren. *Pepper* ist konstant mit dem Internet verbunden, um Informationen wie passende Gesprächsantworten aus einer Datenbank, neue Programme und Updates abrufen zu können. Im Gegensatz dazu scheint *Romeo* auf einen lokalen Speicher beschränkt zu sein, denn ein wichtiger Teil der Forschung widmet sich verschiedenen Lernmethoden und Erinnerungsmechanismen, die die Bedeutung von Informationen bestimmen und diese dann komprimieren, verknüpfen, speichern oder vergessen.

Im Folgenden haben wir die von den Entwicklern angestrebten Aufgaben[2,3,4] der Roboter und die zugehörigen Daten mit besonderer Relevanz für den Datenschutz gelistet:

- Identifikation von Geräuschquellen und audiovisuelles Tracking
- Betreten oder Verlassen des Raums durch Personen
- Gesichtserkennung und Sprecheridentifizierung
- …chen und optimale Anpassung an
- …en wie Tagesablauf und Einkaufs-
- Feststellen ungewöhnlicher Situationen und entsprechendem Handlungsbedarf (Information Notfalldienst)
- Alltagsmanagement (beinhaltet medizinische Daten)
- Führen von Alltagsgesprächen und Erkundigung nach Befinden
- Unterstützung bei Verarbeitung klinischer Informationen
- Vermeiden von Langeweile und Isolation durch Anregung zu sozialer Interaktion mit anderen Menschen
- Erhalt intellektueller Aktivität durch Spiele
- Verstehen und Befolgen von Anweisungen
- Erkennen und Analysieren individueller Verhaltensweisen
- Charakterisierung von Verhalten und Interaktionen
- Erkennung von Emotionen, generellem Aktivitätslevel
- Uhrzeit und Datum bei Verknüpfung mit anderen Informationen

Bisher werden *Romeo*-Prototypen erst in der Forschung eingesetzt, für unsere Analyse unterstellen wir Marktverfügbarkeit.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de