www.jusletter-it.eu

Philipp Fischer

Privacy by (Re)Design bei Apps für Smart Devices

Nutzer von Mobilen Endgeräten (Smart Devices) haben eine zunehmend unüberschaubare Quantität an Applications (Apps) installiert und wenden diese immer alltäglicher für derart intensive Funktionalitäten an, dass dies oft zu Lasten des Datenschutzes und somit ihres Grundrechts auf informationelle Selbstbestimmung geht. Apps werden so zu den neuesten «Datenschleudern». Dieser Beitrag befasst sich mit der Problematik, wie aus datenschutzrechtlicher Sicht einerseits personenbezogene Daten geschützt und andererseits eine benutzerfreundliche Nutzung von Apps ermöglicht werden kann. Eine Lösung dieses Spannungsfeldes könnten die Prinzipien des sog. «Privacy by ReDesign» (PbRD) bieten, welches einen technisch-organisatorischen Ansatz beinhaltet und so möglicherweise dem Recht in die Praxis helfen kann.

Collection: Tagungsband-IRIS-2013
Category: Articles
Field of law: Data Protection
Region: Germany

Citation: Philipp Fischer, Privacy by (Re)Design bei Apps für Smart Devices, in: Jusletter IT 20 February 2013

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1 Einleitung

[Rz 1] In seiner Ausgabe Juni 2012 meldet das deutsche Verbrauchmagazin «test», dass viele Apps personenbezogene Daten (§ 3 BDSG[1]) der Smartphone-Besitzer an Datensammler unverschlüsselt übertragen; «für den Service, den diese Apps bieten, zahlen Nutzer mit ihrer Privatsphäre»[2]. Von 63 geprüften Anwendungen stufte Stiftung Warentest 28 datenschutzrechtlich als kritisch ein. Darunter sind auch «sehr kritische» Anwendungen, zu denen bekannte Apps wie WhatsApp, Facebook, Foodspotting, iTranslate oder Clever tanken zählen.

[Rz 2] Apps sind eine junge Entwicklung. Mit dieser einher zu gehen scheint leider auch, die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ohne gesetzliche Erlaubnis (§ 4 I BDSG) und ohne Einwilligung (§ 4a BDSG) durchzuführen. Bundesverbraucherministerin Ilse Aigner warnte, die Sicherheit der Smartphones hinke der technischen Entwicklung oft hinterher.[3] Auch Datenschützer Dix merkt an, dass derartig datenschutzfeindliche Geschäftsmodelle der «falsche Weg» seien; die Anbieter fragten User nicht etwa nach ihren Vorlieben, sondern beobachten sie.[4]

[Rz 3] Es fragt sich aus datenschutzrechtlicher Sicht, wie einerseits personenbezogene Daten geschützt werden können; andererseits, so Dieter Kempf, dürfe es aber nicht so weit kommen, dass Internetdienste zu einem Hindernisparcours für User werden, sonst «verliert das Smartphone seinen Charme». Die benutzerfreundliche Nutzung einer App muss ermöglicht werden. Eine Lösung könnte das Prinzip des sog. «Privacy by ReDesign» (Pb^{R}D) bieten. Urheberin dieses Prinzips

1 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist.

2 Stiftung Warentest Magazin, Juni 2012, Seite 1.

3 Die Welt vom 07.02.2012, «IT-Branche fürchtet Datenschutz als Konsumbremse», abrufbar unter http://www.welt.de/politik/deutschland/article13855394/IT-Branche-fuerchtet-Datenschutz-als-Konsumbremse.html.

4 Die Zeit vom 24.05.2012, abrufbar unter http://www.zeit.de/digital/datenschutz/2012-05/apps-datenschutz-warentest

ist die Datenschutzbeauftragte von Kanada, Ann Cavoukian.[5]

2 Das Problem: Datenschutz bei Apps für Smart Devices

2.1 Begriffsbestimmung und Nutzerverhalten

[Rz 4] Im allgemeinen Sprachgebrauch werden unter Smart Devices verschiedene mobile Endgeräte, z.B. Smartphones, Tablet-Computer und Personal Digital Assistants (PDAs) zusammengefasst. Solche zeichnen sich durch die ortsunabhängige Verfügbarkeit von Daten des Personal Information Manager (PIM) und auf Endgeräten nutzbaren Anwendungen sowie die gleichzeitige Nutzungsmöglichkeit von Funk-, Mobilfunk- (GSM, GPRS, UMTS, EDGE) und anderen Telekommunikationsdiensten aus.

