
Mobile & Recht

Nina Diercks

Zusammenfassung

Gleich ob „New Business“, „Old Economy“ oder eben „Mobile“, jedes Geschäftsfeld hat (s)einen **rechtlichen** Rahmen. Unbenommen bleibt es den Verantwortlichen betriebswirtschaftliche und rechtliche Risiken einzugehen. Um solche unternehmerischen Entscheidungen verantwortlich treffen zu können, müssen die Risiken jedoch überhaupt erst einmal bekannt sein. Dieses Kapitel liefert einen ersten Ein- und Überblick bezüglich der rechtlichen Fallstricke des Mobile Business.

1 Einleitung

Ein Kapitel zum Recht. Das klingt für die meisten Entscheider der Mobile-Branche – gleich ob Gründer, IT- oder Marketing-Verantwortliche – nicht gerade sexy. Schließlich gelten Juristen gemeinhin als die Bremser guter Ideen, die deswegen besser erst gar nicht gefragt werden. Das verwundert vor dem Hintergrund, dass am Anfang eines Projektes doch ganz selbstverständlich der IT-Entwickler um eine Einschätzung gebeten wird, ob das Ganze auch technisch umsetzbar ist. Danach kommen die UX-Designer dran. Und schließlich wird konkret der Businessplan geschrieben, eine Kennziffer für den ROI festgelegt und der Marketingetat budgetiert.

N. Diercks (✉)
Hamburg, Deutschland
e-mail: kontakt@anwaltskanzlei-diercks.de

© Springer Fachmedien Wiesbaden GmbH 2017
H. Scholz (Hrsg.), *Social goes Mobile – Kunden gezielt erreichen*,
https://doi.org/10.1007/978-3-658-16604-5_2

Ein Budget für Rechtsberatung findet sich hingegen selten. Dieser Posten wird gespart und stattdessen lieber für mehrere tausend Euro in eine große Launch-Party investiert (das ist tatsächlich schon passiert). Ja, der große Markteintritt ist natürlich wichtig. Sich jedoch nicht mit dem Rechtsrahmen des eigenen mobilen Geschäftsmodells auseinanderzusetzen kann fatale, sogar letale Folgen haben. Der Grund: Schwerwiegende rechtliche Probleme werden meist zu spät bemerkt. Hierzu einmal ein ganz einfacher Vergleich: Ist die IT das Knochengerüst, ist Programmierung die Nervenbahn und sind das Marketing sowie das Design Haut und Haare eines mobilen Produkts, so sind die dazugehörigen rechtlichen (Compliance-)Prüfungen und Verträge das Herz-Kreislaufsystem. Bricht ein Knochen, zucken die Nerven unkontrolliert oder werden Haut und Haare grau, so ist das für jeden sofort sichtbar. Schnell kann gegengesteuert werden. Ein Herz-Kreislauf-Kollaps kündigt sich jedoch in den seltensten Fällen mit Vorwarnungen an. Dass die Arterie dann schon beinahe lebensbedrohlich verstopft ist, wird erst bemerkt, wenn der Schlaganfall oder der Herzinfarkt einsetzt.

Ganz ähnlich verhält es sich, wenn das Geschäftsmodell nicht auf rechtliche Tragfähigkeit geprüft, Software-Entwicklungsverträge nicht (hinreichend) geschlossen oder die Nutzungsbedingungen und Datenschutzbestimmungen, also die Verträge mit den Endnutzern, bestenfalls von der vermeintlich erfahrenen Konkurrenz abgeschrieben wurden. In dem einen Fall steht die Bundesfinanzaufsicht mit der Fortführungsversagung (also der sofortigen Firmenschließung) oder die Abmahnung des Mitbewerbers wegen eines Verstoßes gegen das Zahlungsdienstaufsichtsgesetz (ZAG) im Haus. In dem nächsten Fall bricht ein zeit- und kostenintensiver Rechtsstreit darüber aus, wer für die schwerwiegenden Verzögerungen zum kritischen App-Launch verantwortlich ist. Im letzten Fall setzt der mächtige Verband der Konkurrenz dem Unternehmen mittels gerichtlich erwirkter Untersagungsverfügungen im einstweiligen Rechtsschutzverfahren zu.

Geschichten aus der Yucca-Palme? Nein. Alles Geschichten, die das Leben schreibt. Nachzulesen zum Beispiel in der Entscheidung des Landgerichts Köln „Lieferheld“¹ oder in den gerichtlichen Entscheidungen gegen den Dienst Uber.² Und wer „lustige“ bzw. im Ergebnis sehr teure Geschichten zum Thema „Wir brauchen keinen Vertrag“ hören möchte, kann sich gerne mit der Verfasserin dieser

¹ OpenJur: LG Köln, Urteil vom 29. Sept.2011, KfH, Az. 81 O 91/11, <https://openjur.de/u/451040.html>. Zugriffen: 23. Febr.2017

² OpenJur: Hamburgisches OVG, Beschluss vom 24. Sept.2014, Az. 3 Bs 175/14. <https://openjur.de/u/736460.html>. Zugriffen: 23. Febr.2017; Telemedicus: LG Frankfurt: Taxi-Dienst Uber verstößt gegen Wettbewerbsrecht, Beschluss vom 25. Aug.2014, 2-03 O 329/14, <http://tlmd.in/u/1510>. Zugriffen: 23. Febr.2017

Zeilen auf eine Tasse Kaffee für die eine oder andere wahre – wenn auch anonymisierte – Begebenheit aus der Praxis treffen.³

Bei dieser relativ allgemeinen Einleitung mit den konkreten Schreckensszenarien geht es übrigens nicht darum, Entscheidern unnötige Angst zu machen. Es soll vielmehr schlicht deutlich werden, dass das Recht im Mobile Business genauso eine Rolle spielt, wie in jedem anderen Geschäftsfeld auch. Und gleich ob „New Business“ oder „Old Economy“: Es ist eine unternehmerische Entscheidung, rechtliche Risiken einzugehen. Um eine solche unternehmerische Entscheidung – so wie etwa Über millionenschwere Rücklagen für Prozesskosten gebildet hat – treffen zu können, müssen die Risiken jedoch überhaupt bekannt sein.

Der nachfolgende Beitrag gewährt einen ersten Ein- und Überblick hinsichtlich der rechtlichen Fallstricke des Mobile Business. Dabei wird es nicht um die Verwendung von Bildern, die Abbildung von Personen oder User Generated Content gehen. Dies nicht, weil das Urheber- oder Persönlichkeitsrecht mobil nicht gälte, sondern weil es hier keine Besonderheiten gegenüber der Verwendung im „normalen“ (Social) Web gibt. Vielmehr werden hier schwerpunktmäßig die rechtlichen Aspekte der Applikationsentwicklung und -vermarktung (Kap. 2) erläutert und es wird sodann auf die Rechtsprobleme des Mobile Tracking und der Werbe-IDs (Kap. 3), des Mobile Advertising und des Mobile-Shopping (Kap. 4) sowie der Beacon-Technologie (Kap. 5) eingegangen.

2 Rechtliche Aspekte der App-Entwicklung

Applikationen (Apps) sind wesentlich für das Mobile Business. Doch noch immer setzen sich nur wenige App-Betreiber und App-Entwickler mit den zentralen rechtlichen Problemstellungen der Entwicklung und Vermarktung auseinander.

Die zu berücksichtigenden Rechtsfragen ergeben sich aus den an einer App „Beteiligten“, namentlich

- dem App-Betreiber,
- dem App-Entwickler,
- den App-Vermarktern und schlussendlich
- den Nutzern.

