MARKTWÄCHTER
DIGITALE WELT

verbraucherzentrale

SOZIALE MEDIEN UND DIE EU-DATENSCHUTZGRUNDVER-ORDNUNG - TEIL I

Informationspflichten und datenschutzfreundliche Voreinstellungen

Eine Untersuchung der Verbraucherzentralen – September 2018

INHALT:

Abbildungen:

Tabellen:

ZUSAMMENFASSUNG

In der vorliegenden Marktanalyse wurde untersucht, wie Anbieter Sozialer Medien mit ausgewählten Regelungen der DSGVO umgehen. Ein besonderer Fokus der Prüfung lag auf den Informationspflichten der Anbieter sowie auf der Regelung zu datenschutzfreundlichen Grundeinstellungen. Untersucht wurde dies für die Dienste *Facebook*, *Instagram*, *LinkedIn*, *Pinterest*, *Snapchat*, *Twitter*, *WhatsApp* und *YouTube (Google)*.

Nutzer können sich nicht ausreichend informieren. In Bezug auf die Informationspflichten wurde festgestellt, dass die betreffenden Anbieter in Bezug auf die Prüfpunkte (Zweck, Rechtsgrundlage, Empfänger, Dauer der Speicherung, Betroffenenrechte) in der überwiegenden Anzahl der Fälle nicht ausreichend informieren. Aus Perspektive des Verbraucherschutzes muss daher bemängelt werden, dass Nutzer anhand der geprüften Datenschutzerklärungen nicht ausreichend Kenntnis darüber erlangen können, welche Daten von ihnen und gegebenenfalls ihren Kontakten verarbeitet werden und wie sie sich vor unerwünschter Datenverarbeitung schützen können.

Nutzern wird die Kontrolle über ihre Daten erschwert. Im Zuge der Account-Registrierung wurden vier Bereiche identifiziert, die in Zusammenhang mit der Regelung datenschutzfreundlicher Voreinstellungen stehen (Authentifizierung, Kontaktsynchronisation, personalisierte Werbung, Sichtbarkeit und Auffindbarkeit). So sind Nutzer-Beiträge in mehreren Fällen per Voreinstellung öffentlich sichtbar. Die geprüften Apps fordern überwiegend zur Synchronisation der Nutzer-Kontakte auf. Auffällig sind die Anzahl und Formulierungen einiger Aufforderungen, die dem Nutzer suggerieren, die Synchronisation der Kontakte sei erforderlich für die Nutzung des Dienstes. Bei der Kontaktsynchronisation könnten unfreiwillig auch Kontaktdaten von Nutzern an Anbieter übermittelt werden, die sich bewusst gegen die Nutzung des Dienstes entschieden haben. Es gibt kaum eine Möglichkeit, das Ausmaß des Nutzer-Trackings zu kontrollieren. Stattdessen wird teilweise die Option geboten, die Nutzung von Tracking-Daten für die Personalisierung von Werbung einzuschränken.

Wesentliche Mängel festgestellt. Zusammenfassend offenbart die vorliegende Marktanalyse wesentliche Probleme in Bezug auf den Umgang von Anbietern Sozialer Medien mit Vorschriften der DSGVO: Auch nach dem 25.05.2018 bleiben auf Basis der Datenschutzerklärungen wesentliche Aspekte der Datenverarbeitung intransparent für den Nutzer. Hierdurch sowie durch die offenbarten Probleme im Bereich der datenschutzfreundlichen Voreinstellungen wird es Nutzern erschwert, die Kontrolle über ihre personenbezogenen Daten zu behalten.

1 HINTERGRUND

1.1 Soziale Medien

Der Begriff *Soziale Medien* umfasst digitale Dienste, die es Nutzern erlauben, sich mit anderen Personen zu vernetzten, Inhalte mit ihnen zu teilen und miteinander zu kommunizieren.[1] Integraler Bestandteil von unterschiedlichsten Arten Sozialer Medien ist in der Regel ein Nutzerprofil, in dem Informationen zur eigenen Person hinterlegt werden. Darüber hinaus können Beiträge mit Einzelpersonen, Personenkreisen oder dem ganzen Netzwerk geteilt werden. Diese Beiträge können Text-, Bild-, Video- oder Audio-Dateien enthalten.

Die Bedeutung solcher Dienste für Verbraucher[2] in Deutschland ist groß: So sind aktuell bereits 80 Prozent der deutschen Internetnutzer ab 14 Jahren in Sozialen Netzwerken angemeldet.[3] Jeder dritte Befragte gibt überdies an, sich ein Leben ohne Soziale Medien nicht mehr vorstellen zu können.[4]

Gleichzeitig gehen mit der Nutzung Sozialer Medien Probleme einher, da die Verarbeitung der hierdurch entstehenden personenbezogenen Daten in Zusammenhang mit einer großflächig stattfindenden, industriellen Datensammlung und -analyse betrachtet werden muss.[5]

Diese Datensammlung und -auswertung wird neben einer Reihe von damit zusammenhäng-enden Phänomenen unter dem Schlagwort *Big Data* zusammengefasst.[6] Durch Algorithmen basierte Analysen der erhobenen Daten werden weitreichende Rückschlüsse auf die betroffenen Verbraucher möglich. Beispielsweise wurde bereits demonstriert, dass alleine die Fotos auf *Instagram* Indikatoren für depressive Verstimmungen der Nutzer enthalten können.[7] Zusammengeführt mit weiteren Daten stellen derlei Informationen intimes Wissen über den Verbraucher bereit. Dieses ist die Basis für die derzeit verbreiteten datengetriebenen Geschäftsmodelle, nämlich für die Berechnung von Risiko Scores und die Personalisierung von Werbung.[8] Beide Geschäftsmodelle bieten unter anderem Raum für Diskriminierung und gezielte Manipulation der betroffenen Personen. So wurde beispielsweise berichtet, dass *Facebook* die

[1] Vgl. Scheffler, 2014, S. 13.
[2] Aus Gründen der besseren Lesbarkeit wird in der vorliegenden Arbeit mit „Verbraucher“ eine verkürzte geschlechtsneutrale Formulierung verwendet. Der Text richtet sich daher sowohl an Verbraucherinnen als auch an Verbraucher. Diese Formulierungsregel gilt für die gesamte vorliegende Arbeit (z. B. auch in Bezug auf die Verwendung des Begriffs „Internet-Nutzer“).
[3] Bitkom Research, 2018, S. 2.
[4] Vgl. ebd.
[5] Moll, Scheibel & Rusch-Rodosthenous, 2017.
[6] Vgl. z. B. Boyd & Crawford, 2012; Gandomi & Haider, 2015.
[7] Reece et al., 2017.
[8] Christl, 2017.

emotionale Verletzlichkeit von Jugendlichen in Echtzeit auswertet, um ihnen in besonders vulnerablen Momenten eine passende Werbeanzeige schalten zu können.[9]

Ob und in welcher Art und Weise persönliche Daten von Nutzern gesammelt, gespeichert, verarbeitet und weitergeleitet werden, entzieht sich in der Regel der Kontrolle des jeweiligen Verbrauchers. Erst durch Fälle wie dem Cambridge Analytica-Datenskandal wird deutlich, welches Manipulationspotenzial Sozialen Medien inhärent ist.[10] Die öffentliche Empörung über diese Vorkommnisse zeigt zudem, dass sowohl die Geschäftsmodelle als auch deren Umsetzung wenig transparent sind. Derlei Ereignisse spiegeln sich auch in den Ansichten von Verbrauchern wieder. So zeigt eine repräsentative Befragung aus dem Jahr 2018 beispielsweise, dass das Vertrauen in Soziale Medien deutlich geringer ist als das Vertrauen gegenüber klassischen Medienangeboten. Jeder Zweite in Deutschland lehnt eine Datenweitergabe durch Anbieter Sozialer Medien ab.[11] Diese Besorgnis bildet auch das Frühwarnnetzwerk des Marktwächters Digitale Welt ab.[12] Im Jahr 2018 (Januar bis August) sind zum Thema Soziale Medien bislang Fälle aus acht verschiedenen Bundesländern eingegangen, die in vielen Fällen Meldungen zu Datenschutzproblemen bei Dienste-Anbietern wie *Facebook*, *WhatsApp*, *Instagram* oder *Snapchat* enthielten. Darüber hinaus sind unzureichend beantwortete Auskunfts- oder Löschanfragen auch in Bezug auf andere Dienste regelmäßige Beschwerdegründe.

1.2 Die DSGVO in der vorliegenden Untersuchung

DSGVO. Seit dem 25. Mai 2018 wird die Datenschutzgrundverordnung (DSGVO) der Europäischen Union (EU) angewendet und löst damit die EU-Richtlinie 95/46/EG und die darauf aufbauende einzelstaatliche Datenschutzregelung des Bundesdatenschutzgesetzes in der alten Fassung (BDSG a. F.) nach einer zweijährigen Übergangsphase ab. Bis zu diesem Stichtag mussten die in der DSGVO getroffenen Regelungen von allen Dienste-Anbietern umgesetzt sein, die personenbezogene Daten verarbeiten – das trifft auch auf viele Angebote Sozialer Medien zu (vgl. Abschnitt 1.1).[13]

[9] Dachwitz, 2017.
[10] S. z. B. Meyer, 2018.
[11] PricewaterhouseCoopers GmbH (PwC), 2018. In einer im Mai 2018 stattgefundenen bevölkerungsrepräsentativen Onlinepanelbefragung von PwC wurden 1.000 Personen ab 18 Jahren zu dem Thema „Vertrauen in Medien“ befragt.
[12] Beim Frühwarnnetzwerk handelt es sich um ein Erfassungs- und Analysesystem für auffällige Sachverhalte aus der Verbraucherberatung. Grundlage stellt eine ausführliche Sachverhaltsschilderung durch Beratungskräfte der Verbraucherzentralen dar, die eine Kategorisierung sowie eine anschließende qualitative Analyse ermöglicht.
[13] Ausgenommen hiervon können beispielsweise bestimmte Arten von Blogs sein, sofern man diese in die Kategorie der Sozialen Medien zählt. Wird ein Blog lediglich zu privaten oder familiären Zwecken betrieben, findet die DSGVO keine Anwendung (Art. 2 Abs. 1 lit. c DSGVO).

Durch das in der Verordnung verankerte *Marktortprinzip* finden die Vorschriften auch auf Unternehmen Anwendung, die nicht in der EU niedergelassen sind, wenn eine Datenverarbeitung dazu dient, in der EU ansässigen Personen Waren oder Dienstleistungen anzubieten.

Allerdings ist der Regelungsgehalt einiger Vorschriften unklar, sodass sich Auslegungsspielräume für ihre Umsetzung ergeben. Entsprechend stellt sich die Frage, wie Anbieter Sozialer Medien mit den Regelungen der DSGVO derzeit umgehen.

Ziel der vorliegenden Marktanalyse ist es, zunächst eine Bestandsaufnahme zum Umgang von Anbietern Sozialer Medien mit Vorschriften der DSGVO zu machen. Im Fokus sollen zunächst zwei Regelungen der DSGVO stehen, die dem Verbraucher mehr Kontrolle über seine persönlichen Daten einräumen sollen.[14]

Informationspflichten. Eine Erweiterung der Informationspflichten des Anbieters gegenüber seinen Nutzern soll den Betroffenen die Verarbeitung ihrer Daten verständlicher machen. Betroffene sollen hierdurch besser einschätzen können, welches Ausmaß die Datenverarbeitung haben wird und welche Konsequenzen sich hieraus ergeben. So muss beispielsweise nach Vorgabe der DSGVO die Rechtsgrundlage der Datenverarbeitung oder die Dauer der Speicherung angegeben werden. In der vorliegenden Marktanalyse wird untersucht, inwieweit Anbieter Sozialer Medien derzeit diesen erweiterten Informationspflichten nachkommen (Forschungsfrage 1). Hierzu wurden aus den Vorgaben der DSGVO (Art. 13) Prüfpunkte abgeleitet, anhand derer die Datenschutzerklärungen von acht Anbietern Sozialer Medien geprüft wurden (Kapitel 3).

Datenschutz per Grundeinstellung. Als wesentliche Neuerung enthält die DSGVO das Konzept des Datenschutzes durch Technik (*Privacy by design*) und der datenschutzfreundlichen Voreinstellungen (*Privacy by default*).[15] Gerade der Grundsatz der datenschutzfreundlichen Voreinstellungen (Art. 25 Abs. 2 DSGVO) unterstützt Verbraucher dabei, die Kontrolle über ihre Daten zu erhalten. Die Voreinstellungen der Dienste müssen nach dieser Regelung nämlich standardmäßig so konfiguriert sein, dass eine datenschutzfreundliche Einstellung automatisch aktiv ist.[16]

---

[14] Über die nun folgenden Punkte hinaus wird die Kontrolle von Verbrauchern über ihre eigenen Daten auch durch weitere Betroffenenrechte gestärkt. So wurde z. B. das Auskunftsrecht der Betroffenen um weitere wichtige Informationen ergänzt. Eine Vorschrift, die das deutsche und europäische Datenschutzrecht bislang nicht vorgesehen hat, ist das Recht auf Datenübertragbarkeit (*Datenportabilität*). Betroffene können vom Verantwortlichen die Herausgabe der eigenen Daten fordern, um diese im Rahmen eines anderen Dienstes zu nutzen.

[15] Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841, 1846.

[16] Hartung in Kühling/Buchner Datenschutz-Grundverordnung/BDSG Art. 25 Rn. 24.

Allerdings lässt die DSGVO offen, was als datenschutzfreundliche Einstellung gilt. Daher wird in der vorliegenden Marktanalyse untersucht, wie Anbieter Sozialer Medien mit den Vorschriften der DSGVO zu datenschutzfreundlichen Voreinstellungen derzeit umgehen (Forschungsfrage 2). Hierzu wird bei acht verschiedenen Diensten erfasst, welche datenschutzrelevanten Einstellungsoptionen in den jeweiligen Dienst integriert sind und wie diese Optionen vorkonfiguriert sind (Kapitel 4).

Tabelle 1. Forschungsfragen und Methoden.