[Rz 5] Smart Devices gewinnen im Alltag zunehmend an Bedeutung. Im vergangenen Jahr machten sie weltweit bereits 70 Prozent aller Geräteverkäufe aus, in diesem Jahr soll der Absatz von 821 Millionen auf 1,2 Milliarden Geräte ansteigen.[6] Dies bleibt auch in Deutschland nicht ohne Auswirkungen. Nach einer Umfrage im vergangenen Oktober nutzen 29,5 Millionen Deutsche ein Smartphone, was einem Anteil an Mobiltelefonen in Höhe von 35 % entspricht, bei den unter 30 Jährigen sind es gar 58 %.[7] Die beliebtesten Funktionen bei Smartphones sind E-Mails lesen und Nachrichten über soziale Netzwerke austauschen. So prüfen 70 % der Männer und 55 % der Frauen täglich oder mehrmals die Woche ihre E-Mails auf dem Handy. 52 % der Männer und 61 % der Frauen tauschen sich in sozialen Netzwerken aus.[8]

[Rz 6] Smart Devices verfügen also über die verschiedensten Anwendungsmöglichkeiten. Hierzu zählen mobiles Internet, Navigations-, Ortungs- und Kartendienste, mobiler E-Mail-Zugang sowie viele weitere hilfreiche Anwendungen – die sogenannten «Applications» oder kurz «Apps». «Mehr als 15 Millionen Handybesitzer nutzen Apps, im Schnitt sind 17 Programme pro Gerät installiert»[9]. 80 % aller Internetnutzer haben ein persönliches Profil im Internet, auf das sie auch über Smart Devices zugreifen könnten – das sind 43 Millionen Personen.

2.2 Faktischer Datenumgang

[Rz 7] Die Nutzung von Apps (Software) und Smart Devices (Hardware) kann potenziell mit Daten aus Social Media Profilen (Internet) desselben Nutzers verknüpft werden; ein für den Datenschutz gefährliches Triumvirat. Denn zunächst an und für sich unbedeutende Daten aus einer dieser Quellen werden derart miteinander verknüpft, dass sich ein umfangreiches Nutzerprofil einer natürlichen Person ergibt, das einen hohen Wert für betriebswirtschaftliche Zwecke verschiedenster Unternehmen hat.

---

5 www.privacybydesign.ca.

6 http://www.computerwoche.de/a/smartphones-und-tablets-weiter-im-aufwind,2526981.

7 http://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/.

8 http://www.handelsblatt.com/technologie/it-tk/mobile-welt/safer-internet-day-bei-smartphones-verstaerkt-auf-datenschutz-achten/6178736.html.

9 http://www.handelsblatt.com/technologie/it-tk/mobile-welt/safer-internet-day-bei-smartphones-verstaerkt-auf-datenschutz-achten/6178736.html.

[Rz 8] Vielen Anwendern ist nicht bewusst, dass insbesondere viele unentgeltlich erhältliche Apps aus den App Stores keineswegs völlig kostenfrei sind. Denn «nichts im Internet ist kostenlos»[10], sagt Kempf. Und wenn nicht in Euro und Cent, so «zahlen die Nutzer doch mit ihren persönlichen Daten»[11]. «Daten sind die Währung des Internets», sagt auch Bundesverbraucherministerin Aigner. Die Gegenleistung besteht häufig in der Überlassung personenbezogener Daten an Anbieter, welche diese Daten wiederum zumeist entgeltlich an fast ausschließlich im Bereich Datenanalyse tätige, auf Gewinn ausgerichtete Unternehmen wie Flurry, Localytics und Mobclix weitergeben.

[Rz 9] Beispielhaft verdeutlicht der App-Primus[12] «WhatsApp» das datenschutzrechtliche Dilemma. Noch vor wenigen Monaten behielt sich dessen Anbieter das Recht vor, personenbezogene Daten der Anwender an Dritte weiterzugeben, verlangte Zugriff sowohl auf E-Mail-Adresse, Handynummer als auch das komplette Telefonbuch des Anwenders und übertrug Nachrichten unverschlüsselt. Daraufhin wurde die App gemeinsam durch den niederländischen und den kanadischen Datenschutzbeauftragten untersucht und die Ergebnisse am 28.01.2013 per Pressemitteilung[13] mitgeteilt. Danach hat der Anbieter bereits während der Untersuchung Änderungen zum Schutz der persönlichen Informationen vorgenommen beziehungsweise will er weitere Änderungen durchführen. Jacob Kohnstamm, niederländischer Datenschutzbeauftragter, bemängelt trotz dieser Fortschritte, dass bestimmte Verhaltensweisen der App noch immer gegen niederländisches und kanadisches Datenschutzrecht verstoßen.[14]