³ Oder zum Beispiel diesen Blogbeitrag lesen: Die Flatrate im Agenturvertrag – klingt toll, kann teuer ausgehen, Artikel vom 03. Mai 2015, <http://www.socialmediarecht.de/2015/05/03/die-flatrate-im-agenturvertrag-klingt-toll-kann-teuer-ausgehen-ig-koeln-v-20-02-2015-az-12-o-18613-zur-unterscheidung-von-dienstvertrag-und-werkvertrag/>

Außerdem beteiligt sind die damit verbundenen Rechtsgebiete:

- Namens- und Markenrecht,
- IT-/Softwareentwicklungs-Vertragsrecht,
- Datenschutzrecht,
- Nutzungsbedingungen der App – Vertrag zwischen Betreiber und Nutzer (AGB-Recht),
- Nutzungsbedingungen der App-Vermarkter – Vertrag zwischen App-Betreiber und App-Vermarktern (Stores).

Schon die vorgenannte Aufzählung lässt vermuten, dass die rechtlichen Stolpersteine mannigfaltig am Wegesrand verstreut liegen. Im Folgenden nun zu einigen davon.

2.1 Markenrecht – Jede App braucht einen Namen

Die wenigsten App-Betreiber denken über das Markenrecht bei der Konzeption einer App nach. Aber auch eine App braucht einen Namen, bestenfalls einen, der in einigen Jahren eine ebenso überragende Bekanntheit wie Tesa, Tempo oder Facebook erlangt. Natürlich kann das Thema „Marke“ auch später angegangen werden. Es ist allerdings äußerst misslich, eine Applikation unter einem bestimmten Namen auf den Markt zu bringen und erst hinterher mittels der Abmahnung eines Dritten wegen der Verletzung einer Marke, eines Unternehmenskennzeichens oder eines Werktitels⁴ darauf hingewiesen zu werden, dass dieser Name nicht verwendet werden darf.

In diesem Fall hat der App-Betreiber zum einen mit den Kosten der Abmahnung selbst zu kämpfen. Diese belaufen sich im *außergerichtlichen* Verfahren bei dem in markenrechtlichen Angelegenheiten regelmäßig angenommenen Streitwert von 50.000 Euro auf ca. 4000 Euro für den eigenen und den gegnerischen Anwalt. Zum anderen – und das ist de facto noch wesentlicher – muss der App-Betreiber wegen des mit der Abmahnung durchgesetzten Unterlassungsanspruches vor allem auch einen neuen Namen finden, ein neues Branding im Markt einführen und eine entsprechende weitere Marketingkampagne finanzieren. Und dass diese Kosten im

⁴ LG Hamburg, Beschluss v. 8. Okt.2013, Az. 327 O 104/13; bejahend zur Frage, ob eine App ein titelstutzfähiges Werk im Sinne von § 5 Abs. 3 MarkenG sein kann; K&R, 2014, 131-133.

Zweifel weit über denjenigen für eine markenrechtliche Abmahnung liegen, dürfte offensichtlich sein.

Infolgedessen lautet der Rat, das Thema „Marke“ nicht auf später zu verschieben, sondern sich noch vor dem Launch und Markteintritt eben damit zu befassen.⁵

2.2 IT-rechtliche Fragestellungen – der Vertrag zwischen App-Betreiber und Entwickler

In der Regel handelt es sich beim App-Betreiber und beim App-Entwickler um zwei verschiedene Parteien. Nun können Absprachen per Handschlag natürlich gut gehen. Sie können aber genauso gut extrem schief gehen. Da die App-Entwicklung letztlich ein bzw. das Kernstück des App-Business darstellt, sollte mit den vertraglichen Fragen der App-Entwicklung nicht zu nachlässig umgegangen werden.⁶

2.2.1 Vertragsarten, „Probleme“ agiler Projektstrukturen, Mitwirkungspflichten

Bei einem Software-Entwicklungsvertrag handelt es sich in der Regel um einen Werkvertrag.⁷ Wenn jedoch Aspekte der Software-Pflege oder des Software-as-a-Service (SaaS) hinzukommen, können diese Elemente auch dienst- oder mietvertraglicher Natur sein. Die konkrete Einordnung ist genauso einzelfallabhängig wie wichtig. Denn während zum Beispiel bei einem Werkvertrag ein konkreter Erfolg geschuldet ist (App verfügt über Funktionen A und B und funktioniert), wird bei einer Dienstleistung nur die Erbringung der Leistung an sich und kein konkreter Erfolg geschuldet. Die Einordnung der einzelnen Elemente und damit

⁵ Ausführlich zum Themenkomplex des Markenrechts die Reihe: „Von der Marke, der Markenmeldung und deren Eintragung – ein Überblick“, Artikel vom 29. Juni 2015, Juni und 14. Juli 2015, <http://www.socialmediarecht.de/2015/06/29/von-der-marke-der-markenanmeldung-und-deren-eintragung-ein-ueberblick-part-i/>

⁶ Im Rahmen dieses Kapitels kann nur auf einige vertragliche Aspekte eingegangen werden, einen vollständigen Überblick bietet die Reihe „Von der Idee über die Entwicklung bis zur Vermarktung einer App – Wo liegen die rechtlichen Hürden?“ vom 19. März und 18. Mai 2015, <http://www.socialmediarecht.de/2015/03/19/von-der-idee-ueber-die-entwicklung-bis-zur-vermarktung-einer-app-wo-liegen-die-rechtlichen-huerden-part-1/>.

⁷ OpenJur: BGH, Urteil vom 25. März 2010, Az. VII ZR 224/08; <https://openjur.de/u/70090.html>. Zugriffen: 23. Febr.2017

ob Abnahmen (im Werkvertrag) zu erfolgen haben, hat erhebliche rechtliche Konsequenzen für den Fall, dass das Projekt nicht erfolgreich verläuft.⁸

Daneben ist grundsätzlich zu bedenken, dass die wenigsten IT-Projekte linear verlaufen. Das Buzzword lautet „agil“. Letztendlich meint es nichts anderes, als dass fortlaufend unter dem Projekt Änderungen anstehen können und/oder von verschiedenen Seiten zugearbeitet wird. Dabei sind unterschiedliche Agilitätsstufen zu unterscheiden, von einfachen, aber (hoffentlich!) einkalkulierten Projektänderungen bis hin zur Erstellung einer Software mittels der Scrum-Methode.

Doch gleich wie agil ein Projekt ausgestaltet ist – es ändert nichts daran, dass sich die Vertragsparteien auf eine Rahmenbasis im Vorfeld einigen müssen. Leistung und Gegenleistung der Vertragspartner müssen eine Definition erfahren. Ob das jetzt Projektbeschreibung, Lasten- und Pflichtenheft oder Projektziel und Sprint-Plan genannt wird, ist völlig gleichgültig. Ein guter Entwicklungsvertrag bildet schlicht das zwischen den Parteien Vereinbarte ab und nimmt eine – wie auch immer geartete – agile Projektstruktur bzw. Entwicklungsmethode in sich auf bzw. schafft eben dafür den klaren Rahmen. Das heißt, es gibt für „Leistungsänderungen“ einen vorgeschriebenen Workflow, der verbindlich ist.