Wie setzen Anbieter Sozialer Medien ausgewählte Vorschriften der DSGVO um?			
Forschungsfrage		**Methode**	**Kapitel**
1	Inwieweit kommen Anbieter Sozialer Medien derzeit den durch die DSGVO vorgegebenen Informationspflichten nach?	Prüfung der Datenschutzerklärungen	3
2	Wie gehen Anbieter Sozialer Medien derzeit mit den Vorschriften zu datenschutzfreundlichen Voreinstellungen (*Privacy by default*) um?	Prüfung des Registrierungs- und Nutzungsprozesses	4

2 METHODE

2.1 Auswahl der Dienste

Für die Auswahl der Dienste Sozialer Medien wurde in erster Linie deren Marktrelevanz berücksichtigt. Diese wurde anhand von Nutzungszahlen aus verschiedenen repräsentativen Umfragen im deutschsprachigen Raum ermittelt.[17] Da Soziale Medien vorwiegend als mobile Anwendungen genutzt werden,[18] wurden darüber hinaus Downloadstatistiken von Apps in den Kategorien „Kommunikation“ und „Sozial“ berücksichtigt.[19] Von ihrer Marktrelevanz ausgehend umfasst die Auswahl eine möglichst breite Palette an Angebotsarten; abschließend wurden acht Angebote ausgewählt:

Facebook gehört mit 2,34 Milliarden Nutzern weltweit zu den größten Sozialen Netzwerken. Allein in Deutschland gab es im Jahr 2017 23 Millionen täglich aktive Nutzer.[20] *Facebooks* Umsatz durch personalisierte Werbeanzeigen betrug im Jahr 2017 über 40 Millionen US-Dollar.[21] Neben der *Facebook*-Plattform und der Messenger-App gehören auch *Instagram* und *WhatsApp* zur *Facebook* Unternehmensgruppe.

WhatsApp gehört seit 2014 zur *Facebook*-Unternehmensgruppe. *WhatsApp* ist ein Instant-Messenger-Dienst, der in erster Linie der privaten Kommunikation zwischen Einzelpersonen oder (überschaubaren) Personengruppen dient. Der Dienst unterstützt neben klassischen Textnachrichten auch Dateiformate wie Audio oder Video. Weltweit gibt es 1,5 Milliarden aktive *WhatsApp*-Nutzer.[22] Täglich werden bis zu 65 Milliarden *WhatsApp*-Nachrichten verschickt.[23]

Instagram zählt seit August 2012 zur *Facebook*-Unternehmensgruppe. Im Jahr 2018 gab es weltweit eine Milliarde aktive *Instagram*-Nutzer.[24] Der Dienst ist eine Multimedia-Plattform, auf welcher in erster Linie Fotos und Videos geteilt, aber auch private Nachrichten ausgetauscht werden können. *Instagram* hat mit der Einführung sogenannter „*Instagram* Stories“ seine Funktionen erweitert: Stories können Videos oder Bilder sein, die nach 24 Stunden automatisch gelöscht werden.

[17] Bitkom, 2016a; 2016b; Koch & Frees, 2017; Feierabend, Plankenhorn & Rathgeb, 2017; Statista Dossier, 2017.
[18] S. z. B. Bitkom e. V., 2018, S. 8.
[19] Appannie.com; die kriteriengeleitete Auswahl nach App-Rankings wurde analog zu verschiedenen wissenschaftlichen Untersuchungen getroffen, z. B. Ackerman, 2013; Herrmann & Lindemann, 2016.
[20] Statista, 2018a, s. https://de.statista.com/statistik/daten/studie/711113/umfrage/nutzerzahlen-von-facebook-in-deutschland/.
[21] Statista, Dossier, 2017, S. 15.
[22] Statista, 2018b, s. https://de.statista.com/themen/1995/whatsapp/.
[23] Ebd.
[24] Statista, 2018c, s. https://de.statista.com/themen/2506/instagram/.

LinkedIn ist eine Netzwerk-Plattform und dient der beruflichen und privaten Pflege von Kontakten. Nutzer können ein Profil von sich erstellen, private Interessen und berufliche Erfahrungen angeben und mit anderen Nutzern oder Unternehmen kommunizieren. Der Umsatz des Karrierenetzwerks speist sich aus den Mitgliedsbeiträgen von Nutzern der sogenannten Premium-Funktionen[25] sowie dem Verkauf von Onlinewerbung und Personalbeschaffungslösungen. Weltweit verzeichnet *LinkedIn* nach eigenen Angaben 546 Millionen Mitglieder.[26] Im Jahr 2016 hat *Microsoft* das Unternehmen gekauft.

Pinterest kann in der Angebotskategorie Sozialer Medien in das sogenannte Social-Bookmarking eingeordnet werden. Social-Bookmarking-Anwendungen helfen, Informationen zu ordnen und auffindbar zu machen. Bei *Pinterest* können Nutzer sogenannte Pinnwände erstellen, auf denen sie Links thematisch sortiert abspeichern können. *Pinterest* wurde 2010 gegründet und verzeichnete im September 2017 200 Millionen Nutzer weltweit.[27]

Snapchat ist ein Instant-Messenger-Dienst, dessen Kern das Teilen von Fotos und Videos ist (sog. *Snaps*). Nutzer können einzelne oder eine Aneinanderreihung von Snaps (Stories) erstellen und an Freunde senden. Die Bilder und Videos werden gelöscht, nachdem der Kommunikationspartner den Inhalt gesehen hat. Über die „Memories"-Funktion können Snaps und Stories jedoch auch dauerhaft gespeichert werden – entweder lokal oder auf den Servern von *Snapchat*. Eine Haupteinnahmequelle von *Snapchat* besteht in dem Schalten von Werbung. Täglich sind es 191 Millionen Menschen weltweit, die *Snapchat* aktiv nutzen (Stand 2017).[28] *Snapchat* wird insbesondere von Jugendlichen und jungen Erwachsenen im Alter von 14 bis 29 Jahren genutzt.

Twitter ist ein Mikroblogging-Dienstleister und wurde 2006 gegründet. Privatpersonen, (öffentliche) Organisationen und Unternehmen können dort innerhalb von 280 Zeichen eine Nachricht veröffentlichen. *Twitter* hat monatlich 330 Millionen aktive Nutzer weltweit.[29] Der größte Teil seines Umsatzes wird durch das Anzeigengeschäft erwirtschaftet.

YouTube ist eine Multimedia-Plattform, die es Nutzern ermöglicht, unbewegte und bewegte Bilder, Töne und Texte zu veröffentlichen. *YouTube* hat in Deutschland ca. 6 Millionen Nutzer – weltweit kann das Unternehmen 1,5 Milliarden aktive Nutzer verzeichnen und zählt damit zu einer

[25] *LinkedIn* bietet kostenpflichtige Mitgliedschaften an, die verschiedene Funktionen und Angebote beinhalten, bspw. für Jobsuchende („Premium Career"), Vertriebsfachkräfte („Recruiter Lite") oder aber allgemein für die Personalgruppe eines Unternehmens („Premium Business").
[26] S. LinkedIn.de, https://about.linkedin.com/de-de.
[27] Statista Dossier, 2017, S. 7.
[28] Statista Dossier, 2017, S. 27.
[29] Statista, 2018d, s. https://de.statista.com/themen/99/twitter/.

der größten Multimedia-Plattformen der Welt.[30] *YouTube* ist seit 2006 eine Tochtergesellschaft des US-amerikanischen Unternehmens *Google*.

2.2 Durchführung

Material. Die vorliegende Studie wurde App-basiert mit Hilfe eines mobilen Android-Endgeräts durchgeführt.[31] Dies bildet die Realität der Verbraucher bei der Nutzung Sozialer Medien ab. So gaben in einer repräsentativen Befragung des BITKOM e. V. 82 Prozent der Befragten an, dass sie Soziale Netzwerke über mobile Endgeräte aufrufen.[32] Das Betriebssystem Android hat im Vergleich zu iOS einen höheren Marktanteil.[33]

Im Vorfeld der Untersuchung wurden für die Account-Erstellung zwei E-Mail-Adressen eingerichtet. Für die Nutzung des Google Play Store und anderer wesentlicher Funktionen des Android-Smartphones war die Einrichtung einer GMail-Adresse erforderlich. Zusätzlich wurde eine web.de-Adresse erstellt. Diese wurde bei Diensten verwendet, die eine Single Sign-on-Möglichkeit über Google anboten (s. Tabelle 2).[34]

Dokumentation und Auswertung. Die Account-Erstellung fand zwischen dem 15.06. und 04.07.2018 statt (Erhebungszeitraum) und wurde mit Hilfe von ScreenVideos dokumentiert.[35] Die Videos zeigen den Installationsprozess, die Registrierung samt aller Daten-Abfragen, die Verlinkungen zu Nutzungsbedingungen und Datenschutzerklärungen sowie die üblicherweise zusätzlich bereit gestellte Cookie-Richtlinie und Community-Regeln. Diese Dokumente wurden zusätzlich in ausdruckbare Word-Dokumente kopiert. Hierbei wurden auch Inhalte aus Hyperlinks berücksichtigt (s. Kapitel 4). Die Auswertung des dokumentierten Materials enthält Beobachtungen und Bewertungen, die unter Berücksichtigung der Perspektive des Verbrauchers erfasst und vorgenommen wurden. Die Bewertungen geben die Ansicht der Mitarbeiter im Projekt Marktwächter Digitale Welt der Verbraucherzentrale NRW wieder.

---

[30] Statista, 2018e, s. https://de.statista.com/themen/162/youtube/.
[31] Huawei P8 lite 2017, Android 7.0.
[32] Bitkom e. V., 2018, S. 8. In einer repräsentativen Befragung von Bitkom Research wurden 1.011 Social Media-Nutzer (ab 14 Jahren) gefragt, welche Geräte sie nutzen würden, um auf ihre Sozialen Netzwerke zuzugreifen. Hierbei standen Smartphone, Laptop, Desktop-PC, Tablet-Computer und Smart-TV zur Auswahl.
[33] Der Marktanteil des jeweiligen Betriebssystems ergibt sich aus den weltweiten Verkaufszahlen von Smartphones in den Jahren 2009 bis 2017, s. Statista, 2018f.
[34] Single Sign-on (SSO) ist ein Verfahren, bei dem sich Nutzer mit einem Account bei verschiedenen Diensten anmelden können, z. B. mit dem *Google*-Account bei *Pinterest*. In der Regel findet bei der Nutzung von SSO ein Datenaustausch zwischen den beiden beteiligten Webdiensten statt. Da *Google* Bestandteil der vorliegenden Untersuchung war, sollte ein solcher Datenaustausch vermieden werden; s. z. B. https://www.datenschutz-notizen.de/facebook-login-was-sagt-der-datenschutz-zum-single-sign-on-2710695/.
[35] AZ Screen Recorder, Version 5.0.3; in Einzelfällen wurden Nachtestungen durchgeführt, die ebenfalls dokumentiert wurden. Die Accounts wurden von Mitarbeitern im Projekt Marktwächter Digitale Welt der Verbraucherzentrale NRW erstellt. Für die Erstellung der E-Mail-Accounts sowie für die Accounts aller geprüften Social Media-Dienste wurden inhaltsgleiche Angaben einer fiktiven Person verwendet (u. a. Name, Geburtsdatum, Wohnort, Beruf).

Tabelle 2. Installierte Social Media-Apps.

App	Version	zuletzt aktualisiert	verwendet zur Anmeldung
Facebook	175.0.0.40.97	05.06.2018	E-Mail (gmail)
Instagram	49.0.0.15.89	11.06.2018	E-Mail (web.de)
LinkedIn	4.1.186	11.06.2018	E-Mail (web.de)
Pinterest	6.70.0	15.06.2018	E-Mail (web.de)
Snapchat	10.34.5.0	14.06.2018	E-Mail (gmail)
Twitter	7.49.0	11.06.2018	E-Mail (gmail)
WhatsApp	2.18.177	06.06.2018	Mobilfunknummer
YouTube/ Google	13.22.54	07.06.2018	E-Mail (gmail)[a]

3 ÜBERPRÜFUNG DER INFORMATIONSPFLICHTEN

Hintergrund und Prüfpunkte. Anbieter Sozialer Medien treffen vor der erstmaligen Verarbeitung von personenbezogenen Daten umfangreiche Informationspflichten gegenüber den Betroffenen.[36] Die Informationspflichten, die auch zu einer transparenten Verarbeitung notwendig sind, umfassen unter anderem die Angabe des Zwecks, der Rechtsgrundlage sowie die Aufklärung über die dem Betroffenen zustehenden Rechte. Mit Geltung der DSGVO treffen die Unternehmen im Vergleich zum BDSG weitergehende Informationspflichten, die in Art. 13 Abs. 1 DSGVO spezifiziert werden. Die Informationspflichten dienen nach Art. 13 Abs. 2 auch der Gewährleistung einer *fairen und transparenten Verarbeitung von personenbezogenen Daten*. Dies bedeutet, dass eine Unterrichtung der betroffenen Person nicht nur über die Existenz des Verarbeitungsvorganges, den Verantwortlichen und seine Zwecke (vgl. Erwägungsgrund 60) zu erfolgen hat, sondern darüber hinaus auch über verschiedene weitere mit der Verarbeitung zusammenhängende Absichten und Rechtsfolgen.[37] Verbraucher sollen also durch die gegebenen Informationen die Verarbeitung ihrer personenbezogenen Daten einschätzen und einordnen sowie ihre damit im

[36] D. h. diejenigen Personen, die von der Erhebung personenbezogener Daten betroffen sind.
[37] Paal/Pauly, DSGVO BDSG, 2. Auflage 2018, Rn. 4.

Zusammenhang stehenden Rechte erkennen können. In der vorliegenden Untersuchung wurde insbesondere die Unterrichtung der Betroffenen über die folgenden Aspekte geprüft:[38]

- Zweck und Rechtsgrundlage der Datenverarbeitung (Art. 13 Abs. 1 lit. c DSGVO): Anhand dieser Angaben sollen Verbraucher einordnen können, warum ein Unternehmen berechtigt sein soll, ihre Daten zu verarbeiten und welche Reichweite die Datenverarbeitung hat. Konsequenz könnte sein, dass Verbraucher daraufhin eine möglicherweise erteilte Einwilligung widerrufen oder gar nicht erst erteilen. Insbesondere die Nennung der Rechtsgrundlage ist eine Neuerung im Vergleich zum Bundesdatenschutzgesetz (BDSG).
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (Art. 13 Abs. 1 lit. e DSGVO): Der Verantwortliche muss den Betroffenen darüber informieren, wer die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten sind. Hier liegt eine Erweiterung im Vergleich zum BDSG vor, da diese Informationen nach der DSGVO ohne Einschränkung mitgeteilt werden müssen. Im BDSG war dies nur erforderlich, soweit der Betroffene nicht mit einer Übermittlung seiner Daten rechnen musste.
- Dauer der Speicherung der personenbezogenen Daten (Art. 13 Abs. 2 lit. a DSGVO): Die Angabe über die Dauer der Speicherung der personenbezogenen Daten informiert Verbraucher darüber, wie lange das Unternehmen die Daten behalten darf. Dies ist eine Neuerung im Vergleich zum BDSG.
- Aufklärung über die grundlegenden Betroffenenrechte (Art. 13 Abs. 2 lit. b DSGVO): Die Angaben zu Betroffenenrechten informieren Verbraucher über die ihnen zustehenden Rechte, die von ihnen ausgeübt werden können. Hierzu zählen beispielsweise das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art.16 DSGVO) oder Löschung der eigenen Daten (Art. 17 DSGVO). Erst die Wahrung der Informationspflichten aus Art. 13 Abs. 2 lit. b versetzt Verbraucher in die Lage, ihre Rechte auch ausüben zu können und damit die Kontrolle über ihre Daten zu erhalten.