2.3 Relevantes Kollisions- und Sachrecht

[Rz 10] Um zu wissen, an welcher Stelle technisch-organisatorische Maßnahmen denn das Recht als solches komplementieren müssen, muss festgestellt werden, welches Recht Anwendung findet. Da Drittfirmen wie Flurry, Localytics oder Mobclix, deren Geschäftsmodell auf der entgeltlichen Weitergabe aufbereiteter personenbezogener Daten aus Apps beruht, ihren Sitz oft im Ausland haben, ist fraglich, ob deutsches Datenschutzrecht kollisionsrechtlich einschlägig ist, vgl. § 1 Abs. 5 S. 2 BDSG. Zu einer Anwendung des BDSG gelangt man sowohl über das Territorialitäts- als auch das Sitzprinzip. Ersteres gilt, wenn ein Anbieter zwar im EU/EWR-Ausland seinen Sitz hat, jedoch «Mittel» (Art. 4 Abs. 1 lit. c der EU-Datenschutzrichtlinie[15]) verwendet, die in Deutschland belegen sind; ein solches Mittel ist eine App[16]. Hat der Anbieter seinen Sitz innerhalb der EU/EWR, so findet das im jeweiligen Mitgliedsstaat geltende Datenschutzrecht Anwendung, sofern nicht ausnahmsweise der Umgang mit personenbezogenen Da-

10 http://www.welt.de/politik/deutschland/article13855394/IT-Branche-fuerchtet-Datenschutz-als-Konsumbremse.html.

11 http://www.welt.de/politik/deutschland/article13855394/IT-Branche-fuerchtet-Datenschutz-als-Konsumbremse.html.

12 Mit Stand 30.01.2013 die weltweit am häufigsten verkaufte non-games App sowohl in Apple´s App Store als auch in Google´s Play Store.

13 http://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp.

14 http://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp.

15 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 – 0050.

16 Zustimmend *Stadler*, S. 58.

ten durch eine deutsche Niederlassung erfolgt. Wegen der Vollharmonisierung des europäischen Datenschutzrechts ist das Sitzprinzip nur noch von untergeordneter Bedeutung.

[Rz 11] Anstatt einer personenbezogenen[17] IP-Adresse wird im mobilen Bereich die ebenfalls personenbezogene «unique device identifier» (UDID) verwendet. Name, Adresse, E-Mail-Adresse, Handynummer u.a. sind ebenso personenbezogene Daten (§ 3 Abs. 1 BDSG). Der Anbieter einer App ist somit verantwortliche Stelle (§ 3 Abs. 7 BDSG). Sachrechtlich ist das deutsche Datenschutzrecht einschlägig. Zudem ist im nationalen Recht wegen § 1 Abs. 3 S. 1 BDSG auf die Abgrenzung von BDSG, TMG[18] und TKG[19] einzugehen; letztere könnten dem BDSG eventuell als bereichsspezifischere Regelungen (§ 11 ff. TMG und §§ 91 ff. TKG) vorgehen.

[Rz 12] Sofern der Anwendungsbereich von TMG oder TKG eröffnet ist, tritt das BDSG gemäß § 1 Abs. 3 S. 1 BDSG als subsidiär zurück. Nach dem Schichtenmodell gilt – vereinfacht ausgedrückt – das TKG für die Transportebene («Telekommunikationsrecht», z.B. DSL) der Daten, während ein Telemediendienst und somit das TMG anwendbar ist, wenn die Dienstebene («Online-Recht», z.B. Kennungen, Passwörter) betroffen ist, und das BDSG findet Anwendung auf die Inhaltsebene («Offline-Recht», z.B. Bankdienste, Onlinebestellformulare).

[Rz 13] Es kann aber auch Apps geben, die mehrere Funktionalitäten anbieten. An dieser Stelle wird eine Zuordnung zu TMG und TKG selbst für den erfahrenen Fachanwalt im IT-Recht schwierig, für den Laien wohl ungleich schwerer nachzuvollziehen. Denn das deutsche Recht verbietet eine schwerpunktmäßige Betrachtung und es muss diese Zuordnung für jeden Teil einer App gesondert durchgeführt werden.

2.4 Recht auf Anonymität oder Pseudonymität

[Rz 14] § 3a S. 2 BDSG schreibt vor, dass personenbezogene Daten, sofern nach dem Zweck der Datenverarbeitung möglich und zumutbar, zu anonymisieren oder pseudonymisieren sind. Gleiches findet sich in § 13 Abs. 6 S. 1 TMG für die anonyme oder pseudonyme Nutzung von Telemediendiensten. Dieses Recht ignorieren die meisten Apps.

2.5 Verbotsprinzip und Erlaubnistatbestände

2.5.1 Verbotsprinzip

[Rz 15] Nach § 4 Abs. 1 BDSG gilt das Verbotsprinzip. Ein Umgang mit personenbezogenen Daten ist nur dann gestattet, wenn der Betroffene eingewilligt hat oder das BDSG oder eine andere Rechtsvorschrift dies erlaubt.