Die vertraglichen Abbildungen von agilen Projektstrukturen können relativ komplex sein.⁹ Doch wer schon einmal erlebt hat, wie ein IT-Projekt hinsichtlich Budgets und Timelines aus dem Ruder läuft, weiß, wie wichtig die verbindliche, vertragliche Klärung von Verantwortlichkeiten und Zuständigkeiten sein kann.

In Bezug auf Timelines und damit die Umsetzung an sich sollte weiter bedacht werden, dass die Mitwirkungspflichten der Parteien und die Konsequenzen, wenn eine Partei eben diesen nicht nachkommt, vertraglich geregelt werden müssen. Denn was nützt das Datieren eines Milestones und einer Abnahme, wenn der Entwickler letztlich aufgrund mangelnder Mitwirkung des Auftraggebers diesen Milestone überhaupt nicht erreichen konnte? Wenn nun der Auftraggeber dennoch auf die Einhaltung dringt, ist der Ärger mehr als vorprogrammiert. Es wird darüber

⁸ Welche Auswirkung das haben kann, zeigt sich anhand des Urteils des LG Köln vom 20. Febr. 2015, Az. 12 O 18613, dazu: „Die Flatrate im Agenturvertrag – klingt toll, kann teuer ausgehen“, Artikel vom 03. Mai 2015, <http://www.socialmediarecht.de/2015/05/03/die-flatrate-im-agenturvertrag-klingt-toll-kann-teuer-ausgehen-lg-koeln-v-20-02-2015-az-12-o-18613-zur-unterscheidung-von-dienstvertrag-und-werkvertrag/>.

⁹ Erster Überblick zu Vertragsinhalten eines (teils) agilen Projekts: „Von Lastenheften, Pflichtenheften und was das gerade bei agilen Projekten mit Verträgen zu tun hat“, Artikel vom 29. Jan. 2014, <http://www.socialmediarecht.de/2014/01/29/von-lastenheften-pflichtenheften-und-was-das-gerade-bei-agilen-projekten-mit-vertraegen-zu-tun-hat/>.

gestritten, wer, was, wann und wie hätte beibringen müssen und wer für die Leistungsverzögerung verantwortlich ist. Dies kann bei klaren vertraglichen Regelungen von vornherein vermieden werden.¹⁰

2.2.2 Rechteübertragungen, Lizenzen

Gerne vergessen, aber doch so wichtig: Die Übertragung der Rechte an der Software. Software erfährt über die §§ 69a ff. UrhG urheberrechtlichen Schutz. Und demnach hat der Programmierer als Urheber alle Rechte an seiner „geistig-schöpferischen“ Leistung.

Wird eine Software in einem regulären Arbeitsverhältnis entwickelt, ist dies relativ problemlos. Denn hier erwirbt gemäß § 69b UrhG der Arbeitgeber alle vermögensrechtlichen Befugnisse, während der „Arbeitnehmerurheber“ von der Verwertung seines Programms in der Regel ausgeschlossen wird.

Ist der Entwickler aber kein Arbeitnehmer, muss die Rechteübertragung ebenso wie eine potenzielle Herausgabe der Programmierungsgrundlagen (Dokumentation, Quellcode bzw. Hinterlegungsvereinbarungen, wie steht es um Bibliotheken?) unbedingt geregelt werden, damit die Weiterentwicklung der App auch bei einem möglichen Wechsel des Entwicklers bzw. Entwickler-Teams reibungslos stattfinden kann. Die Fragen der Rechteübertragung werden oft unter dem Stichwort „Lizenz“ abgehandelt. Doch gleich, wie dieses Kind genannt wird – der Umfang der Rechteübertragung muss geregelt sein.

2.2.3 Gewährleistung und Haftung

Für den Fall, dass es dennoch einmal dazu kommt, dass die App vom Entwickler zu vertretende Fehler aufweist, ist an Haftungs- und Gewährleistungsklauseln im Vertrag zu denken. Aus Sicht der App-Entwickler sind Haftungs- und Gewährleistungsklauseln natürlich soweit zu „drücken“, wie es Recht und Gesetz zulässt. Das Interesse des Auftraggebers ist hier natürlich gegenteilig. Im Zusammenspiel mit klaren Leistungsverpflichtungen des Auftragnehmers sollte der Auftraggeber versuchen, die Haftung des Programmierers so weit als möglich zu definieren. Hinsichtlich welcher Punkte genau, hängt wieder stark vom einzelnen Projekt ab. Aber

¹⁰ Ausführlich zur Vertragsgestaltung in der Medien- und IT-Branche: „Die Verträge (in der Medien- und IT-Branche“, Artikel vom 16. September und 6. Oktober 2016, <http://www.socialmediarecht.de/2016/09/16/die-unterschiedlichen-vertragstypen-in-der-medien-und-it-branche-teil-1/>.

sagen wir es einmal so: Würden Sie als App-Betreiber gerne für nicht autorisierte In-App-Käufe der Nutzer haften wollen und keinen Regress nehmen können, wenn diese In-App-Käufe auf einer Fehlfunktion im Code beruhen?

2.3 Datenschutz, Datenschutzerklärung, rechtskonforme Implementierung

Datenschutz – das Wort, bei dem zahlreiche Entwickler und Marketeers die Augen verdrehen. Aus drei bzw. vier Gesichtspunkten sollte jedoch auch der Punkt Datenschutz nicht stiefmütterlich behandelt werden. Zum einen können datenschutzrechtliche Verstöße nach einem Urteil des OLG Hamburg grundsätzlich von Mitbewerbern und Wettbewerbsverbänden abgemahnt werden.¹¹ Zum anderen können natürlich die Aufsichtsbehörden, also die Datenschutzbehörden, aktiv werden. Der diesen zur Hand stehende Maßnahmenkatalog beginnt bei einem Bußgeld für eine Ordnungswidrigkeit, z. B. wegen einer mangelnden Datenschutzerklärung nach § 16 Abs. 2 Nr. 2 TMG oder wegen unzulässiger Datenerhebung bzw. Datenübermittlung iSv. § 43 Abs. 1 Nr. 4. Die Bußgelder können im Extremfall bis zu 300.000 betragen. Mit Geltung der EU-Datenschutzgrundverordnung (DSGVO) werden sich die angedrohten Bußgeldbeträge ab 2018 drastisch erhöhen. Die Maßnahmen können aber weit darüber hinaus wirken – bis hin zu einer Untersagungsverfügung. Mit einer solchen kann im Ergebnis der Betrieb einer App und damit im Zweifel die gesamte Unternehmenstätigkeit untersagt werden.¹² Daneben fordern inzwischen die Entwickler-Richtlinien von Google und Apple selbst die Programmierung (relativ) datenschutzkonformer Applikationen. Werden diese Richtlinien nicht beachtet, droht das Entfernen der Applikation aus den Stores (Abschn. 3.2.1). Zuletzt ist darauf hinzuweisen, dass Datenschutz auch bei den Verbrauchern zunehmend einen Stellenwert einnimmt und Transparenz sowie eine möglichst

¹¹ OLG Hamburg, Urteil vom 27. Juni 2013, 3 U 26/12, siehe dazu: <http://www.socialmediarecht.de/2013/07/11/olg-hamburg-mangelhafte-datenschutzerklarungen-sind-wettbewerbswidrig-und-mit-abmahnungen-angreifbar/>.