Vorgehen. Anbieter informieren ihre Nutzer über den Umgang mit den erhobenen Daten in der Regel in ihren Datenschutzerklärungen.[39] Da Nutzer schon vor der ersten Datenerhebung informiert werden müssen, wurden die Datenschutzerklärungen der betreffenden acht Anbieter im

[38] Auf die Überprüfung der Informationspflicht bezüglich der Datenübertragung in ein Drittland (Art. 13 Abs. 1 lit. f) wurde verzichtet, da im Rahmen dieser Untersuchung keine vollständige Kenntnis über die dafür relevanten Datenverarbeitungsvorgänge erlangt werden konnte.

[39] Für derlei Informationen werden oft unterschiedliche Bezeichnungen verwendet, z. B.: Datenschutzrichtlinien, -bestimmungen oder -hinweise.

Zuge der Account-Erstellung abgerufen, also vor der ersten Nutzung des Dienstes (vgl. Tabelle 3).[40] Im Fall von *YouTube* gilt die Datenschutzerklärung des Mutterkonzerns *Google*.[41]

Tabelle 3. Letzte Aktualisierung der Datenschutzerklärungen.

App	Installationsdatum	Letzte Aktualisierung der Datenschutz-erklärung
Facebook	15.06.2018	19.04.2018
Instagram	19.06.2018	19.04.2018
LinkedIn	21.06.2018	08.05.2018[a]
Pinterest	20.06.2018	24.05.2018[b]
Snapchat	20.06.2018	15.05.2018
Twitter	21.06.2018	-[c]
WhatsApp	19.06.2018	24.04.2018
YouTube/Google	04.07.2018	-[d]

[a] Mit Wirkung vom: 08.05.2018.
[b] Datum des Inkrafttretens: 01.05.2018.
[c] Datum des Inkrafttretens. Keine Angabe zur letzten Aktualisierung.
[d] Wirksam ab dem 25.05.2018. Keine Angabe zur letzten Aktualisierung.

Zu Beginn wurden die Datenschutzerklärungen ohne Berücksichtigung von vorhandenen Verlinkungen geprüft (1. Ebene). Aufklapptexte hingegen, die innerhalb derselben URL wie die Datenschutzerklärung erreichbar waren, wurden als Bestandteil dieser ersten Ebene gewertet.
Daran anschließend wurden die in den Datenschutzerklärungen enthaltenen Hyperlinks betätigt (2. Ebene) und die dort aufgeführten Inhalte geprüft. Bei einigen Anbietern finden sich auf der zweiten Ebene weitere Hyperlinks, die wiederum zu weiteren Seiten führen. Auf eine rechtliche Einschätzung von Inhalten, die auf dritten und tieferen Ebenen zu finden sind, wurde verzichtet, da diese Inhalte nach hier vertretener Auffassung für den Nutzer nicht mehr nachvollziehbar in das Ursprungsdokument integrierbar sind. Insofern sind sie nach hier vertretener Auffassung nicht mehr leicht zugänglich, was dem Transparenzgebot nach Art. 12 Abs. 1 DSGVO widerspricht. Die gewählte Vorgehensweise orientiert sich darüber hinaus an einer Position der Artikel-29-

[40] Alle Anbieter forderten die Zustimmung zu den Allgemeinen Geschäftsbedingungen (AGB) und den Datenschutzerklärungen bevor der Account abschließend erstellt wurde.
[41] *YouTube* stellt eine eigene Datenschutzerklärung bereit, die sich aber weniger auf die Datenverarbeitung durch den Anbieter bezieht als vielmehr auf Datenschutzverletzungen durch andere *YouTube*-Nutzer.

Datenschutzgruppe.[42] Diese empfiehlt zwar, dass Links in mehrschichtigen Datenschutzhinweisen zu einzelnen Kategorien von Informationen führen sollten, anstatt alle Informationen auf einmal auf dem Bildschirm darzustellen. Datenschutzerklärungen mit verschiedenen Ebenen dürfen jedoch nach dieser Empfehlung nicht einfach nur ineinander verschachtelte Seiten sein, die mehrere Klicks erfordern, um an die relevanten Informationen zu gelangen. Design und Layout der ersten Ebene müsse so gestaltet sein, dass der Nutzer einen klaren und verständlichen Überblick darüber erhält, welche Informationen über die Datenverarbeitung zur Verfügung gestellt werden, zum Beispiel wo und wie detaillierte Informationen inmitten der Datenschutzerklärung bereitstehen.[43]

Die DSGVO normiert in Art. 12 Abs. 1 DSGVO, dass die Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu übermitteln sind. Aus diesem Grund wurden keine englischsprachigen Inhalte berücksichtigt, da Kenntnisse der englischen Sprache bei deutschen Verbrauchern nicht in einer Weise vorausgesetzt werden können, dass sie die zur Verfügung gestellten Informationen über teils komplexe Datenschutzregelungen hinreichend erfassen können.[44] Ausgenommen von der Prüfung wurden außerdem in den Datenschutzklärungen enthaltene Bilder und Videos, da diese die in Art. 13 DSGVO geregelten Informationen ergänzen aber nicht ersetzen.[45] Darüber hinaus hat die europäische Kommission ihre Befugnis gemäß Art. 12 Abs. 8 DSGVO noch nicht wahrgenommen und keine Bestimmung bezüglich der Frage erlassen, welche Informationen durch Bildsymbole dargestellt werden können und wie das Verfahren für deren Bereitstellung aussehen soll.

3.1 Zweck und Rechtsgrundlage der Datenverarbeitung

Hintergrund. Personenbezogene Daten sind grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke zu erheben (Art. 5 Abs. 1 lit. b). Nach Artikel 13 Abs. 1 lit. c hat der Verantwortliche die Zwecke mitzuteilen, für die die personenbezogenen Daten verarbeitet werden

[42] Artikel-29-Datenschutzgruppe, 2018. Die Artikel-29-Datenschutzgruppe war ein unabhängiges Beratungsgremium der Europäischen Kommission in Bezug auf Fragen des Datenschutzes; sie wurde am 25.05.2018 abgelöst von dem neuen Europäischen Datenschutzausschuss (EDSA).

[43] Um die Übersichtlichkeit von Datenschutzhinweisen zu erhöhen, wird unter anderem der sog. OnePager diskutiert. In diesem ergänzenden Dokument werden nur die wichtigsten Aussagen zur Datenverarbeitung für den Verbraucher dargestellt; s. Plattform Verbraucherschutz in einer digitalisierten Welt, 2015.

[44] Im Hinblick auf das Erfordernis der Verständlichkeit für den Betroffenen aus Art. 12 DSGVO, das zusätzlich auch in Erwägungsgrund 58 hervorgehoben wird, sind die Informationen in der jeweiligen Landessprache wiederzugeben. In Betrachtung des in Art. 3 Abs. 1 eingeführten Marktortprinzips sind im geschäftlichen Bereich Informationen nach den Art. 13 DSGVO Sprachen jener Länder zu übersetzen, in denen der Unternehmer die betreffenden Leistungen anbietet. KG Berlin, Urteil vom 8.4.2016 - 5 U 156/14.

[45] Kühling/Buchner DSGVO Art. 12 Rn. 21.

sollen.[46] Die Mitteilung über die genauen Zwecke der Verarbeitung ist für die betroffenen Personen von entscheidender Bedeutung, damit diese sich einen Überblick über alle Verarbeitungsvorgänge verschaffen können. In diesem Zusammenhang wird die Zweckbindung auch als „Grundstein des Datenschutzrechts“ bezeichnet, da hiermit über die weiteren Rechtsfolgen entschieden wird.[47] Der Zweck legitimiert die Verarbeitung personenbezogener Daten.[48] Die Informationen zum Zweck sollten daher so detailliert sein, dass klar wird, warum welche Daten erhoben werden und wozu.[49] Hierbei soll ein Bezug zwischen der Nennung der erhobenen personenbezogenen Daten sowie dem Zweck dieser Erhebung hergestellt werden. Beispielsweise ist der Betroffene bei der Verwendung von Cookies darüber in Kenntnis zu setzen, warum genau Cookies gesetzt werden („Warum“; z. B. weil einige Funktionen der Internetseite ohne Cookies nicht angeboten werden können). Außerdem ist über die genaue Verwendung aufzuklären („Wofür“, z. B. weil Cookies für folgende Anwendungen, dem Warenkorb oder der Übernahme von Suchbegriffen benötigt werden).

Neben dem Zweck der Datenverarbeitung ist den Betroffenen die Rechtsgrundlage der Verarbeitung mitzuteilen. Art. 6 DSGVO ist die zentrale Vorschrift zur Zulässigkeit der Verarbeitung personenbezogener Daten. Es gilt weiterhin ein Verbot der Datenverarbeitung unter dem Vorbehalt, dass ein gesetzlicher Erlaubnistatbestand vorliegt (z. B. durch Einwilligung oder Vertrag).[50] Die Angabe der Rechtsgrundlage muss einen Bezug zu der Angabe des Zweckes haben.

Um der Informationspflicht gemäß Art. 13 Abs. 1 lit. c zu genügen, ist mindestens *eine* Rechtsgrundlage für den jeweiligen Datenverarbeitungsvorgang zu nennen.[51] Anhand der Rechtsgrundlage soll der Verbraucher nachprüfen können, ob eine Datenverarbeitung rechtmäßig ist.

Ergebnis. Die rechtliche Prüfung ergab, dass in allen geprüften Datenschutzerklärungen durchaus Informationen zu den Zwecken und den Rechtsgrundlagen der Datenverarbeitung gegeben werden. Allerdings wird zwischen den Verarbeitungsvorgängen, dem Zweck und der Rechtsgrundlage in der Regel kein Bezug hergestellt. Hierdurch bleibt unklar, welches Datum auf Basis welcher Rechtsgrundlage und zu welchem Zweck verarbeitet wird. Auf Ebene der Informationspflichten ist die Datenschutzerklärung von *Twitter* positiv hervorzuheben. Dort wird in

[46] Paal/Pauly/Paal/Hennemann DSGVO Art. 13 Rn. 16.
[47] Artikel-29-Datenschutzgruppe, 2013, S. 4.
[48] Paal/Pauly/Frenzel DSGVO Art. 5 Rn. 23-25.
[49] Kühling/Buchner DSGVO Art. 13 Rn. 26.
[50] Paal/Pauly/Frenzel DSGVO Art. 6 Rn. 1-2
[51] Plath-Kamlah Art. 13 Rn. 11; Kühling/Buchner Art. 13 Rn. 26; Schwartmann/Schneider Art. 13 Rn. 38.

Tabellenform Auskunft über die Zwecke der Verarbeitung personenbezogenen Daten und der daraus resultierenden Rechtsgrundlage gegeben. *Twitter* informiert den Nutzer unter anderem wie folgt (Auszüge):

Verarbeitungszweck	***Daten***	***Primäre Rechtsgrundlage(n)***
Betrieb unserer Dienste, u. a.: • Erstellung des Accounts • Account-Steuerung • Inhaltserstellung, u. a. Tweets, Retweets, „Gefällt mir"-Markierungen und Direktnachrichten • Inhaltsanzeige, Empfehlungen und Rangfolgen wie z. B. in deiner Timeline, in Trends, Unterhaltungen, in Moments oder in der Suche […]	Daten die du uns mitteilst, u. a.: • Grundlegende Account-Daten • Öffentliche Daten • Kontaktdaten […] Zusätzliche Daten, die wir über dich erhalten, u. a.: • Standortdaten Interaktionen mit Links […] Die oben beschriebenen Schlussfolgerungen über dich, die wir aus diesen Daten ziehen.	Notwendig zur Vertragserfüllung
Werbung, die wir dir auf Twitter zeigen und die auf Daten basiert, die du bereitstellst oder die wir auf Twitter erfassen. […]	Daten die du uns mitteilst, u. a.: […] Zusätzliche Daten, die wir über dich erhalten, u. a.: […] Die oben beschriebenen Schlussfolgerungen […]	Legitimes Interesse

3.2 Empfänger oder Kategorien von Empfängern

Hintergrund. Nach Art. 13 Abs. 1 lit. e DSGVO muss der Verantwortliche mitteilen, wer „gegebenenfalls" die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten sind, wenn die Daten vom Verantwortlichen zum Zeitpunkt der Datenerhebung an Dritte übermittelt werden.[52] Die reine Wortlautauslegung überlässt dem Verantwortlichen die Auswahl, ob er die Empfänger oder die Kategorien von Empfängern angibt.[53] Aus Verbraucherschutzperspektive sollten jedoch konkrete Empfänger genannt werden, da Verbraucher durch konkrete Angaben einen besseren Überblick darüber erhalten, welche Dritten personenbezogene Daten erhalten.

[52] BeckOK DatenschutzR/Schmidt-Wudy DSGVO Art. 14 Rn. 51-53.
[53] Wie auch in § 34 Abs. 1 S. 1 Nr. 2 BDSG sowie § 19 Abs. 1 S. 1 Nr. 2 BDSG und auch Art. 12 lit. a RL 95/46/EG findet sich zwischen dem Begriff „Empfänger" und den Begriffen „Kategorien von Empfängern" ein **„oder".** Es ist daher – wie auch zum BDSG – fraglich, ob das „oder" eine Alternativität impliziert.

Erwägungsgrund 63 scheint ebenfalls die Ansicht zu stützen, dass die konkreten Empfänger zu benennen sind, falls diese bekannt sind.[54] Anbietern Sozialer Medien sollte zumindest zum Zeitpunkt der Registrierung bekannt sein, wer seine Geschäftspartner und Dienstleister sind und entsprechend auch, an wen Daten des Betroffenen weitergegeben werden.