---

17 Unter anderen *Hoeren*, S. 4.

18 Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist.

19 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958) geändert worden ist.

2.5.2 Einwilligung

[Rz 16] Bereits vor Beginn der ersten Erhebung personenbezogener Daten müsste der Anwender einer App einwilligen, § 4a Abs. 1 BDSG, § 13 Abs. 2 TMG und § 94 TMG. Eine wirksame Einwilligung muss schriftlich und freiwillig erfolgen, sie kann unter den Voraussetzungen der § 13 Abs. 2 TMG und § 94 TMG auch elektronisch erteilt werden. § 28 Abs. 3a S. 1 BDSG schreibt diese Voraussetzungen nur für die Zwecke des Adresshandels und der Werbung fest, entspricht inhaltlich aber § 13 Abs. 2 TMG und § 94 TMG. Für die elektronische Einwilligung bedarf es weder der elektronischen Form (§§ 126 Abs. 3, 126a BGB) noch der Textform (§ 126b BGB), es genügt der «Klick» auf eine dann aber entsprechend deutlich darzustellende Schaltfläche innerhalb der App.

[Rz 17] Der Anwender ist vor Einwilligung besonders hinzuweisen i.S.d. § 4 Abs. 1 S. 2 BDSG. Die Einwilligung ist nur wirksam, «wenn sie auf der freien Entscheidung des Betroffenen beruht», § 4a Abs. 1 S. 1 BDSG. Die Freiwilligkeit ist dann zweifelhaft, wenn die Einwilligung nicht frei von äußerem Druck erfolgt. Ein solcher ist regelmäßig dann anzunehmen, wenn gegen das in § 28 Abs. 3b S. 1 BDSG und § 95 Abs. 5 S. 1 TKG normierte Kopplungsverbot verstoßen wird. An der bewussten und eindeutigen Einwilligungserklärung des Anwenders fehlt es auch dann, wenn dieser die Einwilligung nicht wissentlich und willentlich erteilt.

[Rz 18] Weiterhin werden Smart Devices oft von mehreren Anwendern genutzt und bislang bietet deren Technik keine zuverlässige Benutzerverwaltung. Es könnten somit verschiedene Anwender Datenverarbeitungsvorgänge beginnen und in diese zuvor einwilligen. Läge eine solche wirksame Einwilligung eines Anwenders X für eine App vor, und benutzt anschließend Anwender Y dieselbe App, so hat Anwender Y selbst noch nicht wirksam eingewilligt. Zumeist hat sich das Smart Device – mangels anderweitiger Funktionalität – die Einwilligung des Anwenders X bereits gemerkt und Anwender Y wird schlicht nicht mehr oder mangelhaft über seine Rechte aus §§ 4 Abs.1, 4a BDSG informiert.

[Rz 19] Das Recht trifft auch besondere Vorkehrungen hinsichtlich der Minderjährigkeit der Anwender, Apps treffen diese meist nicht. Zwar verlangt §4a Abs. 1 S. 1 BDSG lediglich Einsichtsfähigkeit in die Tragweite der Einwilligung, nicht auch Geschäftsfähigkeit.[20] Wann aber von einer Einsichtsfähigkeit ausgegangen werden kann, bedarf einer Einzelfallabwägung, die wiederum von dem Verwendungszweck der personenbezogenen Daten abhängt.

[Rz 20] Ist die Einwilligung erteilt worden, so ist sie zu protokollieren und dem Anwender die Möglichkeit zu geben, die Einwilligung jederzeit abzurufen und zu widerrufen. Viele Anbieter scheinen auch den Zweckbindungsgrundsatz zu vergessen. Danach darf ein Dritter, dem die Daten übermittelt worden sind, diese nur für den Zweck verarbeiten und nutzen, für den die Einwilligung des Betroffenen zuvor gegeben wurde, § 28 Abs. 5 BDSG.

2.5.3 Erlaubnistatbestände

[Rz 21] Die Erlaubnistatbestände in BDSG, TMG und TKG sind sehr zahlreich und können hier nicht umfassend behandelt werden. Für die spätere Betrachtung des Pb^RD müssen aber zwei Abgrenzungen vorab geklärt sein:

[20] *Wintermeier*, S. 212; *Jandt/Roßnagel*, S. 640.

[Rz 22] Zum einen muss bei den Datenverarbeitungsvorgängen in der App *zwischen* Inhaltsebene (BDSG), Diensteebene/Interaktionsebene (TMG) und Telekommunikationsebene/Erlaubnistatbestände (TKG) unterschieden werden, um hernach auch die entsprechenden Erlaubnistatbestände im richtigen Gesetz anzuwenden.