¹² Ausführlich zu den tatsächlichen Risiken von datenschutzrechtlichen Verstößen, insb. zur Höhe von verhängten Bußgeldern: „Von der Idee über die Entwicklung bis zur Vermarktung einer App – Wo liegen die rechtlichen Hürden?“ vom 19. März und 18. Mai 2015, <http://www.socialmediarecht.de/2015/03/19/von-der-idee-ueber-die-entwicklung-bis-zur-vermarktung-einer-app-wo-liegen-die-rechtlichen-huerden-part-1/>; daneben können Datenschutzverstöße im Übrigen auch Straftatbestände darstellen, vgl. § 44 BDSG.

hohe Datenkontrolle des einzelnen Nutzers vertrauensbildend sein und damit auch einen Wettbewerbsvorteil darstellen können.

Doch nicht nur der Nutzerwunsch nach Transparenz oder die Entwickler-Richtlinien führen zu einer Datenschutzerklärung. Vielmehr verpflichtet § 13 TMG jeden App-Betreiber als sogenannten Diensteanbieter ganz klar, „den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten [...] in allgemein verständlicher Form zu unterrichten.“

Hierbei ist zu beachten, dass nicht nur über die Verwendung von Daten aufgeklärt werden muss, die über die App während/durch die Nutzung selbst erhoben, gespeichert und genutzt werden. Vielmehr muss auch über die Daten, die bei der Installation der App vom Telefon „abgegriffen“ und anschließend verwendet werden, aufgeklärt werden. Dazu zählen z. B. die Geräte-ID, die Werbe-ID (Kap. 3) oder der Zugriff und die Verwendung auf Fotodateien etc. Hierüber wird jedoch nur sehr selten aufgeklärt: Scheinbar führt ein solcher Verstoß, anders als ein Verstoß gegen den Umgang mit Werbe-IDs, nicht zur Zurückweisung der Applikation (Abschn. 3.2.1). Der User sieht – wenn überhaupt – nur beim Installieren der App übersichtsartig, worauf Zugriff genommen wird. Teilweise sind die Datenzugriffe natürlich für den Betrieb der App zwingend und damit zur Vertragserfüllung notwendig. Das wiederum bedeutet, dass ein gesetzlicher Erlaubnistatbestand zur Erhebung dieser Daten vorliegt. Sehr oft benötigt die App für den Betrieb jedoch nur einen Bruchteil der Daten. Für alle anderen – für den App-Betreiber offensichtlich wirtschaftlich attraktiven – Daten, bräuchte es dann gemäß § 12 TMG einer ausdrücklichen Einwilligung des Nutzers. Denn die Erhebung von personenbezogenen Daten ist nur dann rechtmäßig, wenn eine gesetzliche Vorschrift dies erlaubt oder der Nutzer selbst in die Datenerhebung eingewilligt hat. Daran wird sich auch mit der Geltung der DSGVO ab 2018 nichts ändern. Ausdrückliche Einwilligung bedeutet, dass der Nutzer im Double-Opt-In-Verfahren¹³ der Datenerhebung zustimmen muss. Doch eine solche lässt sich zumeist nicht finden. Ganz grundsätzlich muss die Datenschutzerklärung leicht in der App aufzufinden sein, so dass der User jederzeit darauf Zugriff nehmen kann. Da der Nutzer vor Beginn des Nutzungsvorgangs über die Datenverwendungen aufgeklärt werden muss, genügt jedoch das Vorhalten in der App dann nicht, wenn die App schon bei der Installation auf Daten zugreift.

¹³ Ausführlich zum rechtskonformen Double-Opt-In Verfahren: Diercks, Nina - E-Mail-Marketing – Den Klassiker des digitalen Marketings rechtskonform umsetzen, Artikel vom 05. Febr.2015. <https://www.munich-digital.com/fachartikel/recht-datenschutz/e-mail-marketing-rechtskonform-umsetzen.pdf>.

Die Datenschutzerklärung muss in diesem Fall (und sollte sonst auch) vielmehr im App Store selbst schon über einen Link abrufbar sein, so dass sich der Nutzer eben vor Beginn des Nutzungsvorgangs informieren kann. Und wenn für die Datenverwendungen Einwilligungen notwendig sind, dann muss diese Einwilligung auch vor Beginn des Nutzungsvorgangs erfolgen. Ist dies nicht möglich, weil z. B. der Store diese Möglichkeit nicht bietet, dann ist diese Einwilligung umgehend nach der Installation der App einzuholen.

Die soeben aufgeführten und speziell für Diensteanbieter formulierten Vorgaben des TMG werden mit Geltung der EU-Datenschutzgrundverordnung (DSGVO) ab 2018¹⁴ durch abstraktere und nicht speziell auf Internetanbieter abgestimmte Vorschriften ersetzt. Ob die Bestimmungen des TMG neben denen der DSGVO bestehen bleiben, steht derzeit noch in den Sternen. So oder so ändert sich an den Informationspflichten, dem Einwilligungserfordernis oder der Notwendigkeit von Datenschutzerklärungen jedoch nichts, da auch die DSGVO derartige Vorgaben enthält.

Abschließend ist zu sagen, dass bislang (!) das Risiko, aufgrund von Datenschutzverstößen seitens der Behörde Bußgeldbescheide oder seitens Mitbewerbern, bzw. Wettbewerbszentralen, Abmahnungen zu erhalten, tatsächlich relativ gering war. Allerdings sollte sich hierauf besser kein App-Betreiber verlassen. Denn zum einen zeigen Unternehmen zunehmend nicht datenschutzkonform handelnde Mitbewerber auch bei den Behörden an – anstelle zum Mittel der wettbewerbsrechtlichen Abmahnung zu greifen. Und zum anderen hat der Gesetzgeber mit einer Änderung des Unterlassungsklagegesetzes (UKlaG) den Verbraucherschutzverbänden ausdrücklich die Möglichkeit eingeräumt, nun auch Datenschutzverstöße abzumahnern.¹⁵ Ferner sollte im Hinterkopf behalten werden, dass die Aufsichtsbehörden zu drastischen Mitteln wie der Untersagungsverfügung greifen können.

Ab Mai 2018, wenn die DSGVO Wirkung entfaltet, kommt noch ein weiterer wichtiger Punkt hinzu: Wenn die Aufsichtsbehörden Bußgelder nach dem BDSG verhängen, dann bewegen diese sich regelmäßig im unteren vierstelligen bis unteren fünfstelligen Bereich. Je nach Häufigkeit und Intensität des Verstoßes oder der Verstöße. Nur sehr selten wurden Bußgelder im sechsstelligen Bereich

¹⁴ Im Social Media Recht Blog findet sich eine umfangreiche Serie zur EU-Datenschutzgrundverordnung und den künftigen datenschutzrechtlichen Anforderungen, denen Unternehmen ab 2018 begegnen müssen: <http://www.socialmediarecht.de/?s=dsgvo>.