Ergebnis. Die rechtliche Prüfung der Datenschutzerklärungen ergab insgesamt, dass aus Verbraucherperspektive in keiner der untersuchten Datenschutzerklärungen ausreichend konkret über die Empfänger der personenbezogenen Daten informiert wird.

Hierbei werden in allen acht Datenschutzerklärungen Auskünfte zu den *Kategorien* von Empfängern gegeben. Beispielsweise informiert der Anbieter *LinkedIn* über die Empfänger wie folgt:

„Möglicherweise nutzen wir die Dienste Dritter zur Unterstützung unserer Dienste. Wir nutzen die Dienste Dritter, um uns bei der Bereitstellung unserer Dienste zu unterstützen (beispielsweise Wartung, Analyse, Prüfung, Zahlung, Betrugserkennung, Marketing und Entwicklung). Diese Dritten haben in dem Ausmaß Zugang zu Ihren Informationen wie angemessen erforderlich, um die betreffenden Aufgaben für uns zu erledigen, und sind verpflichtet, Ihre Informationen nicht offenzulegen oder für andere Zwecke zu nutzen."

Unabhängig davon, dass die Formulierung „möglicherweise“ in der Klausel völlig offen lässt, ob die Dienste Dritter (und damit auch eine etwaige Datenweitergabe) überhaupt in Anspruch genommen werden, ist vor allem die Bezeichnung „Dritte“ als Empfänger der Daten nach hier vertretener Auffassung zu allgemein. Ein „Dritter“ kann jede natürliche oder juristische Person sein, die außer dem direkten Verantwortlichen der Datenverarbeitung, ebenfalls an der Verarbeitung personenbezogener Daten beteiligt ist. Auch *Google* beschränkt sich in seinen Ausführungen auf Kategorien von Empfängern („*Personen, Unternehmen und Organisationen*“), ohne diese näher zu beschreiben.

In fünf der acht untersuchten Fälle (*Snapchat, Facebook, Instagram, Pinterest, Twitter*) werden neben Kategorien von Empfängern zum Teil auch konkrete Empfänger aufgeführt. Wenn Anbieter teilweise konkrete Empfänger nennen können, wirft dies die Frage auf, warum diese Konkretisierung nicht durchgehend möglich ist. Beispielsweise müsste Anbietern bekannt sein, wer genau ihre Werbepartner oder Drittanbieter sind. Entsprechend müssten diese auch konkret genannt werden. Daher können zusammenfassend auch die Aufzählungen in den betreffenden fünf Datenschutzerklärungen nicht als abschließend betrachtet werden.

[54] S. auch BeckOK DatenschutzR/Schmidt-Wudy DSGVO Art. 15 Rn. 58-62; Schwartmann/Schneider DSGVO Art. 13 Rn. 17; Kühling/Buchner DSGVO Art. 13 Rn. 30.

3.3 Dauer der Speicherung

Hintergrund. Gemäß Art. 13 Abs. 2 lit. a DSGVO hat der Verantwortliche der betroffenen Person die Dauer der Speicherung der personenbezogenen Daten mitzuteilen oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Dauer.[55] Die Dauer ist als genauer Zeitraum anzugeben (Tage, Monate etc.).[56] Falls keine konkrete Speicherdauer angegeben werden kann, müssen Kriterien genannt werden, anhand derer sich der Betroffene die Speicherdauer selbst ableiten kann.[57]

Ergebnis. Insgesamt werden in sieben der acht untersuchten Datenschutzerklärungen unzureichende Angaben zur Speicherdauer gemacht (*Google*, *Facebook, Instagram, LinkedIn, Pinterest, Snapchat, Twitter*). Beispielsweise informiert *Twitter* nur über die konkrete Speicherdauer für Log-Daten (18 Monate).[58] Darüber hinaus enthält die Datenschutzerklärung nur vage Formulierungen bezüglich der Speicherdauer. Genauere Kriterien anhand derer die Speicherdauer abgeleitet werden kann, werden nicht angegeben. In diesem Zusammenhang erfolgt auch keine Konkretisierung der von der Speicherdauer betroffenen Daten, sondern es wird lediglich allgemein von Daten oder Informationen gesprochen. So informiert *Twitter* über die Speicherdauer wie folgt:

„Twitter speichert verschiedene Arten von Informationen unterschiedlich lange und gemäß unseren Allgemeinen Geschäftsbedingungen sowie unseren Datenschutzrichtlinien. Twitter basiert auf Echtzeitkommunikation; es ist daher möglich, dass einige Daten (z. B. Protokolle des IP-Verkehrs) nur für sehr kurze Zeit gespeichert werden.“

Nur aus der Datenschutzerklärung von *Snapcha*t ist die Dauer der Speicherung konkret ableitbar. Des Weiteren werden Beispiele genannt und Angaben dazu gemacht, wie lange personenbezogene Daten gespeichert werden. Ebenso sind Hinweise zu Löschvorgängen vorhanden.

3.4 Betroffenenrechte

Hintergrund. Nach Art. 13 Abs. 2 DSGVO hat der Verantwortliche zusätzlich zu den Informationen nach Abs. 1 die Pflicht, den Nutzer über die Betroffenenrechte zu informieren.[59] Gemäß Art. 13 Abs. 2 lit. b, c DSGVO sind die Betroffenen spätestens zum Zeitpunkt der ersten

[55] Schwartmann/Schneider DSGVO Art. 13 Rn. 48.
[56] Paal/Pauly/Paal/Hennemann DSGVO Art. 13 Rn. 25-26.
[57] Kühling/Buchner DSGVO Art. 13 Rn. 36.
[58] Als Log-Datei bezeichnet man von einem Server aufgezeichnete Informationen, von einem Client ausgehende Transaktionen, die einen Zugriff auf den Server nach sich ziehen; Schmidl, 2014.
[59] In Betrachtung der Einhaltung der Informationspflichten aus § 13 Abs. 2 DSGVO konzentriert sich die Prüfung primär auf die Einhaltung der Betroffenenrechte nach lit. b und lit. c.

Datenerhebung ausdrücklich auf die im Absatz 2 lit. b genannten Rechte hinzuweisen. Dies sind im Einzelnen Folgende:

- Recht auf Auskunft (Art. 15 DSGVO): Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über die personenbezogenen Daten.
- Recht auf Berichtigung (Art. 16 DSGVO): Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen (sog. Recht auf Vergessen werden).
- Recht auf Löschung (Art. 17 DSGVO): Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden.
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO): Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen.
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO): Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen zu übermitteln.
- Recht auf Widerspruch (Art. 21 DSGVO): Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. e oder f erfolgt, Widerspruch einzulegen.

Die vorgenannten Betroffenenrechte stehen jeweils unter den in den Vorschriften genannten Voraussetzungen. Aus der Aufklärung muss hervorgehen, dass es sich um ein gesetzlich festgelegtes Recht des Nutzers handelt. Grundsätzlich ist über alle Rechte vollständig zu informieren.[60] Dabei ist nicht ausschlaggebend, ob ein Recht tatsächlich besteht oder nicht.[61] Die Entscheidung darüber, ob ein Recht im Einzelfall besteht oder nicht unterliegt nicht dem Verantwortlichen. Ein Verantwortlicher, der von der Rechtmäßigkeit und Richtigkeit seiner Datenverarbeitung ausgeht, würde beispielsweise nicht unbedingt über Löschung oder ein Widerspruchsrecht informieren, weil er dies nicht für notwendig hält.[62]

[60] Paal/Pauly/Paal/Hennemann DSGVO Art. 13 Rn. 27-27a.
[61] Z. B. ist es unschädlich, wenn auf das Recht des Einwilligungswiderrufs hingewiesen wird, obwohl eine Rechtmäßigkeit der Datenverarbeitung aus Einwilligung nicht besteht; s. Schmidt-Wudy Art. 15 Rn. 69.
[62] Gola DSGVO Art. 13. Rn. 21.

Erst durch die Aufklärung des Betroffenen über die ihm zustehenden Rechte ist sichergestellt, dass der Verbraucher so informiert ist, dass er diese Rechte auch tatsächlich ausüben kann.

Ergebnis. Die vorgenommene Prüfung ergab insgesamt, dass in allen untersuchten Datenschutzerklärungen die Betroffenenrechte der Nutzer angesprochen werden. Sechs Datenschutzerklärungen zählen hierbei alle Betroffenenrechte vollständig auf.

Zwei der acht untersuchten Datenschutzerklärungen (*LinkedIn, Snapchat*) nennen nicht alle Rechte, die der Betroffene hat. So informiert *Snapchat* beispielsweise nicht über die Rechte auf Berichtigung, Einschränkung und Verarbeitung. *LinkedIn* informiert nicht eindeutig über die Möglichkeit der Ausübung der Rechte auf Widerspruch und Datenübertragbarkeit.

Drei von acht Anbietern unterlassen es darüber hinaus, die Betroffenenrechte als gesetzlich festgelegtes Recht kenntlich zu machen (*Pinterest*, *Snapchat*, *Twitter*). So informiert *Snapchat* im Kapitel „Kontrolle deiner Daten“ wie folgt: *„Wir möchten, dass du die Kontrolle über deine Daten behältst. Deshalb stellen wir folgende Tools bereit. [...]“*

Für den Verbraucher ist nicht erkennbar, dass das vorliegende Kapitel „Kontrollen deiner Daten“ über gesetzlich normierte Betroffenenrechte aufklären soll. Die darüber hinausgehenden Informationen „Meine Daten herunterladen“, „Widerruf der Zugriffberechtigung“ oder „Löschung“ vermitteln eher den Eindruck, dass es sich seitens des Anbieters um ein freiwilliges Angebot und nicht um gesetzlich festgelegte Informationen bezüglich bestehender Rechte handelt.

3.5 Zwischenfazit: Informationspflichten

Die rechtliche Prüfung der Datenschutzerklärungen von acht Anbietern Sozialer Medien ergab, dass diese in Bezug auf die geprüften Aspekte Lücken aufweisen. Für den Nutzer bleibt es hierdurch schwierig, sich einen Überblick über die mit der Nutzung verbundenen Verarbeitungsvorgänge zu verschaffen.

Bis auf eine Ausnahme (*Twitter*) wird in den geprüften Datenschutzerklärungen kein Bezug zwischen dem Zweck, der Rechtsgrundlage und Verarbeitungsvorgängen hergestellt.

Die Überprüfung ergab weiterhin, dass in sieben Datenschutzerklärungen unzureichende Angaben zu einem konkreten Speicherzeitraum gemacht werden; nur in einem Fall ist ein konkreter Speicherzeitraum für personenbezogene Daten ableitbar (*Snapchat*). In Bezug auf die Empfänger der verarbeiteten personenbezogenen Daten bleiben die geprüften Angaben ebenfalls vage. Darüber hinaus wird teilweise nicht ausreichend über die Betroffenenrechte des Nutzers aufgeklärt.

4 ÜBERPRÜFUNG PRIVACY BY DEFAULT

Hintergrund. Art. 5 Abs. 1 DSGVO regelt die Grundsätze der Verarbeitung personenbezogener Daten, unter anderem in 5 Abs. 1 lit. b den Zweckbindungsgrundsatz sowie in 5 Abs. 1 lit. c den Grundsatz der *Datenminimierung*. Nach dem Grundsatz der Datenvermeidung und Datensparsamkeit sind Datenverarbeitungssysteme an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Danach ist die Verarbeitung personenbezogener Daten, die für den genannten Zweck unerheblich sind, unzulässig. Der übermäßigen Erhebung personenbezogener Daten durch Anbieter soll mit anderen Worten Einhalt geboten werden, indem die Datenverarbeitung auf das für die Zweckerfüllung notwendige Maß reduziert wird.[63] Die Umsetzung des Grundsatzes der Datenminimierung wird unter anderem durch die Regelung zur datenschutzfreundlichen Voreinstellung (*Privacy by default*) gestaltet. Diese wird in Art. 25 Abs. 2 DSGVO aufgegriffen. Der Verantwortliche soll *„geeignete technische und organisatorische Maßnahmen [ergreifen], die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden."*

Gerade im Kontext Sozialer Medien ist dies eine wichtige Neuerung. Bei der Anmeldung bei einem Social Media-Dienst nimmt nämlich nur eine Minderheit von Nutzern Veränderungen an den Standard- und Datenschutzeinstellungen vor.[64] Dies kann verschiedene Gründe haben. So neigen Personen auch in anderen Kontexten dazu, bei vorausgewählten Optionen den Status quo nicht zu verändern – auch ohne, dass es hierfür einen rationalen Grund gibt.[65] In Bezug auf Datenschutz bei Sozialen Medien wissen Nutzer oftmals überhaupt nicht, welche Datenschutzeinstellungen für ihre Inhalte gelten.[66] Hinzu kommt, dass die zugrundeliegenden Verarbeitungsvorgänge und potenziellen Konsequenzen von mangelndem Datenschutz insbesondere von Laien nicht realistisch eingeschätzt werden können – beispielweise bedingt durch fehlende Information oder kognitive Verzerrungen.[67] Mit der Privacy-by-default-Regelung werden daher insbesondere Nutzer geschützt, die aus eigenem Antrieb keine Änderungen an den vorausgewählten Einstellungen vornehmen.[68]

---

[63] Paal/Pauly DSGVO 2. Auflage 2018, Art. 25 Rn. 12.
[64] Artikel-29-Datenschutzgruppe, 2009, S. 8.
[65] Sog. *Status Quo Bias*, s. Samuelson & Zeckhauser, 1988; ein prominent gewordenes Beispiel hierfür ist das Thema Organspende: In Ländern, in denen Organspende der gesetzliche Standard ist (Opt-out), ist die Mehrheit der Bevölkerung potenzieller Organspender. In Ländern wie Deutschland hingegen, wo Organspende per Opt-in gelöst wird, ist nur eine Minderheit Organspender; vgl. Johnson & Goldstein, 2004.
[66] Moll, Pieschl & Bromme, 2014.
[67] Acquisti, 2004.
[68] Paal/Pauly DSGVO/BDSG 2. Auflage Art. 25 Rn. 12.

Vorgehen. Im Rahmen der vorliegenden Marktanalyse wurde zunächst beobachtend erfasst, welche Einstellungsmöglichkeiten in die betreffenden Dienste integriert sind und welche Voreinstellungen direkt im Anschluss an die Account-Erstellung vorzufinden sind.[69] Im Fall von *YouTube* wurden insbesondere die Einstellungsmöglichkeiten innerhalb des *Google*-Accounts erfasst, über den der Dienst *YouTube* in der Regel genutzt wird.