[Rz 23] Zum anderen muss *innerhalb* des richtigen Gesetzes ein Erlaubnistatbestand für die verarbeitete «Datenart» gefunden werden. Im TKG ist dafür eine Abgrenzung zwischen Bestandsdaten (Definition in § 3 Nr. 3 TKG), Verkehrsdaten (Definition in § 3 Nr. 30 TKG) und Standortdaten (Definition in § 3 Nr. 19 TKG) notwendig. Im TMG gilt Ähnliches für Bestandsdaten (Definition in § 14 Abs. 1 TMG) und Nutzungsdaten (Definition in § 15 Abs. 1 TMG).

3 Eine mögliche Lösung: Privacy by ReDesign

3.1 Begriffsbestimmung

3.1.1 Privacy by Design (PbD)

[Rz 24] Das Recht stellt das Design als mögliche Lösung also vor große Aufgaben. PbD stützt die Auffassung, dass die Zukunft des Datenschutzes nicht allein durch die Einhaltung von Rechtsvorschriften gewährleistet werden kann; vielmehr sollte idealerweise die Gewährleistung des Datenschutzes zum Standardbetriebsmodus einer Organisation werden. Ursprünglich wurde der Einsatz datenschutzfreundlicher Technologien («privacy enhancing technologies», kurz PETs) als Lösung angesehen. Aktuell wird die Erweiterung des Einsatzes von Technologien auf PETs Plus – die Aufnahme eines Positivsummenansatzes (volle Funktionalität) und keines Nullsummenansatzes – versucht.

[Rz 25] PbD erstreckt sich auf eine «Trilogie» von umfassenden Anwendungen: 1) IT-Systeme, 2) verantwortungsvolle Geschäftspraktiken und 3) physikalisches Design und vernetzte Infrastrukturen. Die Grundsätze des PbD sind auf alle Arten personenbezogener Informationen anwendbar, sie sollten aber mit besonderem Nachdruck auf sensible Daten wie medizinische und finanzielle Daten angewendet werden. Die Intensität der datenschutzrechtlichen Maßnahmen muss der Sensibilität der Daten gerecht werden.

[Rz 26] Die Ziele des PbD können durch die Anwendung der folgenden 7 Grundprinzipien erreicht werden:

- *Proaktiv, nicht reaktiv, als Vorbeugung nicht als Abhilfe*: Durch technische Maßnahmen soll ein Verstoß gegen datenschutzrechtliche Vorschriften vermieden werden, bevor sie eintreten.
- *Datenschutz als Standardeinstellung*: Das aktuell höchste Datenschutzniveau wird als Basisstandard voreingestellt.
- *In das Design eingebetteter Datenschutz*: Datenschutzrechtlich relevante Vorgänge werden bereits im Entwicklungsstadium berücksichtigt.
- *Volle Funktionalität, eine Positivsumme, keine Nullsumme*: Die mit dem Datenschutz kollidierende Funktionalität wird angemessen berücksichtigt.
- *Konstanter Schutz während des gesamten Lebenszyklus*: Datenschutzrelevante Aspekte sollen während des gesamten Umgangs mit den personenbezogenen Daten, von der Erhebung bis zur Löschung, berücksichtigt werden.
- *Sichtbarkeit und Transparenz*: Der Betroffene ist von Anfang an umfassend zu informieren, wie mit seinen personenbezogenen Daten umgegangen wird.

- *Durch nutzerzentrierte Gestaltung* die Privatsphäre der Nutzer wahren: Die Technik soll es dem Nutzer ermöglichen, die Datenschutzeinstellungen selbst zu bestimmen.

3.1.2 Privacy by ReDesign (PbRD)

[Rz 27] Viele Organisationen operieren mit bestehenden, relativ ausgereiften IT-Systemen und Unternehmenspraktiken, die sie über die Jahre entwickelt haben und die untrennbar mit alltäglichen Geschäftsabläufen verbunden sind. Solche Systeme auszutauschen steht dann meist nicht auf der Agenda. Die Aufgabe der Implementierung von PbD in solche Systeme kommt dann dem Pb^{R}D zu, einer Erweiterung von PbD. Bezogen auf Smart Devices muss bei bereits in Service Operation laufenden Apps das Ziel sein, sich dem Endzustand von PbD, den höchsten Standards für den Schutz personenbezogener Daten, zu nähern. Dies soll laut der Urheberin von PbD unterstützt werden durch die «3 R» des Pb^{R}D: «Rethink, Redesign, and Revive».