¹⁵ Piltz, Carlo: Verbandsklagerecht bei Datenschutzverstößen: Geplante Änderungen und offene Fragen, 05.02.2015. <http://www.delegedata.de/2015/02/verbandsklagerecht-bei-datenschutzverstoessen-geplante-aenderungen-und-offene-fragen/>, letzter Zugriff: 23.02.2017

verhängt. Maximal sieht das BDSG eine Summe von 300.000 Euro vor. Dies ändert sich jedoch massiv mit der DSGVO. Je nach Verstoß droht dann eine Zahlung von bis zu 10 Millionen Euro bzw. bis zu 2 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres oder bis zu 20 Millionen Euro bzw. bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres. Dies sind Summen für die kaum eine Firma eine „Rücklage“ einrichten kann. Infolgedessen gilt es für Unternehmen, die Anforderungen, die das Datenschutzrecht mit sich bringt, künftig weit ernster zu nehmen als dies bisher der Fall war – und zwar nicht nur im Bereich der App-Entwicklung.¹⁶

2.4 Nutzungsbedingungen, Vertragsbeziehungen mit dem Nutzer

Neben all dem ist auch noch an die Vertragsbeziehungen zwischen dem App-Betreiber und dem Nutzer zu denken. Das gilt insbesondere dann, wenn über die App etwa urheberrechtlich geschützte Inhalte hochgeladen werden oder Nutzer untereinander kommunizieren sollen. Hier müssen Nutzungsrechte an den Inhalten eingeräumt, Regeln für die sonstige Nutzung erstellt und vor allem klar gemacht werden, was passiert, wenn ein Nutzer gegen diese Regelungen verstößt (Regress- und Freistellungsansprüche).

Noch komplexer wird es, wenn die App oder eine Upgrade-Version mit bestimmten Funktionen kostenpflichtig ist. Grundlegend müssen Leistung – wie die Funktionen der App – und Gegenleistung definiert werden, im Falle von Abonnements sind auch Laufzeiten und Kündigungsmöglichkeiten zu definieren. Was alles genau qua Nutzungsbedingungen vereinbart werden muss, hängt – wieder einmal – vom Einzelfall und den Funktionen der App ab.

Dazu ist beim Verkauf der Apps an das Widerrufsrecht bei Softwaredownloads und dessen regelrechte, leider nicht ganz unkomplizierte, Umsetzung, zu denken.¹⁷

Eine der „Königsdisziplinen“ der Nutzungsbedingungen von Apps sind diejenigen für In-App-Käufe. Hier muss besonders auf ein wirksames Zustandekommen

¹⁶ Im Social Media Recht Blog findet sich eine umfangreiche Serie zur EU-Datenschutzgrundverordnung und den künftigen datenschutzrechtlichen Anforderungen, denen Unternehmen ab 2018 begegnen müssen: <http://www.socialmediarecht.de/?s=dsgvo>.

¹⁷ „Das neue Widerrufsrecht beim Verkauf von Software-Downloads“, Artikel vom 16. Mai 2014. <http://www.socialmediarecht.de/2014/05/16/die-verbraucherrechtsnovelle-das-neue-widerrufsrecht-beim-verkauf-von-software-downloads/>.

des Vertrages zwischen Nutzer und App-Betreiber gedungen werden. Auch sollte nicht vergessen werden, dass sich In-App-Käufe häufig in Spielen finden und diese häufig von Kindern genutzt werden (könnten). Bei der Verarbeitung personenbezogener Daten von Kindern ist weiter zu berücksichtigen, dass ab 2018 für die Einwilligung durch Minderjährige die speziellen und erhöhten Anforderungen der DSGVO gelten. Die Regelung des Art. 8 DSGVO sieht vor, dass Eltern für das Kind die Einwilligung erteilen müssen, bis dieses das 16. Lebensjahr vollendet hat. Dem deutschen Gesetzgeber steht es frei, von dieser Altersgrenze abzuweichen. Diese darf jedoch nicht unter das vollendete dreizehnte Lebensjahr fallen. Auch derartige Überlegungen müssen sowohl in der Konzeption der App als auch in der Vertragsgestaltung berücksichtigt werden.

2.5 Vertragsbeziehungen zwischen App-Betreibern und App-Vermarktern

Wer eine App auf bzw. in den Markt bringen will, der kommt an den App-Stores von – maßgeblich – Apple und Google kaum vorbei. Das heißt, dass die eingestellten Apps den Anforderungen der Stores gerecht werden müssen. Es würde den Umfang des Kapitels bei weitem sprengen, die mannigfaltigen Voraussetzungen, die in den Entwickler-Richtlinien¹⁸ der Stores festgehalten sind, hier aufzuführen (auf einige datenschutzrechtliche bzw. technische Voraussetzungen wird in Kap. 3 eingegangen). Fakt ist aber, dass die Apps vor Veröffentlichung durch die Stores geprüft werden. Und erfüllt die App nicht die von den Stores vorgegebenen Voraussetzungen, wird die App nicht zum Vertrieb über den Store zugelassen.

2.6 Fazit zu rechtlichen Aspekten der App-Entwicklung

So sehr der einzuhaltende rechtliche Rahmen bei der Entwicklung einer App für einen kreativen Kopf eines Unternehmens auch hinderlich zu sein scheint, so sehr lohnt es sich doch, diesem Thema genügend Beachtung zu schenken – und zwar von Beginn an. Denn kaum ein Unternehmen möchte im Zweifel viel Geld für die technische Entwicklung einer App ausgegeben haben, um dann wahlweise

¹⁸ Google Play-Programmrichtlinien für Entwickler, <https://play.google.com/about/developer-content-policy.html>; die Apple App Store Review Guidelines, <https://developer.apple.com/app-store/review/guidelines/#privacy> mit Verweis auf zum Program License Agreement (nicht öffentlich einsehbar).

- festzustellen, dass das grundlegende Geschäftsmodell der App rechtswidrig ist,
- nach der Markteinführung zu merken, dass diese Bezeichnung niemals hätte verwendet werden dürfen,
- mit den Entwicklern über Kreuz zu liegen, eine unfertige App, aber dafür einen Rechtsstreit am Laufen zu haben,
- eine Abmahnung der Konkurrenz oder ein entsprechendes Schreiben der Datenschutzbehörden mit anschließendem Bußgeldbescheid (ab 2018 in kaum absehbaren Höhen) wegen Datenschutzverstößen im Briefkasten zu haben und/oder
- verärgerten Endkunden gegenüberzustehen, weil es die Verträge mit eben diesen für Selbstgänger gehalten hat.

3 Mobile Tracking, Werbe-IDs & Datenschutzrecht

Ein besonderes datenschutzrechtliches Feld ist das mobile Tracking. Natürlich möchten Werbetreibende auch das mobile Verhalten der Nutzer analysieren können. Nachdem hierfür anfangs die Geräte-IDs (Unique Device Identifiers, UDID) verwendet wurden, sind Apple und Google längst auf geräteunabhängige IDs umgeschwenkt. Maßgeblich waren zwei Gründe. Zum einen liefen die Datenschutzbeauftragten Sturm gegen die (fast) unauslöschlichen Geräte-IDs, über die sich ein Personenbezug relativ leicht herstellen ließ. Zum anderen war die Verwendung der Geräte-ID auch für die werbende Industrie suboptimal, da die Geräte-ID einem Gerät und nicht einem Nutzer zugeordnet ist. Das hat zur Folge, dass ein damit generiertes „Nutzerprofil“ in dem Moment, in dem ein Gerät seinen Besitzer wechselt, wertlos wird.

Die von Google und Apple verwendeten/vergebenen IDs sind nun systemabhängig. Dies bedeutet, dass jedem Nutzer eines Apple-Accounts oder Google-Kontos mit der Anmeldung eine ID zugeordnet wird. Zur Freude der Vermarkter kann diesem Nutzer somit über beliebige Devices, Apps und mobile Browser hinweg gefolgt werden (im Folgenden: „Werbe-ID“).