Obwohl die ausgewählten Dienste schon in Umfang und Art ihrer Funktionen sehr heterogen sind, wurden neben einer Reihe von Einzelbeobachtungen vier Bereiche identifiziert, die sich auf die ein oder andere Weise bei allen analysierten Diensten wiederfanden und nach Auffassung des Marktwächter-Teams der Verbraucherzentrale NRW in Zusammenhang mit der Regelung der datenschutzfreundlichen Voreinstellungen stehen.[70] Diese vier Bereiche betreffen die Voreinstellungen bei der Authentifizierung des Nutzers (Abschnitt 4.1), die Aufforderungen zur Kontaktsynchronisation (Abschnitt 4.2), personalisierter Werbung (Abschnitt 4.3) sowie die Sichtbarkeit und Auffindbarkeit nutzergenerierter Inhalte für andere Nutzer (Abschnitt 4.4). Im Folgenden werden für jeden dieser Aspekte zunächst die Beobachtungen beschrieben und anschließend aus Verbraucherschutzperspektive bewertet.

4.1 Authentifizierung

Hintergrund. Online-Dienste fordern im Zuge der Registrierung in der Regel ein Referenzdatum, mit der sich der Nutzer nach Registrierung bei dem Dienst anmelden kann. Klassischerweise wird hierfür eine E-Mail-Adresse abgefragt, zu der man ein Dienstspezifisches Passwort erstellen muss. Die E-Mail-Adresse wird also zur Authentifizierung des Nutzers innerhalb des Dienstes genutzt.

Beobachtung. In vier der acht untersuchten Fälle (*Facebook, Instagram, Twitter und Snapchat*) können Nutzer auswählen, ob sie sich per E-Mail-Adresse oder mit ihrer Mobilfunknummer registrieren (s. z. B. Abbildung 1).

[69] Für die nachfolgende Darstellung wurden neben ggf. vorhandenen Einstellungsmöglichkeiten auch Informationen aus dem Hilfebereich des Dienstes entnommen. Im Fall von *YouTube* wurden neben den Einstellungsmöglichkeiten im *YouTube*-Account auch die Optionen innerhalb des *Google*-Kontos geprüft.

[70] Da das Ziel der vorliegenden Marktanalyse ein kompakter Überblick zur Umsetzung der datenschutzfreundlichen Grundeinstellungen ist, wurde auf die Darstellung von dokumentierten Einzelbeobachtungen verzichtet, wenn sie nicht in einen der identifizierten Bereiche fielen.

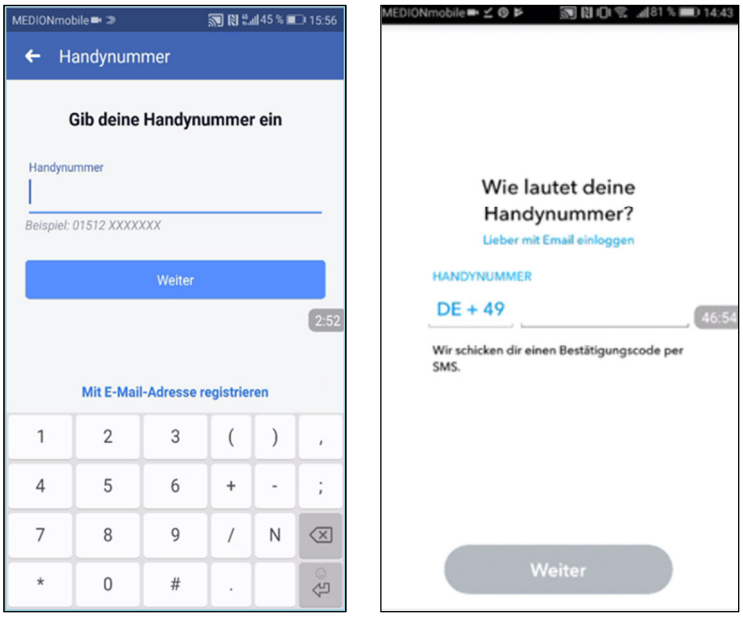

Abbildung 1. Voreinstellung zur Authentifizierung bei *Facebook* (links) und *Snapchat* (rechts).

In allen vier Fällen ist jedoch die Mobilfunknummer als Authentifizierungsdatum voreingestellt (Tabelle 4).[71]

Bei zwei Diensten (*LinkedIn* und *Pinterest*) ist eine Registrierung ausschließlich via E-Mail-Adresse möglich. Im Fall von *YouTube* (*Google)* ist bei mobiler Registrierung kein weiteres Referenzdatum zur Registrierung erforderlich. Die Mobilfunknummer wird in einem weiteren Schritt optional abgefragt, es gibt jedoch keine entsprechende Voreinstellung.

Bewertung. Für die Bewertung der beschriebenen Beobachtung muss in Betracht gezogen werden, dass es einen qualitativen Unterschied zwischen dem Authentifizierungsdatum der Mobilfunknummer und dem der E-Mail-Adresse gibt. Insbesondere ist mit Angabe der Mobilfunknummer im Gegensatz zur E-Mail-Adresse eine pseudonyme Nutzung des Dienstes ausgeschlossen.

So ist die Mobilfunknummer seit der Registrierungspflicht für SIM-Karten in der EU mit einer eindeutig – das heißt per Personalausweis – identifizierten Person verknüpft.[72] Darüber hinaus benutzt man in der Regel nur eine einzige Mobilfunknummer für private Zwecke, während ein und dieselbe Person ohne viel Aufwand verschiedene E-Mail-Adressen für unterschiedliche Dienste nutzen kann. Diese eindeutig identifizierende Mobilfunknummer ist darüber hinaus persistenter als

[71] Teilweise ist vorab ersichtlich, dass die Registrierung sowohl per E-Mail-Adresse als auch per Mobilfunknummer möglich ist.
[72] S. Biselli, 2017.

eine E-Mail-Adresse. So behalten Verbraucher ihre Mobilfunknummer üblicherweise über viele Jahre hinweg, auch wenn sie zwischenzeitlich den Mobilfunkanbieter wechseln.

Tabelle 4. Voreinstellungen zur Authentifizierung bei Registrierung.

Dienst	Registrierung ist möglich via		Voreinstellung
	E-Mail	Mobilfunknummer	
Facebook	ja	ja	Mobil
Instagram	ja	ja	Mobil
LinkedIn	ja	nein	E-Mail
Pinterest	ja	nein	E-Mail
Snapchat	ja	ja	Mobil
Twitter	ja	ja	Mobil
WhatsApp	nein	ja	-[a]
YouTube/ Google	ja	-[b]	E-Mail

[a] Dienst kann nur unter Angabe der Mobilfunknummer registriert werden.
[b] Für die mobile Nutzung des *YouTube*-Accounts muss ein *Google*-Konto erstellt werden.

Wegen ihres hohen Potenzials einen Nutzer eindeutig über mehrere Dienste hinweg zu identifizieren, wird die Mobilfunknummer im Online-Bereich zusehends als Ersatz für eindeutige Identifizierungsdokumente wie den Führerschein oder die Sozialversicherungsnummer betrachtet.[73] Insofern entscheidet das Authentifizierungsdatum (E-Mail-Adresse oder Mobilfunknummer) auch darüber, wie stark ein Dienst mit der Identität des Nutzers verknüpft ist.
Der Grundsatz der Datenminimierung schreibt vor, dass die erhobenen personenbezogenen Daten für die Zwecke, zu denen sie verarbeitet werden, „angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt“ sein sollen. Bei der Datenverarbeitung sollen also nur solche Daten verarbeitet werden, die für den Verarbeitungszweck notwendig sind. Auch die Vorschrift zur datenschutzfreundlichen Grundeinstellung, die eine Umsetzungsregelung für diesen Grundsatz der Datenminimierung darstellt, stellt klar, dass durch Voreinstellungen nur solche Daten verarbeitet werden dürfen, die für den jeweiligen Zweck erforderlich sind. Die Angabe der Mobilfunknummer ist nach hier vertretener Auffassung in den meisten Fällen für die Registrierung nicht erforderlich und erschwert darüber hinaus die pseudonyme Nutzung des Dienstes. Die Authentifizierung kann auch unter Angabe

[73] S. http://www.martinpi.com/your-cell-phone-number-is-your-new-social-security-number/.

einer E-Mail-Adresse erfolgen. Dies zeigt schon die angebotene Auswahlmöglichkeit im Rahmen der Installationsprozesse. Die Voreinstellung der Mobilfunknummer als Authentifizierungsmerkmal ist daher nach hier vertretener Auffassung vom Grundsatz der Datenminimierung und der Vorschrift zur datenschutzfreundlichen Voreinstellung betroffen.

Für den Nutzer sollen sich durch die Angabe der Mobilfunknummer verschiedene Vorteile ergeben. Insbesondere soll die Abfrage der Mobilfunknummer die Sicherheit des Accounts erhöhen.[74] Dieselbe Eigenschaft der Mobilfunknummer, die die Sicherheit vor unbefugtem Zugriff durch andere Personen erhöhen soll – nämlich das hohe Potenzial zur eindeutigen Identifizierung und somit Authentifizierung des Nutzers – bedeutet wesentliche Nachteile hinsichtlich Privatsphäre und Datenschutz gegenüber dem Anbieter. So vereinfacht die Mobilfunknummer als eindeutiges Identifizierungsmerkmal die Verknüpfung von Daten und das Tracken von Nutzern über verschiedene Dienste hinweg. Darüber hinaus kann gerade die Preisgabe der Mobilfunknummer ein zusätzliches Sicherheitsrisiko bedeuten, da Nutzerdaten auf externen Servern nicht immer ausreichend geschützt werden.[75]

Sofern die Nutzung des Dienstes auch allein über die E-Mail-Adresse möglich ist, entspricht die Vorauswahl der Mobilfunknummer als Authentifizierungsdatum nicht einer datenschutzfreundlichen Voreinstellung, da ihre Preisgabe eine pseudonyme Nutzung des Dienstes erschwert und das Tracken des Nutzers zu Werbezwecken vereinfacht.

4.2 Kontaktsynchronisation

Hintergrund. An die mobile Nutzung eines Dienstes sind in der Regel Zugriffsberechtigungen geknüpft, die die App vom Nutzer einfordert. Dies kann auch die Berechtigung beinhalten, auf das Telefonbuch des Smartphones und somit auf die abgespeicherten Kontakte des Nutzers zuzugreifen. Hier können auch Kontaktdaten von Personen abgespeichert sein, die den betreffenden Dienst nicht nutzen. Bei der Kontaktsynchronisation wird in der Regel das komplette Adressbuch auf die Anbieter-Server hochgeladen, die sich teilweise außerhalb der EU befinden.

Seit der Version Android 6.0 lassen sich unter dem Betriebssystem Android Zugriffsrechte von Apps einzeln verwalten. Zusätzlich wird der Nutzer nach der App-Installation vom Android-Berechtigungsmanager bei jeder Zugriffsanfrage der App über ein Pop-Up benachrichtigt und

[74] S. https://www.power-datenschutz.de/facebook-fragt-nach-handynummer/.
[75] Kaiser, 2018.

muss dann entscheiden, ob Android der App den Zugriff gewähren soll. [76] In der vorliegenden Untersuchung wurden derlei Zugriffsanfragen während des Registrierungsprozesses abgelehnt.

Beobachtung. Im Zuge der Registrierung forderten mit Ausnahme von zwei Diensten (*YouTube/Google, Pinterest*) alle Apps den Nutzer auf ihrer Benutzeroberfläche zur Synchronisation seiner Kontakte auf (s. Abbildung 2 für ein Beispiel). Mit Ausnahme von *WhatsApp* enthalten diese Aufforderungen eine Vorauswahl, die den Nutzer zum Synchronisieren der Kontakte leitet (s. Tabelle 6).[77] Auffällig hierbei sind die Apps von *Snapchat* und *Facebook*, bei denen der Android-Berechtigungsmanager über die Zugriffsanfrage der App auf die Kontakte benachrichtigt, *bevor* eine Aufforderung auf der Benutzeroberfläche der App erscheint. Dies kann auf eine nicht datenschutzfreundliche Voreinstellung in Bezug auf die Kontaktsynchronisation hinweisen. In Bezug auf die Aufforderungen zur Synchronisation auf der Benutzeroberfläche der Apps sind weitere Auffälligkeiten zu verzeichnen. Im Fall von *Facebook* und *Instagram* wird nicht deutlich, dass die in der Aufforderung vorausgewählte Option die Synchronisation der Kontakte beinhaltet. Im Fall von Twitter wird dem Nutzer bei der ersten Aufforderung keine Möglichkeit zum Ablehnen der Synchronisation gegeben (Abbildung 2, links).

Nach Klicken des blau hinterlegten Buttons (Abbildung 2, links) erscheint die entsprechende Benachrichtigung des Android-Berechtigungsmanagers (Abbildung 2, Mitte). Erst wenn man dort auf „Ablehnen" klickt, erhält man die Möglichkeit, die Synchronisation auch auf der Benutzeroberfläche der App abzulehnen (Abbildung 2, rechts). Die Grundeinstellung ist jedoch die Option „Gehe zur App-Information", wo man die entsprechende Einstellung ändern kann. Dem Nutzer wird schon durch die dargestellte Abfolge suggeriert, der Zugriff sei erforderlich für die Nutzung des Dienstes. Die nach Ablehnen der Synchronisation erscheinende Nachricht unterstützt diesen Eindruck (Abbildung 2, rechts).

[76] S. z. B. https://mobilsicher.de/hintergrund/neue-aera-rechteverwaltung-mit-android-6-marshmallow/.
[77] *WhatsApp* ist ohne diese Zugriffsberechtigung nicht wie vorgesehen nutzbar, s. auch Abschnitt 4.1.