- *Rethink (Umdenken)* lädt Unternehmen ein, ihre Strategien zur Risikominderung zu überprüfen, für ihre Systeme und Prozesse – einschließlich Informationstechnologien, Geschäftspraktiken, physikalisches Design, und vernetzte Infrastruktur – alternative Ansätze zu finden, die einen besseren Datenschutz innerhalb der App gewährleisten. Dies kann auch Untersuchungen darüber einschließen, wie viele personenbezogene Daten überhaupt für die App notwendig sind und wie lange diese für den Betrieb bereitgehalten werden müssen.
- *Redesign (Neugestalten)* bietet die Chance, Verbesserungen umzusetzen, einerseits einen funktionaleren Datenschutz zu implementieren, gleichermaßen aber auch dafür Sorge zu tragen, dass die wichtigsten Business-Anforderungen in einer win-win-Beziehung erreicht werden. Eine Neugestaltung wird wahrscheinlich dann spiegelbildlich bei bestehenden Datenbanken beachtet werden, Daten müssen kaskadiert und gelöscht werden, unnötige Datenfelder beseitigt werden.
- *Revive (Wiederbeleben*) des Systems in einer neuen, den Datenschutz verbessernden Umgebung, ist das endgültige Ziel.

3.2 Privacy by ReDesign im (künftigen) Gemeinschaftsrecht

[Rz 28] Im europäischen Gemeinschaftsrecht existiert keine ausdrückliche Verpflichtung, datenschutzrechtliche Aspekte bereits während Entwicklung und Herstellung einer App zu beachten. Dies soll sich mit dem aktuellen Entwurf der Europäischen Datenschutz-Grundverordnung[21] und der Europäischen Datenschutzrichtlinie[22] ändern. Beide[23] sehen die Verpflichtung zur Vornahme von technischen und organisatorischen Maßnahmen und Verfahren zur Wahrung der Betroffenenrechte vor. Dies bedeutet für die Akzeptanz von PbRD einen wesentlichen Fortschritt, da» «data protection by design and by default»Vgl. Art. 23 der Grundverordnung sowie Art. 19

[21] Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM/2012/011, abrufbar unter http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.

[22] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_de.pdf.

[23] Die Grundverordnung in Erwägungsgrund (66), die Richtlinie in Erwägungsgrund (46).

der Richtlinie.[24] so unmittelbar geltendes Recht innerhalb der EU/EWR würde.

3.3 Privacy by ReDesign im geltenden deutschen Recht

[Rz 29] Pb^{R}D ist im deutschen Recht kein ausdrücklich normiertes Prinzip. Jedoch sieht das BDSG in § 9 nebst Anlage einen technisch-organisatorischen Datenschutz vor, der dem Prinzip des Pb^{R}D sehr nahe kommt. Der Datenschutz (siehe Abb. 1, Kreis links) schützt die natürlichen Personen – und somit nur die personenbezogenen Daten – vor der Gefahr der Verletzung von Persönlichkeitsrechten. Die Datensicherheit (siehe Abb. 1, Kreis rechts) schützt alle Daten, Hardware und Software vor der Gefahr durch Verlust, Zerstörung und Missbrauch durch Unbefugte.

Abbildung 1: Vorgaben des Datenschutzes

[Rz 30] Gemäß § 9 BDSG sind alle Stellen, welche personenbezogene Daten erheben, verarbeiten oder nutzen, verpflichtet, technisch-organisatorische Maßnahmen (kurz: TOMs) zu treffen um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind. Die Spezifizierung dieser Anforderung ergibt sich aus der Anlage zu § 9 BDSG. Das Recht fordert also die Technik.

[Rz 31] Die Zielrichtung von Pb^{R}D geht in die entgegengesetzte Richtung. Durch proaktives Design kann dem Datenschutz dahingehend geholfen werden, dass die Gefahr der Verletzung von Rechten der Betroffenen minimiert oder gänzlich verhindert wird. Die Technik unterstützt und verhilft dem Recht zur Geltung.

Abbildung 2: Unterstützung durch Pb^{R}D

[24] Vgl. Art. 23 der Grundverordnung sowie Art. 19 der Richtlinie.

[Rz 32] In der Anlage zu § 9 BDSG werden die sog. «acht Gebote» des technisch-organisatorischen Datenschutzes für Fälle automatisierter Erhebung, Verarbeitung oder Nutzung personenbezogener Daten dargestellt. Zu treffen sind insbesondere folgende Maßnahmen: Zutrittskontrolle, Zugangskontrolle (z.B. Benutzerkennung mit Passwort, biometrische Benutzeridentifikation), Zugriffskontrolle (z.B. zertifikatsbasierte Zugriffsberechtigung, Berechtigungskonzept), Weitergabekontrolle (z.B. Verschlüsselung), Eingabekontrolle (z.B. Protokollierung, Benutzeridentifikation), Auftragskontrolle, Verfügbarkeitskontrolle, Gebot der Datentrennung.