3.1 Der Personenbezug von Werbe-IDs

Was für die Werbetreibenden noch besser klingt, lässt die Datenschützer nach wie vor erschauern. Problematisch ist der Personenbezug der Werbe-ID. Dieser ist unweigerlich vorhanden, sobald eine App mit dem Google-Konto oder Apple-Account verbunden wird. Doch selbst wenn eine Applikation eine solche Verbindung nicht herstellt: Nach Auffassung der meisten Datenschutzbeauftragten der Länder

genügt die Personenbeziehbarkeit eines Datums, also die reine Möglichkeit der Verknüpfung zwischen Information und Mensch, für die Anwendung des Datenschutzrechts nach dem BDSG.¹⁹ Und diese Möglichkeit liegt bei den System-IDs stets vor. Dabei ist es nicht notwendig, dass der App-Betreiber die Verknüpfung selbst durchführen kann. Es reicht aus, dass die theoretische Möglichkeit besteht, dass durch die Abfrage eines Dritten die hinter der ID stehende Person ermittelt werden kann – also eine sogenannte „Personenbeziehbarkeit“ besteht. Dieses Verständnis setzt sich auch auf europäischer Ebene fort. Nachdem bereits der Europäische Gerichtshof (EuGH)²⁰ einen Personenbezug von dynamischen IP-Adressen angenommen hat, schlägt sich der Gedanke einer nur möglichen Identifizierung von Personen durch die Verknüpfung mit (Online-)Kennungen wie z. B. Cookies oder IP-Adressen nun auch (wörtlich!) in der DSGVO nieder. Dies bedeutet, dass spätestens ab 2018 Werbe-IDs unstrittig immer dann einen Personenbezug aufweisen, wenn das Apple- oder Google-Konto eine Verknüpfung mit der Werbe-ID erfahren hat und/oder wenn eine Verbindung mit der Geräte-ID hergestellt wird und der App-Anbieter auf diese Daten zugreifen könnte (nicht: kann).

Das wird faktisch nahezu immer der Fall sein. Denn theoretisch existiert zwar die Möglichkeit, die Werbe-IDs auf den Smartphones zurückzusetzen, praktisch macht das jedoch kaum ein Nutzer.

3.2 Die rechtlichen Konsequenzen

Bevor mit dem Tracking über eine ID begonnen wird, muss daher die Einwilligung des Nutzers vorliegen. Eine solche wird aber in der Regel nicht eingeholt. Nun ist das Risiko, von Seiten der Behörde oder dem Mitbewerber angegriffen zu werden, derzeit faktisch nicht sehr hoch. Wie gezeigt, sollten Unternehmen sich darauf jedoch nicht verlassen, da zu erwarten ist, dass sich dies spätestens mit Geltung der DSGVO ab 2018 ernsthaft ändern wird. Darüber hinaus gibt es noch einen

¹⁹ So hinsichtlich von IP-Adressen: Beschluss des Düsseldorfer Kreises vom 26./27. Sept. 2009. „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“, <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entscheidungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf> oder „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“ des Düsseldorfer Kreises vom 16. Juni 2014. https://www.lida.bayern.de/media/oh_apps.pdf.

²⁰ EuGH, Urteil vom 19. Okt. 2016 in der Rechtssache C-582/14, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>

weiteren Grund, weshalb an dieser Stelle nicht zu nachlässig gearbeitet werden sollte – wie im Folgenden dargestellt.

3.2.1 Die Entwickler-Richtlinien von Apple und Google

Google und Apple wollen sich selbst datenschutzrechtlich so wenig wie möglich angreifbar machen. Folglich legen Sie in Ihren Entwickler-Richtlinien²¹ fest, wie mit den Werbe-IDs umzugehen ist.

In der Google-Play-Programm-Richtlinie heißt es, dass die systemabhängigen Werbe-IDs nur zu Werbezwecken und zur Nutzeranalyse verwendet werden dürfen, wobei der *„Status der Einstellung zur Deaktivierung interessenbezogener Werbung bei jedem Zugriff auf die ID überprüft werden“* muss. Die *„Verknüpfung der Werbe-ID mit personenbezogenen Daten oder statischen Geräte-IDs wie SSAID, MAC-Adresse oder IMEI darf gar nur mit ausdrücklicher Zustimmung des Nutzers“* erfolgen. Und nach Zurücksetzen der ID darf eine neue Werbe-ID *„nur mit ausdrücklicher Zustimmung des Nutzers mit einer vorherigen Werbe-ID oder daraus stammenden Daten verknüpft werden“*. Darüber hinaus muss *„die Erfassung und Nutzung der Werbe-ID den Nutzern in einer rechtlich angemessenen Benachrichtigung zum Datenschutz mitgeteilt werden“*.²² Ergo: Es bedarf auch nach den Entwickler-Richtlinien einer Datenschutzerklärung.

Apple verbietet zudem ausdrücklich das Nutzen der Werbe-ID, wenn die App selbst keine Ads ausliefert. In dem Program Licence Agreement (das nicht öffentlich einsehbar ist), heißt es in Ziffer 3.3.12 wörtlich: *„You and Your Applications (and any third party with whom you have contracted to serve advertising) may use the Advertising Identifier, and any information obtained through the use of the Advertising Identifier, only for the purpose of serving advertising.“*

²¹ Google Play-Programmrichtlinien für Entwickler, <https://play.google.com/about/developer-content-policy.html>; die Apple App Store Review Guidelines, <https://developer.apple.com/app-store/review/guidelines/#privacy> mit Verweis auf zum Program License Agreement (nicht öffentlich einsehbar), aber sinngemäß mehr oder weniger die gleichen Regelungen wie die Google-Programmrichtlinien; einen übersichtsartigen Artikel zu den Regelungen zur Apple-ID bietet Techcrunch: Perez, Sarah - „Apple’s Latest Crackdown: Apps Pulling The Advertising Identifier, But Not Showing Ads, Are Being Rejected From App Store“, 03.02.2014. <http://techcrunch.com/2014/02/03/apples-latest-crackdown-apps-pulling-the-advertising-identifier-but-not-showing-ads-are-being-rejected-from-app-store/>.

²² Google Play: Verwendung der Android-Werbe-ID, Richtlinien für Entwickler, https://play.google.com/intl/de_ALL/about/monetization-ads/ads/ad-id/. Zugegriffen: 23.Febr.2017.

Ein Verstoß gegen die Richtlinien kann zur Folge haben, dass die jeweilige Applikation aus den Stores entfernt, bzw. beim Review zurückgewiesen wird. Das ist keine leere Drohung ist, zeigen ein Blick in Foren wie Stack-Over-Flow²³ bzw. Gespräche mit Entwicklern. Und wie oben schon angedeutet, sorgt dieses Szenario gegebenenfalls für mehr Schweißperlen auf der Stirn als die Aussicht, dass möglicherweise doch einmal ein Bescheid der Datenschutzbehörde kommt.

3.2.2 Brauche ich jetzt eine Einwilligung für die Nutzung von Werbe-IDs oder nicht?

Sollte der geneigte Leser inhaltlich gerade ein wenig darüber stolpern, dass es eingangs dieses Unterkapitels hieß, eine Einwilligung des Nutzers sei schon bei einem reinen Tracking über die Werbe-ID nötig, während nun die Entwickler-Richtlinien dergestalt wiedergegeben werden, dass eine Einwilligung erst bei der weiteren Verknüpfung von Daten notwendig sei, so stolpert er in gewisser Weise zu Recht.