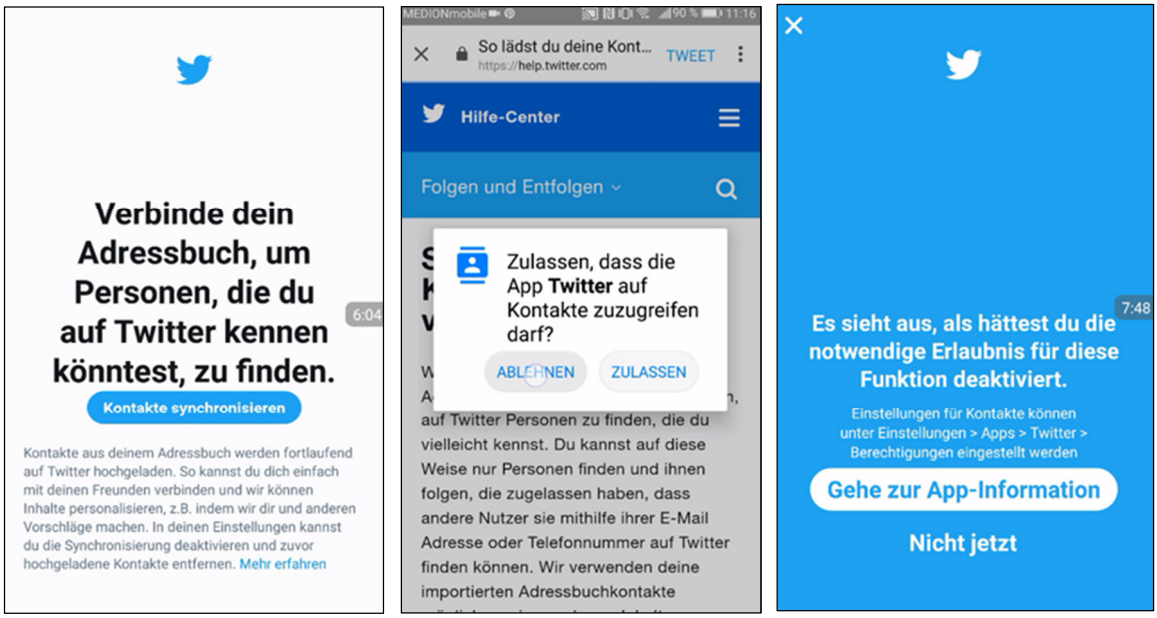

Abbildung 2. Kontaktsynchronisation bei *Twitter*.

Tabelle 5. Aufforderungen zur Kontaktsynchronisation.

Dienst	Nutzung des Dienstes ist ohne Kontakt-synchronisation möglich	Aufforderungen zur Kontakt-synchronisation auf der Benutzeroberfläche der App	
		vorhanden	Voreinstellung datenschutzfreundlich
Facebook	ja	ja	nein
Instagram	ja	ja	nein
LinkedIn	ja	ja	nein
Pinterest	ja	nein	-
Snapchat	ja	ja	nein
Twitter	ja	ja	nein
WhatsApp	nein	ja	-[a]
YouTube/ Google	ja	nein	-

[a] Dienst ist ohne Kontaktsynchronisation nicht wie vorgesehen nutzbar.

Bewertung. Bei der Bewertung der beschriebenen Beobachtungen muss beachtet werden, dass die untersuchten Apps in der Regel nicht automatisch eine Berechtigung zur Kontaktsynchronisation über das Betriebssystem vorsehen (mögliche Ausnahmen: *Facebook, Snapchat*). In diesen Fällen ist die Voreinstellung zur Kontaktsynchronisation durchaus als datenschutzfreundlich zu bewerten. Zur Debatte steht darüber hinaus nicht der grundsätzliche Umstand, *dass* im Rahmen der Registrierung auf der Benutzeroberfläche der Apps zur Kontaktsynchronisation aufgefordert wird. Allerdings wird in den integrierten Aufforderungen teilweise suggeriert, die Synchronisation der Kontakte sei erforderlich für die Nutzung des Dienstes. Durch wiederholte Aufforderungen, intransparente Optionen oder auch einzelne Formulierungen kann der Nutzer dazu gebracht werden, die datenschutzfreundliche Voreinstellung umzukehren.[78] Insofern stellt dies nach hier vertretener Auffassung eine Umgehung verbraucherschützender Vorschriften dar.

Anhand der geschilderten Beobachtungen wird deutlich, wie groß das Interesse des Anbieters an der Kontaktsynchronisation ist. Diese erweitert in zweierlei Hinsicht die Menge an Daten, die der Anbieter über Nutzer erhält:

Erstens werden durch die Kontaktsynchronisation auch Daten von Nutzern übermittelt, die ihre Mobilfunknummer explizit nicht angegeben haben (s. Abschnitt 4.1) oder sich gegen die Nutzung des Dienstes entschieden haben – zum Beispiel aufgrund ihrer Datenschutzbedenken. Diese Personen werden bei Erhebung ihrer Kontaktdaten nach aktuellem Stand weder informiert, noch wird eine Einwilligung für die Erhebung ihrer Daten eingeholt.

Zweitens werden durch die Synchronisation der Kontakte weitere Informationen über den betreffenden Nutzer gesammelt: So kann die Kenntnis darüber, welche Kontakte ein Nutzer in seinem Adressbuch abgespeichert hat, genauere Aussagen über das persönliche Netzwerk des Nutzers zulassen. Beispielsweise sagt eine Follower-Verbindung auf Twitter in der Regel wenig über die tatsächliche Beziehung der betreffenden Twitter-Nutzer aus, da die Follower-Struktur Rückschlüsse auf Interesse, nicht aber Bekanntschaft erlaubt. Das Wissen darüber, ob beziehungsweise dass zwei Nutzer auch ihre Kontaktdaten ausgetauscht haben, lässt zumindest den Rückschluss zu, dass die beiden sich auf persönliche(re) Art und Weise kennen. Kenntnisse über die Netzwerkstruktur von Nutzern können wiederum für algorithmenbasierte Prognosen genutzt werden. So wurde beispielsweise berichtet, dass *Facebook*-Freunde einen Einfluss auf die Beurteilung der Kreditwürdigkeit einer Person haben können.

[78] Vgl. Forbrukerrådet, 2018.

4.3 Personalisierte Werbung

Hintergrund. Das Geschäftsmodell Sozialer Medien beinhaltet oft das Schalten personalisierter Werbung. Für diese Personalisierung werden insbesondere Daten hinzugezogen, die auf der Praktik des sogenannten Trackings basieren. Hierbei werden die Aktivitäten des Nutzers verfolgt und gespeichert, um Rückschlüsse auf Vorlieben, Interessen und letztendlich das Konsumverhalten des Nutzers zu ziehen. Je nach Ausmaß des Trackings und der Zusammenführung der gesammelten Daten können hierdurch detaillierte Nutzerprofile erstellt werden.
Zum Zeitpunkt der Untersuchung sehen mit nur einer Ausnahme (*WhatsApp*) alle ausgewählten Dienste vor, personenbezogene Daten für die Personalisierung von Werbung zu nutzen.[79]

Beobachtung. Vorgefunden wurde eine heterogene Menge an Einstellungsmöglichkeiten im Kontext personalisierter Werbung (s. Abbildung 3 für zwei Beispiele). So bietet *LinkedIn* vierzehn unterschiedliche Einstellungsmöglichkeiten im Kontext personalisierter Werbung an, während andere Anbieter nur zwei Optionen anbieten (z. B. *Pinterest*, *Snapchat*). Die Erklärungen zu den Einstellungsmöglichkeiten wurden für die nachfolgende Darstellung dem Wortlaut nach interpretiert; allerdings konnte auf Basis der Formulierungen in einigen Fällen nicht mit Sicherheit geklärt werden, wie umfassend verschiedene Einstellungsmöglichkeiten tatsächlich sind.

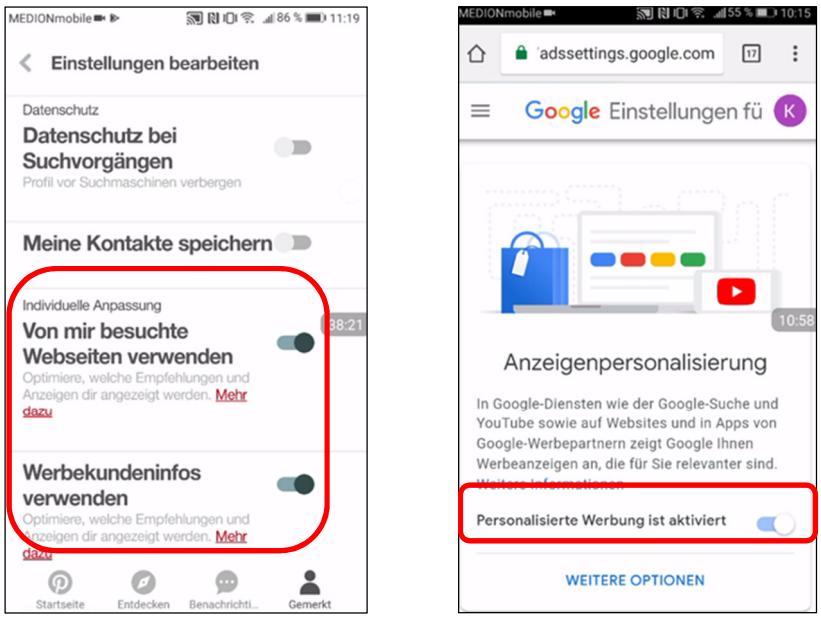

Abbildung 3. Voreinstellung zur personalisierten Werbung bei *Pinterest* (links) und *Google* (rechts).

[79] *WhatsApp* gibt allerdings Nutzerdaten an den Mutterkonzern *Facebook* weiter (s. Greis, 2018) und hat zwischenzeitlich angekündigt, Werbung innerhalb der Status-Meldungen des Messengers zuzulassen; s. Berger, 2018.

Die nachfolgende Darstellung ist daher nicht abschließend und stellt vielmehr einen Versuch dar, einen Teil der komplexen und heterogenen Menge an Einstellungsmöglichkeiten greifbar zu machen. Bei den vorgefundenen Einstellungsmöglichkeiten wird häufig unterschieden zwischen der Personalisierung von Werbung anhand von internen versus externen Tracking-Daten. Interne Tracking-Daten entstehen im Zuge der Nutzung des Social Media-Dienstes, beispielsweise beim „Liken", Teilen und Kommentieren von Beiträgen oder dem Besuch von Nutzerprofilen. Externe Tracking-Daten entstehen durch Online-Aktivitäten, die nicht die Nutzung des Kern-Dienstes umfassen, wie beispielsweise der Besuch einer Webseite außerhalb der Anwendung. Die folgende Darstellung berücksichtigt diese Unterscheidung.

Verwendung interner Tracking-Daten zur Personalisierung. Nach Registrierung sehen sieben der acht geprüften Dienste vor, dass interne Tracking-Daten zur Personalisierung von Werbung genutzt werden (Ausnahme: *WhatsApp*, s.o.). Bei zwei der sieben Dienste kann die Verwendung interner Tracking-Daten zu diesem Zweck eingeschränkt werden (*YouTube/Google*, *LinkedIn*). Bei den verbleibenden fünf Diensten, scheint es keine Möglichkeit zu geben, die Verwendung interner Tracking-Daten zur Personalisierung von Werbung zu unterbinden (*Facebook, Instagram, Pinterest, Snapchat, Twitter*). Zwar kann im Fall von *Facebook* unterbunden werden, dass interne Tracking-Daten zur Personalisierung von Werbung *außerhalb* von *Facebook* genutzt werden; vom Wortlaut nicht umfasst ist jedoch Werbung, die *innerhalb* von *Facebook* geschaltet wird.[80]

Bei *Instagram* gibt es *keinerlei* Einstellungsmöglichkeiten in Bezug auf personalisierte Werbung. Stattdessen findet sich im Hilfebereich ein Hinweis, dass Werbeeinstellungen im *Facebook*-Konto vorgenommen werden könnten. Die Modifikation dieser Einstellungen setzt also voraus, dass man ein *Facebook*-Konto hat und dieses mit dem *Instagram*-Konto verknüpft hat.

Verwendung externer Tracking-Daten zur Personalisierung. Bei fünf der untersuchten Dienste (*LinkedIn, Pinterest, Snapchat, Twitter, YouTube/Google*) kann die Verwendung externer Tracking-Daten zur Personalisierung unterbunden werden. *Facebook* hat hierzu eine per Voreinstellung deaktivierte Option, allerdings wird in der betreffenden Einstellung nicht erwähnt, inwieweit sie das externe Tracking durch die Integration des Like-Buttons auf externen Webseiten umfasst. Insofern kann die Personalisierung möglicherweise auch bei deaktivierter Einstellung auf externen Tracking-Daten basieren, die in diesem Fall letzten Endes nicht ausgeschaltet werden kann.

[80] Bei *Facebook, Snapchat, Twitter* und *YouTube (Google)* kann innerhalb des Profils eingesehen werden, von welchen Interessen des Nutzers ausgegangen wird (basierend auf internen Tracking-Daten). Der Nutzer kann diese modifizieren. Das Entfernen der Interessen aus dem Profil muss jedoch nicht zur Löschung der zugrunde liegenden Daten auf den Anbieter-Servern führen.

Bewertung. Die beschriebene Praxis der Anbieter ist vom Grundsatz der Datenminimierung und somit von der Regelung zur datenschutzfreundlichen Voreinstellung betroffen. Zu berücksichtigen ist hierbei, dass Anbieter personenbezogene Daten verarbeiten dürfen, wenn diese für den jeweiligen Verarbeitungszweck erforderlich sind. Dieser Verarbeitungszweck kann unter anderem unter Berücksichtigung gesetzlicher Vorgaben auch das Aussenden von Werbung beinhalten.[81]

Tabelle 6. Nutzung von Tracking-Daten für personalisierte Werbung.

Dienst	Personalisierung von Werbung anhand von					
	internen Tracking-Daten			externen Tracking-Daten		
	Vorge-sehen[a]	Einstellungs-möglichkeit vorhanden	Voreinstellung datenschutz-freundlich	Vorge-sehen[a]	Einstellungs-möglichkeit vorhanden	Voreinstellung datenschutz-freundlich
Facebook	ja	nein[b]	(nein)[c]	ja	nein[d]	(nein)[c]
Instagram	ja	nein	(nein)[c]	ja	nein	(nein)[c]
LinkedIn	ja	ja	nein	ja	ja	nein
Pinterest	ja	nein	(nein)[c]	ja	ja	nein
Snapchat	ja	nein	(nein)[c]	ja	ja	nein
Twitter	ja	nein	(nein)[c]	ja	ja	ja
WhatsApp	nein	-	-	nein	-	-
YouTube/ Google	ja	ja	nein	ja	ja	nein

[a] Aus dem Hilfebereich oder anderweitigen Informationen geht hervor, dass interne bzw. externe Tracking-Daten für die Personalisierung verwendet werden.
[b] Modifizierbar nur für Werbung, die auf Basis dieser Daten außerhalb der *Facebook*-Produkte angezeigt werden. Die Nutzung von internen Tracking-Daten für Werbung innerhalb von *Facebook*-Produkten kann mit dieser Einstellung offenbar nicht beeinflusst werden.
[c] Keine Einstellungsmöglichkeit vorhanden.
[d] Die vorhandene Einstellungsoption (deaktiviert) lässt offen, inwieweit die Datenübermittlung durch in externe Webseiten integrierte Like-Buttons umfasst ist.