3.4 Herausforderungen

- *Einwilligung des Anwenders*: Eine elektronische Einwilligung ist rechtlich möglich, müsste technisch aber ebenso einige Herausforderungen meistern. Zum einen ist die Schaltfläche, mit der eingewilligt wird, deutlich darzustellen, damit die Einwilligung wissentlich und willentlich erteilt wird. Der Anwender muss «informiert» einwilligen, bedeutet für das Design die Integration von einigem Aufklärungstext an geeigneter, gut erkennbarer Stelle. Diese Aufklärung des Anwenders ist bisher selten ausreichend einsehbar, gar versteckt oder wird anderen Nutzungsbedingungen «untergemischt», was wegen der mangelnden «Informiertheit» des Anwenders dann gegen § 4 Abs. 1 S. 4 BDSG verstoßen kann. Es muss der Hinweis des Anbieters auf Art, Umfang und Zweck des Umgangs mit personenbezogenen Daten zu finden sein. Weiterhin muss es dem Anwender möglich sein, andere vergleichbare Dienste des Anbieters zu nutzen, selbst wenn er bei einem Dienst dieses Anbieters nicht einwilligt. Zuletzt muss das «Einwilligungsverhalten» des Anwenders durchgehend protokolliert werden, jederzeit abrufbar und widerrufbar sein. Will, so Kremer, «der Anbieter der App auf das für ihn riskante Spiel mit der Einwilligung verzichten, ist er gezwungen, für jeden einzelnen Schritt bei Erhebung und Verwendung der personenbezogenen Daten durch seine App eine gesetzliche Grundlage zu finden [...]»[25]. Es wäre allenfalls möglich, so Kremer weiter, «die Einwilligung des Anwenders nicht mehr im Ganzen einzuholen, sondern nach und nach für

[25] *Kremer*, S. 446.

einzelne Funktionalitäten einer App Teil-Einwilligungen einzuholen [...]»[26].

- *Anonymität und Pseudonymität*: Dem Anwender sollte die anonyme oder pseudonyme Nutzung seiner Telemediendienste ermöglicht werden. Hier besteht möglicherweise das politische Problem, dass noch immer davon ausgegangen wird, dass anonymisierte Teilnahme an solchen Diensten die Gefahr von Rechtsverletzungen zu Lasten Dritter erhöht. Zudem zeigte das Beispiel Google+, dass eine Anonymisierung oder Pseudonymisierung bei umfangreicheren, bekannteren Diensten oft leerläuft. Anwender von Google+, die dort Spitznamen verwenden, werden von den übrigen Google Diensten dennoch erkannt und weiterhin öffentlich mit dem richtigen Namen geführt.
- *Mehrere Nutzer*: Das Risiko der Nutzung von Smart Devices durch mehrere Anwender könnte reduziert werden, wenn der App-Anbieter den Anwender durch entsprechende Nutzungsbedingungen wirksam dazu verpflichtet, sein Smart Device vor der Nutzung durch andere Anwender zu sichern, beispielsweise ihm einen kostenfreien Zusatzservice zur Installation anbietet, der Zugangssperren einrichtet, oder aber die Nutzung der App selbst erst nach erfolgreicher Bewältigung einer App-bezogenen Zugangssperre ermöglicht.
- *Verantwortliche Stelle*: Grundsätzlich gibt es nach der Systematik des BDSG nur eine «verantwortliche Stelle» (§ 3 Abs. 7 BDSG) bei Apps, nämlich den Anbieter, der umfassende Einwirkungsmöglichkeiten auf die Programmierung der Software hat oder zugleich selber der Entwickler der Software ist. Pb^{R}D würde dazu führen, dass Hersteller und Entwickler von Soft- und Hardware verpflichtend Gestaltungen implementieren müssen und ggfs. sanktioniert werden können, falls sie dies nicht tun. Sie wären dann allerdings quasi «verantwortliche Stelle neben der verantwortlichen Stelle». Es bleibt abzuwarten, ob diese Verschiebung / Verdopplung der Verantwortlichkeit nicht mit Art. 12 und 14 GG[27] kollidiert und wo der deutsche Gesetzgeber dies thematisch verorten will.
- *Datenschutz ex ante*: Grundsätzlich gilt die datenschutzrechtliche Verantwortlichkeit erst dann, wenn mit den personenbezogenen Daten umgegangen wird. Allenfalls § 3a BDSG, das Prinzip der Datenvermeidung und Datensparsamkeit «strahlt bereits de lege lata in das Vorfeld dieses Anwendungsbereiches aus»[28]. Pb^{R}D wäre dann zu beachten, bevor auch nur ein personenbezogenes Datum erhoben wurde. Ob eine App-Funktion Gefahren für die informationelle Selbstbestimmung des Betroffenen birgt, wird im Zweifel erst über eine im Vorfeld durchzuführende «Technikfolgenabschätzung» bestimmbar sein; grundsätzlich kann eine solche Abschätzung funktionieren, wie das Beispiel der RFID-Anwendungen zeigte.[29] Die Kehrseite: Eine Dämonisierung noch nicht näher bestimmter, unmöglich genau abzuschätzender Gefahren durch technische Entwicklung für den betroffenen Anwender.
- *Wirtschaftlichkeit*: Belastbare Vorhersagen hinsichtlich der Wirtschaftlichkeit einer App, die verpflichtend Prinzipien des Pb^{R}D in sich trägt, sind oft nur schwer und unter zusätzlichen Kosten machbar. U.a. ist weder vorhersehbar, wie sich der Markt für Apps entwickeln wird, die mehr oder weniger auf Datenschutz Rücksicht nehmen, noch ist abzuschätzen, wie die