Sowohl nach bisher herrschender Auffassung der Datenschutzbeauftragten als auch nach dem der DSGVO zugrunde gelegten Verständnis sind Daten wie die IP-Adresse oder eine Werbe-ID personenbeziehbar, so dass zur Verwendung schon dieser Daten eine Einwilligung des Nutzers vorliegen muss. Diese in der Vergangenheit kontrovers und scharf diskutierte Frage wurde auch vom EuGH im oben verstandenen Sinne entschieden. Danach soll es zwar nicht genügen, dass eine beliebige Person zur Identifizierung der Person in der Lage wäre. Es reicht jedoch aus, wenn der Internetanbieter die rechtlichen Möglichkeiten dazu besitzt. Dazu zählt bspw. schon die Möglichkeit, sich im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten.²⁴ Allein dadurch wird eine Person durch die Daten bestimmbar bzw. identifizierbar. In Deutschland und Europa herrscht damit ein weites Verständnis vom Personenbezug, dass für Unternehmen spätestens mit Geltung der DSGVO ab 2018 maßgeblich sein wird. Denn dann muss der Nutzer bei einer Verwendung von Werbe-IDs nicht mehr nur informiert werden, so wie es die Entwicklerrichtlinien fordern. Für

²³ Beispielhaft: <http://stackoverflow.com/questions/21489097/my-app-was-just-rejected-for-using-the-ad-support-framework-which-library-is-re>; <http://stackoverflow.com/questions/30553598/app-rejected-due-to-adsupport-framework>.

²⁴ InfoCuria: EuGH, Urteil vom 19. Okt.2016 in der Rechtssache C-582/14. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>. Zugriffen: 23. Febr.2017

eine datenschutzkonforme Nutzung ist vielmehr die Einwilligung bereits beim Tracking (und nicht erst bei einer Verknüpfung der Werbe-ID mit weiteren Daten) erforderlich.

3.3 Fazit

Nach alldem ist festzuhalten, dass grundsätzlich Einwilligungen von Nutzern für die Verwendung von Werbe-IDs für das Tracking eingeholt werden müssen – Datenschutzerklärungen allein reichen dafür nicht aus. An dem Einwilligungserfordernis für die Verknüpfung der Werbe-ID mit anderen personenbezogenen Daten, also auch statischer Geräte-IDs, ändert sich dagegen nichts. Sowohl das Tracking als auch die Verknüpfung sind damit einwilligungsbedürftig.

Möglicherweise lachen Sie gerade schallend, weil Sie noch nicht ein einziger Anbieter irgendwo gefragt hat, ob er Ihre Werbe-ID zu Zwecken des Trackings verarbeiten darf. Denn es ist tatsächlich nicht verständlich, dass über die Frage der Personenbeziehbarkeit von IP-Adressen scheinbar endlos gestritten und geschrieben wurde, während Geräte-IDs und Werbe-ID ihr Leben abseits der öffentlichen Diskussion im datenschutzrechtlichen Schatten führen. Es könnte daran liegen, dass inzwischen viele Juristen eine Vorstellung von einer IP-Adresse haben, kaum aber von weiteren Tracking-Methoden. Doch wie dem auch sei, die DSGVO ist hier eindeutig. Die DSGVO benennt derartige IDs wörtlich. Folglich müssen entsprechende Einwilligungen eingeholt werden – es sei denn, man mag die Möglichkeit äußerst kostspieliger Bußgeldbescheide in Kauf nehmen.

4 Mobile Advertising, Mobile-Shops, Adblocker & Wettbewerbsrecht

Mit dem mobilen Advertising, dem M-Commerce und dem „Gesetz gegen den unlauteren Wettbewerb“ (kurz UWG) verhält es sich ganz einfach: Das UWG gilt – gleich ob analog oder (mobil) digital geworben und verkauft wird. Das heißt, es darf etwa kein Verbraucher in die Irre geführt, der Werbecharakter von geschäftlichen Handlungen nicht verschleiert,²⁵ Kinder nicht gezielt werblich mit

²⁵ Von Content-Marketing (Y-Titty), Leserporträts (Handelsblatt) und Schleichwerbung, 28. März 2014. <http://www.socialmediarecht.de/2014/03/28/von-content-marketing-y-titty-leserportraets-handelsblatt-und-schleichwerbung/>.

Kaufaufforderungen angesprochen²⁶ und Mitbewerber dürfen weder herabgesetzt noch gezielt behindert werden.²⁷ Dazu darf selbstverständlich nicht gegen gesetzliche Vorschriften verstoßen werden, die dazu bestimmt sind, im Interesse der Marktteilnehmer das Marktverhalten zu regeln – wie etwa die Datenschutzvorschriften.²⁸ In all diesen Fällen können Mitbewerber oder Verbände den Werbetreibenden abmahnen.

Eine solche Abmahnung zwingt den Abgemahnten wirtschaftlich noch nicht in die Knie. Bei einem Unterlassungsstreitwert von 10.000 Euro werden im außergerichtlichen Verfahren für den eigenen und gegnerischen Anwalt zusammen gut 1800 Euro fällig. Ärgerlich ist sie aber allemal, da die Rechtslage – trotz des neuen, mobilen Umfeldes – in der Regel eindeutig sein wird.

Nun ist es in den kleinen mobilen Ansichten zugegebenermaßen schwierig, all den Informationspflichten, die Werbetreibenden gerade im M-Commerce und mobilen Advertising auferlegt werden, nachzukommen. Doch auch hier gilt beispielsweise, dass der Anbieter der Ware oder Dienstleistung im Fall der Werbung mit abschlussfähigen Angeboten (wie beispielsweise: Kreuzfahrt ab Kiel mit der MS Nordia, Norwegischen Fjorde, 12.10. – 19.10., Innenkabine, All-Inc. 499,- EUR p.P.) schon in der Werbung klar gekennzeichnet werden muss – und zwar unter Nennung der geschäftlichen Zeichnung und der Adresse.²⁹ Und genauso müssen auch in Mobile-Shops (bzw. den entsprechenden Apps) die Preise regelrecht ausgezeichnet oder die Widerrufsbelehrung und das Impressum vorhanden und leicht erreichbar sein.

Der mangelnde Platz ist dabei jedoch kein Grund, den gesetzlichen Pflichten nicht oder nur unvollständig nachzukommen. Dies entschied das OLG Hamm

²⁶ Zum Verbot der gezielten Werbeansprache von Kindern bei In-App-Käufen: BGH, Urteil vom 17. Juli 2013, Az. I ZR 34/12. <https://openjur.de/u/639396.html>.

²⁷ Zur gezielten Verhinderung von Mitbewerbern: Diercks, Nina, – Warum Sie für die schmutzigen Tricks Ihrer Affiliate-Partner haften, Lead Digital, 16. Jan. 2014, zur Entscheidung des OLG Köln vom 18. Oktober 2013, Az. 6 U 36/13. http://www.lead-digital.de/aktuelle/e_commerce/warum_sie_fuer_die_schmutzigen_tricks_ihrer_affiliate_partner_haften.

²⁸ OLG Hamburg: Mangelhafte Datenschutzerklärungen sind wettbewerbswidrig und mit Abmahnungen angreifbar, Artikel vom 11. Juli 2013. <http://www.socialmediarecht.de/2013/07/11/olg-hamburg-mangelhafte-datenschutzerklarungen-sind-wettbewerbswidrig-und-mit-abmahnungen-angreifbar>. Klarstellung nun auch durch den Gesetzgeber in § 2 UKlaG; siehe oben 2.3.