Nichtsdestotrotz muss auch für den Verarbeitungszweck des Schaltens personalisierter Werbung der Grundsatz der Datenminimierung berücksichtigt werden.[82] Nach hier vertretener Auffassung werden jedoch mehr personenbezogene Daten verarbeitet als für das Schalten personalisierter Werbung erforderlich ist. Personalisierung von Werbung ist schon auf Basis von statischen Personenmerkmalen möglich. Dementgegen werden per Voreinstellung sowohl Nutzer-Daten

[81] S. Verbraucherzentrale Bundesverband (2018, S. 7ff.); Datenschutzkonferenz (2017).
[82] Paal/Pauly/Martini DSGVO Art. 25 Rn. 12-14.

verwendet, die auf dem Tracking des Nutzers innerhalb und in vielen Fällen auch außerhalb des Dienstes basieren. In nur zwei Fällen kann die Verwendung interner Tracking-Daten eingeschränkt werden; in Bezug auf die Verwendung von externen Tracking-Daten sind es fünf der sieben Dienste, die eine entsprechende Einstellungsmöglichkeit für personalisierte Werbung vorsehen.

Wenn Tracking-Daten nicht erforderlich für die Personalisierung von Werbung sind, stellt sich die Frage, inwieweit ihre Verarbeitung in dem beobachteten Ausmaß rechtmäßig ist.[83] Auffällig ist, dass es bei den geprüften Diensten kaum eine Möglichkeit gibt, das Nutzer-Tracking selbst einzuschränken.[84] Im Verhältnis hierzu stellt nach hier vertretener Auffassung die vorhandene Option, personalisierte Werbung einzuschränken, lediglich eine Illusion von Kontrolle dar. Nutzer können hierdurch schließlich nicht kontrollieren, wie viel Anbieter über sie wissen, sondern nur, in welchem Ausmaß sie dieses Wissen aktuell zum Beispiel für personalisierte Werbung nutzen dürfen.

4.4 Sichtbarkeit und Auffindbarkeit

Beobachtung. In der Regel integrieren Social Media-Dienste auch Einstellungsmöglichkeiten, die sich auf die Sichtbarkeit und Auffindbarkeit von Nutzerinformationen für andere Nutzer oder auch für Nicht-Nutzer des Dienstes beziehen. Im Folgenden geht es entsprechend um die Frage, inwieweit Nutzer-Daten, die vom Anbieter gespeichert wurden, per Voreinstellung sichtbar beziehungsweise auffindbar für andere Personen sind.

Für die vorliegende Untersuchung wurde geprüft, welche Voreinstellungen für die Sichtbarkeit von Profilinformationen einerseits und Beiträgen beziehungsweise Status-Updates andererseits vorzufinden sind. Profilinformationen betreffen hierbei Details, die die betroffene Person zur expliziten Selbstbeschreibung über sich preisgegeben hat. Diese selbstreferentiellen Informationen sind statisch, d. h. sie verändern sich nicht ständig, sondern begleiten die Aktivität des Nutzers durchgehend.

Beiträge hingegen betreffen jegliche Inhalte (z. B. Text, Bild, Video), die der Nutzer als Status-Update, Story oder Post seinem Netzwerk mitteilt. Diese Inhalte sind dynamisch, das heißt, ältere Inhalte stehen mit der Zeit weniger im Fokus als aktuelle Informationen. Mit Ausnahme von *Facebook* und *LinkedIn* (s. Abbildung 4 für ein Beispiel) sind Möglichkeiten zur Angabe von

[83] Mögliche Rechtsgrundlagen hierfür sind: Erforderlichkeit für die Vertragserfüllung, informierte Einwilligung, Interessensabwägung. Die Rechtmäßigkeit der Verarbeitung wurde in der vorliegenden Analyse nicht geprüft.
[84] S. auch Paal/Pauly/Martini DSGVO Art. 25 Rn. 13.

Profilinformationen begrenzt auf eine Art Selbstbeschreibung und gegebenenfalls Geschlecht oder Geburtsdatum.

Ergebnis. Im Zuge der Registrierung und ersten Nutzung zeigte sich, dass die Sichtbarkeit von Profilinhalten per Voreinstellung in nur zwei Fällen (*Snapchat, YouTube*) weitestgehend auf die bestätigten Kontakte innerhalb des Netzwerks beschränkt war (Tabelle 7). Bei allen übrigen Diensten waren diese Inhalte öffentlich sichtbar, das heißt im Mindesten für alle eingeloggten Nutzer, gegebenenfalls jedoch auch für Nicht-Mitglieder des Netzwerks (z. B. im Fall von *LinkedIn*).

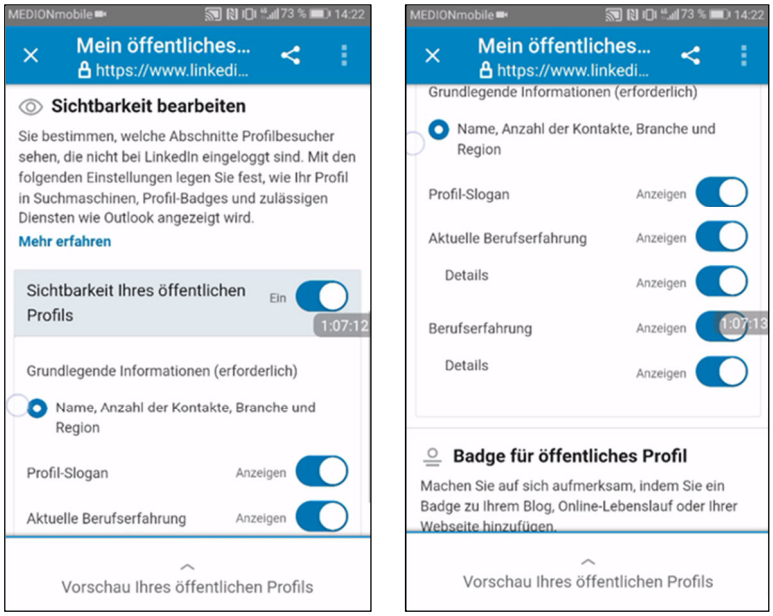

Abbildung 4. Voreinstellung zur Sichtbarkeit des *LinkedIn*-Profils.

Im Fall von *Facebook* zählte zu den als standardmäßig öffentlich eingestellten Informationen auch die sexuelle Orientierung. Für „Freunde von Freunden“ war die politische und religiöse Orientierung sichtbar. In fünf Fällen ist die Sichtbarkeit von Beiträgen, die Nutzer online teilen, nicht auf bestätigte Kontakte beschränkt (*Instagram, LinkedIn, Pinterest, Twitter, YouTube/Google*). Weiterhin fiel auf, dass fünf der acht Dienste vorsehen, dass Profilinhalte und/oder Beiträge in externen Suchmaschinen gefunden werden können (*Facebook*, *Instagram*, *LinkedIn*, *Pinterest, Twitter*). Dies impliziert auch, dass öffentliche Inhalte unter Umständen auch für Personen sichtbar sind, die keine Mitglieder des Netzwerks sind beziehungsweise nicht eingeloggt sind.

Bewertung. Nach hier vertretener Auffassung sind Einstellungen zu Sichtbarkeit und Auffindbarkeit von personenbezogenen Daten für andere natürliche Personen von der Regelung zur datenschutzfreundlichen Grundeinstellung betroffen. Nach Art. 25 DSGVO muss sichergestellt werden, „*dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden*."

Im Fall von Sozialen Medien dürfen Nutzerprofile in der Ausgangseinstellung nur dem kleinstmöglichen Empfängerkreis angezeigt werden – das ist der Kreis an Personen, zu denen man einen Kontakt bestätigt hat. In Bezug auf die Sichtbarkeit von Profilinhalten stehen nach hier vertretener Auffassung sechs von acht Anbietern (*Facebook*, *Instagram*, *LinkedIn*, *Pinterest*, *Twitter*, *WhatsApp*) in Widerspruch zu dieser Regelung. In Bezug auf die geposteten Beiträge trifft dies auf fünf von acht Diensten zu (*Instagram, LinkedIn, Pinterest, Twitter, YouTube/Google*).

Für einige dieser Anbieter (z. B. *Twitter*) ließe sich entgegnen, dass der integrale Zweck des Dienstes der öffentliche Austausch von Nachrichten ist und die Voreinstellung zur Sichtbarkeit von Beiträgen eben diesen Zweck berücksichtigt. Gleichzeitig steht es mit Hilfe der Einstellungsoptionen jedem Nutzer frei, die eigenen Inhalte einem erweiterten Empfängerkreis zugänglich zu machen. Für diese Öffentlichkeit soll sich der Nutzer aktiv entscheiden, sodass eine Nichtveränderung der Einstellungen zu einem datenschutzfreundlichen Status Quo führt.[85]

[85][85] Kerber/Keppeler in Gola DSGVO/BDSG Art. 25 Rn. 64; s. auch LG Nürnberg-Fürth (7. Zivilkammer), Urteil vom 17.04.2018 - 7 O 6829/17 (nicht rechtskräftig); LG Berlin, Urteil vom 16.1.2018 – 16 O 341/15 (nicht rechtskräftig).

Tabelle 7. Voreinstellungen für Sichtbarkeit und Auffindbarkeit.

Dienst	nur für bestätigte Kontakte sichtbar	
	Profilinhalte	Beiträge/Status
Facebook	nein	ja
Instagram	nein	nein
LinkedIn	nein	nein
Pinterest	nein	nein[a]
Snapchat	ja[b]	ja
Twitter	nein[c]	nein
WhatsApp	nein	ja
YouTube (Google)	ja[c]	nein[d]

[a] Betrifft die Option „Pinnwand geheim halten“.
[b] Keine Einstellungsmöglichkeit vorhanden.
[c] Ausnahme: Geburtsdatum (*Twitter*) bzw. Geburtsjahr (*Google*).
[d] Bezieht sich auf Beiträge/Videos, die auf *YouTube* gepostet werden.

In diesem Kontext verstoßen nicht nur vorausgewählte Optionen gegen die Regelung der datenschutzfreundlichen Voreinstellung, die nutzergenerierte Inhalte sichtbar für Nicht-Mitglieder des Netzwerks macht (z. B. *LinkedIn*). Vielmehr sind nach hier vertretener Auffassung auch Einstellungen betroffen, die die Sichtbarkeit für alle *eingeloggten* Mitglieder ermöglicht (z. B. Profilinhalte auf *Facebook*). Schließlich kann jede beliebige Person zu jedem beliebigen Zeitpunkt einen Account erstellen. Insofern ist der potenzielle Empfängerkreis einer geteilten Information potenziell unbegrenzt, selbst wenn die Voreinstellung die Sichtbarkeit der Information auf das Netzwerk begrenzt.

4.5 Zwischenfazit: Privacy by default

Im Zuge der Registrierung und Nutzung der Accounts wurden verschiedene Auffälligkeiten offenbar. Neben einer Reihe von Einzelbeobachtungen wurden vier inhaltliche Bereiche identifiziert, die sich bei den analysierten Diensten wiederfanden und nach hier vertretener Auffassung mit der Vorschrift der datenschutzfreundlichen Voreinstellungen zusammenhängen:

Authentifizierungsdatum. In allen vier Fällen, in denen der Nutzer auswählen konnte, ob er sich mit seiner E-Mail-Adresse oder seiner Mobilfunknummer authentifiziert (*Facebook, Instagram, Twitter* und *Snapchat*), war die Mobilfunknummer als Authentifizierungsdatum voreingestellt. Die Preisgabe der Mobilfunknummer verhindert eine pseudonyme Nutzung des Dienstes und vereinfacht das Tracken des Nutzers zu Werbezwecken.

Kontaktsynchronisation. Mit nur zwei Ausnahmen (*YouTube/Google, Pinterest*) fordern alle Apps den Nutzer zur Synchronisation seiner Kontakte auf. Auffällig sind die Anzahl und Formulierungen der Aufforderungen, die dem Nutzer suggerieren, die Synchronisation der Kontakte sei erforderlich für die Nutzung des Dienstes. Durch die Synchronisation der Kontakte werden unter Umständen auch Daten von Personen an den Anbieter übermittelt, die sich gegen die Nutzung des Dienstes entschieden haben.

Personalisierte Werbung. Der Nutzer kann teilweise einschränken, inwieweit Tracking-Daten für die Personalisierung von Werbung genutzt werden. Das Nutzer-Tracking selbst kann kaum eingeschränkt werden.

Sichtbarkeit und Auffindbarkeit. In nur zwei Fällen (*Snapchat, YouTube/Google*) ist die Sichtbarkeit der Profilinhalte bzw. Beiträge auf die bestätigten Kontakte innerhalb des Netzwerks beschränkt. Bei allen übrigen Diensten waren diese Inhalte öffentlich sichtbar – das heißt im Mindesten für alle eingeloggten Nutzer, gegebenenfalls jedoch auch für Nicht-Mitglieder des Netzwerks.

5 FAZIT

In der vorliegenden Marktanalyse wurde untersucht, wie Anbieter Sozialer Medien mit ausgewählten Vorschriften der DSGVO umgehen. Ein besonderer Fokus der Prüfung lag auf den Informationspflichten sowie auf der Umsetzung der Regelung zu datenschutzfreundlichen Grundeinstellungen. Untersucht wurde dies für die Anbieter *Facebook*, *Instagram*, *LinkedIn*, *Pinterest*, *Snapchat*, *Twitter*, *WhatsApp* und *YouTube (Google)*.

Informationspflichten. In Bezug auf die Informationspflichten wurde festgestellt, dass in den betreffenden Datenschutzerklärungen in Bezug auf die Prüfpunkte (Zweck, Rechtsgrundlage, Dauer der Speicherung, Betroffenenrechte) überwiegend nicht ausreichend informiert wird. Bis auf eine Ausnahme wird in den geprüften Datenschutzerklärungen auf die Nennung der Rechtsgrundlage im Kontext der Zweckaufzählung für die Verarbeitung personenbezogener Daten verzichtet. Die Überprüfung ergab weiterhin, dass nur in einem Fall ein konkreter Speicherzeitraum für personenbezogene Daten ableitbar war. In Bezug auf die Empfänger der verarbeiteten personenbezogenen Daten bleiben die geprüften Angaben ebenfalls vage. Zwei Anbieter informieren nicht über alle bestehende Rechte der Betroffenen. Drei Anbieter machen die Betroffenenrechte nicht als gesetzlich festgelegtes Recht kenntlich.