---

26 *Kremer*, S. 446.

27 Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch das Gesetz vom 21. Juli 2010 (BGBl. I S. 944).

28 *Schulz*, S. 207.

29 Im April 2011 wurde ein Rahmenwerk zur Datenschutzfolgenabschätzung für RFID-Anwendungen verabschiedet, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile.

Aufsichtsbehörden auf technische Neuerungen in Apps reagieren.

- *Bedienbarkeit*: Wird eine App mit ausschließlich vordefinierten und als unbedenklich eingestuften Funktionalitäten betrieben und dabei der Umgang mit personenbezogenen Daten minimiert, so leidet darunter sicherlich die Bedienbarkeit. Vielmehr sollte die App flexibel gestaltet werden, Upgrades und Updates zur Verfügung gestellt werden und dem Anwender selbst die Möglichkeit gegeben werden, in bestimmtem Umfang seine Privacy-Einstellungen nicht nur zu aktualisieren, sondern selber manuell anzupassen.

4 Ausblick

[Rz 33] Die Chancen von PbD und Pb^{R}D sind groß, die Fronten in Teilfragen allerdings noch verhärtet:

- *Pro Spielraum für die Anbieter*: «Wenn selbst die Herstellung und das Inverkehrbringen von Kriegswaffen nach behördlicher Genehmigung zulässig ist, können an Softwareentwickler gerichtete Totalverbote nicht der Weisheit letzter Schluss sein»[30].
- *Contra Spielraum für die Anbieter*: Die oberste Staatsanwältin des US-Staates Kalifornien, Kamala Harris, fordert von einer Vielzahl an Betreibern von App-Stores und App-Entwicklern ein Bußgeld von 2.500 Dollar pro Download einer App ein, die gegen die scharfen kalifornischen Datenschutzgesetze verstößt. Diese[31] besagen u.a., dass jede App an einer prominenten Stelle den Nutzer informieren muss, welche persönlichen Daten sie speichert und was mit diesen Daten passiert.

[Rz 34] Was bleibt? Die künftige Lösung liegt wohl in der salomonischen Mitte. Bis dahin kann nach Meinung des Autors auf die Empfehlungen der GSM Association zurückgegriffen werden, die im Februar 2012 hervorragende «Privacy Design Guidelines for Mobile Application Development'[32] veröffentlicht hat und eine Liste technisch-organisatorischer Maßnahmen – in thematische Bereiche unterteilt – vorschlägt.

5 Literatur

Hoeren, Thomas, Google Analytics – datenschutzrechtlich unbedenklich? Verwendbarkeit von Webtracking-Tools nach BDSG und TMG, In: Zeitschrift für Datenschutz (ZD), Heft 1, Seite 3-6 (2011)

Jandt, Silke/Roßnagel, Alexander, Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?, Multimedia und Recht (MMR), Heft 10, Seite 637-642 (2011)

Kremer, Sascha, Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, Computer und Recht (CR), Heft 7, Seite 438-446 (2012)

Schulz, Sebastian, Privacy by Design, Computer und Recht (CR), Heft 3, Seite 204-208 (2012)

Stadler, Thomas, Verstoßen Facebook und Google Plus gegen deutsches Recht? – Ausschluss von

30 *Schulz*, S. 207.

31 California Online Privacy Protection Act (COPPA).

32 http://www.gsma.com/publicpolicy/mobile-and-privacy/design-guidelines.

Pseudonymen auf Social-Media-Plattformen, Zeitschrift für Datenschutz (ZD), Heft 2, Seite 57-59 (2011)

Wintermeier, *Martin*, Inanspruchnahme sozialer Netzwerke durch Minderjährige – Datenschutz aus dem Blickwinkel des Vertragsrechts, Zeitschrift für Datenschutz (ZD), Heft 5, Seite 210-215 (2012)

Philipp E. Fischer, LL.M. (Intellectual Property Law, London / Dresden), Datenschutzbeauftragter & -auditor (TÜV), ITIL® Expert, Geschäftsführer, SuiGeneris Consulting.