Aus der Perspektive des Verbraucherschutzes muss daher bemängelt werden, dass sich Nutzer anhand der geprüften Informationen nicht ausreichend über die Hintergründe und Reichweite der Datenverarbeitung informieren können.

Privacy by default. Im Zuge der Registrierung und Nutzung des Accounts wurden folgende Bereiche identifiziert, die in Zusammenhang mit der Regelung datenschutzfreundlicher Voreinstellungen beziehungsweise dem zugrundeliegenden Grundsatz der Datenminimierung stehen: Authentifizierungsdatum, Kontaktsynchronisation, personalisierte Werbung und Sichtbarkeit und Auffindbarkeit.

Neben der Tatsache, dass bei vielen der betreffenden Einstellungsmöglichkeiten keine datenschutzfreundliche Variante vorausgewählt war, offenbart auch die Heterogenität der Einstellungsmöglichkeiten – insbesondere in Zusammenhang mit personalisierter Werbung – ein Problem für Verbraucher. So ist es nicht nur teilweise schwierig nachzuvollziehen, welche Kontrolle eine Einstellungsmöglichkeit tatsächlich bietet. Vielmehr können Anbieter sich entscheiden, bestimmte Einstellungsmöglichkeiten von vornherein nicht in den Dienst zu integrieren. Beispielsweise können Nutzer teilweise modifizieren, inwieweit Tracking-Daten für die Personalisierung von Werbung *genutzt* werden dürfen. Diese Einstellungsmöglichkeit kann

durchaus suggerieren, dass Kontrolle über personenbezogene Daten gewährt wird. Dies kann jedoch auch als Kontrollillusion verstanden werden, da gerade das in vielen Kontexten bedenkliche Ausmaß von Nutzer-Tracking nicht einschränkt werden kann.

Zusammenfassend offenbart die vorliegende Marktanalyse wesentliche Probleme in Bezug auf den Umgang von Anbietern Sozialer Medien mit Vorschriften der DSGVO: Auch nach dem 25.05.2018 bleiben auf Basis der Datenschutzerklärungen wesentliche Aspekte der Datenverarbeitung intransparent für den Nutzer. Hierdurch sowie durch die offenbarten Probleme im Bereich der datenschutzfreundlichen Voreinstellungen wird es Nutzern nach wie vor erschwert, die Kontrolle über ihre personenbezogenen Daten zu behalten.

6 QUELLEN

Literatur

Ackerman, L. (2013). Mobile health and fitness applications and information privacy: Report to California Consumer Protection Foundation. Privacy Rights Clearinghouse. Abgerufen von https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks [Stand: 12.01.2017].

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM conference on Electronic commerce 21-29. New York, USA. Abgerufen von http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf [Stand: 11.01.2017].

Artikel-29-Datenschutzgruppe (2013). Opinion 03/2013 on purpose limitation. Working Paper 203. Abgerufen von http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Stand: 10.09.2018].

Artikel-29-Datenschutzgruppe (2018). Guidelines on transparency under Regulation 2016/679. Working Paper 260, rev.1. Abgerufen von https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf [Stand: 10.09.2018].

Artikel-29-Datenschutzgruppe (2009). Stellungnahme 05/2009 zur Nutzung sozialer Online-Netzwerke Working Paper 163, rev.1. Abgerufen von https://cnpd.public.lu/content/dam/cnpd/de/publications/groupe-art29/wp163_de.pdf [Stand: 10.09.2018].

Berger, D. (2018). Werbung bei WhatsApp: Jetzt wird Geld verdient!. *Heise* (03.08.2018). Abgerufen von https://www.heise.de/newsticker/meldung/Werbung-bei-WhatsApp-Jetzt-wird-Geld-verdient-4128652.html [Stand: 10.09.2018].

Biselli, A. (2017). Interaktive Karte: Registrierungspflicht für Prepaid-SIM-Karten in Europa weit verbreitet. Netzpolitik.org. Abgerufen von https://netzpolitik.org/2017/interaktive-karte-registrierungspflicht-fuer-prepaid-sim-karten-in-europa-weit-verbreitet/ [Stand: 05.09.2018].

Bitkom (2016a). Zwei von drei Internetnutzern sind in sozialen Netzwerken aktiv. Abgerufen von https://www.bitkom.org/Presse/Presseinformation/Zwei-von-drei-Internetnutzern-sind-in-sozialen-Netzwerken-aktiv.html [Stand: 07.08.2018].

Bitkom (2016b). Zwei von drei Internetnutzern verwenden Messenger. Abgerufen von https://www.bitkom.org/Presse/Presseinformation/Zwei-von-drei-Internetnutzern-verwenden-Messenger.html [Stand: 07.08.2018].

Bitkom (2018). Social-Media-Trends 2018. Abgerufen von https://www.bitkom.org/Presse/Anhaenge-an-PIs/2018/180227-Bitkom-PK-Charts-Social-Media-Trends-2.pdf [Stand: 10.08.2018].

Boyd, D. & Crawford, K. (2012). Critical Questions for Big Data: Provocations for a Cultural, Technological and Scholarly Phenomenon. *Information, Communication & Society 5*(15), 662–679. Abgerufen von http://www.danah.org/papers/2012/BigData-ICS-Draft.pdf [Stand: 16.11.2017].

Christl, W. (2017). Corporate surveillance in everyday life. How companies collect, combine, analyze, trade, and use personal data on billions. A report by Cracked Labs. Abgerufen von http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf [Stand: 13.08.2018].

Dachwitz, I. (2018). Verhaltensbasierte Werbung: Facebook identifiziert emotional verletzliche Jugendliche. Netzpolitik.org. Abgerufen von https://netzpolitik.org/2017/verhaltensbasierte-werbung-facebook-australien-analysiert-emotionen-und-aengste-von-jugendlichen/ [Stand: 04.09.2018].

Datenschutzkonferenz (2017). Kurzpapier Nr. 3 – Verarbeitung personenbezogener Daten für Werbung. Abgerufen von https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_3_Werbung.pdf [Stand: 18.09.2018].

Feierabend, S., Plankenhorn, T., Rathgeb, T. (2017). JIM-Studie 2017 – Jugend, Information, (Multi-) Media. Basisuntersuchung zum Medienumgang 12-19-Jähriger. Medienpädagogischer Forschungsverbund Südwest (Hrsg.). Abgerufen von http://www.mpfs.de/studien/jim-studie/2017/ [Stand: 27.02.2018].

FORBRUKERRÅDET (2018). Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy. Abgerufen von https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [Stand: 07.08.2018].

Gandomi, A. & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35, S. 137-144.

Greis, F. (2018). WhatsApp teilt nun massenhaft Daten mit Facebook. *Golem* (23.05.2018). Angerufen von https://www.golem.de/news/trotz-dsgvo-whatsapp-teilt-nun-massenhaft-nutzerdaten-mit-facebook-1805-134528.html [Stand: 10.09.2018].

Herrmann, D. & Lindemann, J. (2016). Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights? *CoRR*, abs/1602.0. Abgerufen von http://arxiv.org/abs/1602.01804 [Stand: 11.01.2017].

Johnson, E.J. & Goldstein, D. (2003). Do defaults save lives? *Science*, *302*(5649), 1338-1339. Abgerufen von http://www.dangoldstein.com/papers/DefaultsScience.pdf [Stand: 13.08.2018].

Kaiser, L. (2018). Facebook-Bug gab Werbekunden die Telefonnummern von Nutzern preis. Netzpolitik.org. Abgerufen von https://netzpolitik.org/2018/facebook-bug-gab-werbekunden-die-telefonnummern-von-nutzern-preis/ [Stand: 11.09.2018].

Koch, W. & Frees, B. (2017). ARD/ZDF-Onlinestudie 2017: Neun von zehn Deutschen online. Media Perspektiven 9/2017, S. 444. Abgerufen von http://www.ard-zdf-onlinestudie.de/files/2017/Artikel/917_Koch_Frees.pdf [Stand: 26.02.2018].

Meister, A. (2013). Willst du einen Kredit? Aber nur, wenn uns deine Facebook-Freunde passen und du uns in deinen PayPal Account lässt. *Netzpolitik.org.* Abgerufen von https://netzpolitik.org/2013/willst-du-einen-kredit-aber-nur-wenn-uns-deine-facebook-freunde-passen-und-du-uns-in-deinen-paypal-account-laesst/ [Stand: 10.09.2018].

Meyer, R. (2018). The Cambridge Analytica Scandal, in 3 Paragraphs. Abgerufen von https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/ [Stand: 04.09.2018]

Moll, R., Pieschl, S., & Bromme, R. (2014). Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in Human Behavior*, *41*, 212-219.

Moll, R., Scheibel, L. & Rusch-Rodosthenous, M. (2017). Digitale Gesundheit – Anbieter-kommunikation über Datenschutz am Beispiel von Wearables und Fitness-Apps. In V. Scherenberg & J. Pundt (Hrsg.). *Digitale Gesundheitskommunikation. Zwischen Meinungsbildung und Manipulation*, (S. 293-305). Bremen: APOLLON University Press.

Plattform Verbraucherschutz in einer digitalisierten Welt (2015). One Pager: Muster für transparente Datenschutzhinweise. Abgerufen von

https://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html [Stand: 07.08.2018].

PricewaterhouseCoopers GmbH (PwC) (2018). Vertrauen in Medien. Abgerufen von https://www.pwc.de/de/technologie-medien-und-telekommunikation/pwc-studie-vertrauen-in-medien-2018.pdf [Stand: 07.08.2018].

Reece, A. G., Reagan, A. J., Lix, K. L. M., Dodds, P., Danforth, C. M. & Langer, E. J. (2016). Forecasting the onset and course of mental illness with Twitter data. *Scientific Reports*, *7*. [Stand: 07.03.2018].

Samuelson, W. & Zeckhauser, R. (1988). Status quo bias in decision-making. *Journal of Risk and Uncertainty*, *1*, 7–59. Abgerufen von http://doi.org/10.1007/bf00055564 [Stand: 13.08.2018].

Scheffler, H. (2014). Soziale Medien. Einführung in das Thema aus Sicht der Marktforschung. In C. König C., M. Stahl & E. Wiegand (Hrsg.). *Soziale Medien*. Schriftenreihe der ASI – Arbeitsgemeinschaft Sozialwissenschaftlicher Institute (S. 13-27). Wiesbaden: Springer VS.

Statista Dossier (2017). Instant Messenger. Abgerufen von https://de.statista.com/download/MTUzMzYzNjU0NSMjNzE5NjE4IyMyMTY2MSMjMSMjcGRmIyNTdHVkeQ== [Stand: 07.08.2018].

Statista (2018a). Nutzerzahlen von Facebook in Deutschland. Abgerufen von https://de.statista.com/statistik/daten/studie/711113/umfrage/nutzerzahlen-von-facebook-in-deutschland/ [Stand: 28.08.2018].

Statista (2018b). Statistiken zu WhatsApp. Abgerufen von https://de.statista.com/themen/1995/whatsapp/. [Stand: 28.08.2018].

Statista (2018c). Statistiken zu Instagram. Abgerufen von https://de.statista.com/themen/2506/instagram/ [Stand: 13.08.2018].

Statista (2018d). Statistiken zu Twitter. Abgerufen von https://de.statista.com/themen/99/twitter/ [Stand: 13.08.2018].

Statista (2018e). Statistiken zu YouTube. Abgerufen von https://de.statista.com/themen/162/youtube/ [Stand: 13.08.2018].

Statista (2018f). Endkundenabsatz von Smartphones weltweit nach Betriebssystem von 2009 bis 2017 (in Millionen Stück). Abgerufen von

https://de.statista.com/statistik/daten/studie/12881/umfrage/weltweiter-absatz-von-smartphones-nach-betriebssystem-seit-2009/ [Stand: 12.09.2018].

Verbraucherzentrale Bundesverband (2018). Anwendbarkeit des Telemediengesetzes - Stellungnahme des Verbraucherzentrale Bundesverbands e. V. zur Positionsbestimmung der Datenschutzkonferenz „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018. Abgerufen von https://www.vzbv.de/sites/default/files/downloads/2018/06/29/18-06-28_vzbv-stellungnahme_dsk_tmg-dsgvo.pdf [Stand: 13:08.2018].

Kommentare und Handbücher

Brink, S. & Wolf, A. (2018). BeckOK Datenschutzrecht, Kommentar (24. Auflage). München: Verlag C. H. Beck.

Esser, M. (2018). Auernhammer DSGVO/BDSG, Kommentar (6.Auflage). Köln: Carl Heymanns Verlag.

Gola, P. (2016). Datenschutzgrundverordnung, Kommentar (2. Auflage). München: Verlag C. H. Beck.

Härting, N. (2016). Datenschutzgrund-verordnung, Kommentar (2. Auflage). Köln: Verlag Otto Schmidt.

Kühling, J. & Buchner, B. (2018). Datenschutzgrundverordnung/BDSG, Kommentar (2. Auflage). München: Verlag C. H. Beck.

Paal, B. & Pauly, D. (2018). Datenschutzgrundverordnung & Bundesdatenschutzgesetz, Kommentar (2. Auflage). München: Verlag C. H. Beck.

Plath, K.-U. (2018). DSGVO/BDSG, Kommentar (3. Auflage). Köln: Verlag Dr. Otto-Schmidt.

Schantz, P. (2016). Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016.

Schwartmann, R., Jaspers, A., Thüsing, G. & Kugelmann, D. (2018). Datenschutzgrundverordnung & Bundesdatenschutzgesetz Kommentar (2. Auflage). München: Verlag C. H. Beck.

Schmidl, M. (2014). IT-Recht von A-Z, Kommentar (2. Auflage). München: Verlag C. H. Beck.

Zitiervorschlag:

Moll, R., Horn, M., Scheibel, L., & Rusch-Rodosthenous, M. (2018). Soziale Medien und die EU-Datenschutzgrundverordnung Informationspflichten und datenschutzfreundliche Voreinstellungen. Verbraucherzentrale NRW e. V. (Hrsg.). Online verfügbar unter https://www.marktwaechter.de/digitale-welt/marktbeobachtung/soziale-medien-und-die-dsgvo

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

IMPRESSUM

Herausgeber
Verbraucherzentrale NRW e. V.
Mintropstr. 27, 40215 Düsseldorf
Tel. (0211) 38060
Fax (0211) 3809 172
marktwaechter@verbraucherzentrale.nrw

Text: Dr. Ricarda Moll, Marco Horn, Lisa Scheibel, Miriam Rusch-Rodosthenous

Titelbild: Vasily Merkushev/Fotolia
Gestaltung: Ute Böhm
Stand: September 2018

verbraucherzentrale