²⁹ OpenJur: Schleswig-Holsteinisches OLG, Az. 6 U 28/12, Urteil vom 03. Juli 2013. <https://openjur.de/u/641138.html>. Zugriffen: 23. Febr. 2017

bereits 2009³⁰ und seit der letzten UWG-Reform 2015 ergibt sich dies auch aus dem Gesetz: § 5a Abs. 5 UWG bestimmt für den Fall, dass bei nicht ausreichendem Raum oder ausreichender Zeit zur Bereitstellung der Informationen diese dem Verbraucher mitunter auf andere Weise zur Verfügung gestellt werden müssen. Infolgedessen sind hier ganz besonders die UX-Designer gefragt.

Im Zusammenhang mit Mobile Advertising sind derzeit AdBlocker ein großes Thema. Unter wirtschaftlichen Aspekten ist die Aufregung verständlich. Juristisch ist aber schon lange klar, dass Werbeblocker grundsätzlich nicht wettbewerbswidrig sind. Dies entschied bereits 2004 der BGH in Bezug auf die „Fernsehfee“, ein Gerät, das Werbeblöcke im Fernsehen ausblendet.³¹ Nun gibt es für Internet- wie Mobile-Werbung inzwischen Adblocker wie „AdBlock Plus“, bei denen eine Whitelist-Funktion, „gute“ (d. h. von den Werbetreibenden nochmals bezahlte) Werbung einblendet.

Hiergegen liefen die Verlage mit Erfolg Sturm. Während die Landgerichte in Köln, München und Hamburg³² in dem Angebot „nur das Werkzeug des Nutzers, das ihm die Ausübung seiner Handlungsalternativen ermöglicht“, erkannten und „diese Freiheit als Teil der grundrechtlich geschützten negativen Informationsfreiheit der Nutzer“ ansahen, hielt das OLG Köln (die Berufungsinstanz) das bezahlte Whitelisting von AdBlock Plus für eine aggressive geschäftliche Handlung gegenüber den Werbenden, welche wettbewerbswidrig sei.³³ Das Adblocking selbst soll damit aber weiterhin zulässig bleiben, lediglich das bezahlte Geschäftsmodell sei nicht mit dem Wettbewerbsrecht vereinbar. Für ein Ende der Diskussion dürfte hier wohl erst die – vom OLG Köln zugelassene – Revision durch den BGH sorgen.

³⁰ OpenJur: OLG Hamm, Urteil vom 16. Juni 2009 · 4 U 51/09. <https://openjur.de/u/31346.html>. Zugegriffen: 23. Febr.2017

³¹ Telemedicus: BGH: Zur Zulässigkeit von Werbeblockern – Fernsehfee, Urteil v. 24. Juni 2004, Az. I ZR 26/02. <http://tlmd.in/u/509>. Zugegriffen: 23. Febr.2017

³² LG München, Urteile vom 27. Mai 2015, Az. 37 O 11673/14 <https://openjur.de/u/771330.html> und Az. 37 O 11843/14. <https://openjur.de/u/771387.html>; LG Hamburg, Urteil vom 21. Apr.2015, Az.416 HKO 159/14. <http://www.landesrecht-hamburg.de/jportal/portal/page/bsharpprod.psml?showdoccase=1&doc.id=JURE150011562&st=ent>; zur Entscheidung des LG Köln vom 29. Sept.2015 – Ziegelmayer, David, CMS HS Bloggt, „LG Köln: Werbeblocker Adblock Plus ist (noch immer) nicht wettbewerbswidrig“. <http://www.cms-hs-bloggt.de/gewerblicher-rechtsschutz/wettbewerbsrecht/lg-koeln-werbeblocker-adblock-plus-ist-noch-immer-nicht-wettbewerbswidrig/>.

³³ Justiz-online: OLG Köln, Urteil vom 24. Juni 2016 – Az. 6 U 149/15, https://www.justiz.nrw.de/nrwe/olgs/koeln/j2016/6_U_149_15_Urteil_20160624.html. Zugegriffen: 23. Febr.2017

5 Beacon-Technologie aus rechtlicher Sicht

Beacons („Leuchtfeuer“) sind kleine Sender, die, basierend auf dem neuen Bluetooth-Standard 4.0, spezielle Mitteilungen mit hinterlegten Services und Informationen an die mobilen Geräte der Smartphone User im Umkreis von zwei bis 30 Metern senden können. Die einzige Funktion von einem Beacon ist das permanente Aussenden eines Signals. Dieses Signal beinhaltet eine eindeutige Identifikationsnummer.³⁴ Die Idee hinter den Beacons ist, Smartphone-Nutzer, die sich in der Nähe eines solchen Leuchtfeuers befinden, zu erreichen. Zum Beispiel, um ihnen in einem Ladengeschäft aktuelle Angebote direkt per Push-Nachricht zu übersenden oder den Nutzer zielgerichtet an einem langen Zug zu dem Waggon, in dem eine Sitzplatzreservierung vorgenommen wurde, zu geleiten.

Um aber solche Nachrichten und/oder Informationen auf dem Smartphone des Users qua Beacon-Signal auszulösen, muss – zumindest bei den iBeacons von Apple – überhaupt eine entsprechende App auf dem Smartphone installiert sein. Die Beacon-Technologie „Eddystone“ von Google kann demgegenüber wohl auch ohne App unmittelbar Webanzeigen oder sonstige Informationen im Browser des Nutzers anzeigen.³⁵

5.1 Beacon-Technologie & Datenschutz

Wie dargestellt, bedarf es zur „Auswertung“ des Beacon-Signals, also z. B. dem Einblenden einer Rabatt-Aktion, eines Empfänger-Programms auf dem Smartphone des Users. Dies wird in der Regel eine App, z. B. des Ladenlokal-Inhabers, sein. Da eine solche App wiederum gewöhnlich (s.o.) mit einem Nutzerkonto verbunden ist, werden hier personenbezogene Daten erhoben und gespeichert. Zum Beispiel, dass Nutzer A am Tag X zur Uhrzeit Y im Ladengeschäft Z war und sich im Bereich der Produktgruppe 123 aufgehalten hat.

³⁴ Süssel, Alexander: Beacon Kompendium (1/5) – Am Anfang steht die Technik, mobile zeitgeist, 25. Nov.2014, <http://www.mobile-zeitgeist.com/2014/11/25/beacon-kompendium-am-anfang-steht-die-technik/>. Zugegriffen: 23. Febr.2017

³⁵ Google Beacons, Eddystone format, Entwickler-Leitfäden: <https://developers.google.com/beacons/eddytone>; Vgl. auch Heise-Online vom 15. Juli 2015, Beacon-System Eddystone: Google veröffentlicht quelloffenes Format zur Indoor-Navigation. <http://www.heise.de/newsticker/meldung/Beacon-System-Eddystone-Google-veroeffentlicht-quelloffenes-Format-zur-Indoor-Navigation-2750923.html>

Aufgrund dieses direkten Personenbezugs ist eine solche Datenverarbeitung wie schon oben erläutert grundsätzlich nur mit der Einwilligung des Nutzers möglich. Diese Einwilligung könnte nur dann entbehrlich sein, wenn die Datenverarbeitung zur Vertragserfüllung notwendig wäre, z. B. um eben dem Kunden bestimmte Rabatt-Aktionen anbieten zu können. Denn die Datenerhebung zur Vertragserfüllung ist gesetzlich erlaubt. In diesem Fall müsste der Nutzer aber jedenfalls hinreichend über die Datenverarbeitung mittels einer Datenschutzerklärung bei der Installation der App informiert werden. Ob eine derartige Erhebung von Standortdaten über den Zweck der Vertragserfüllung gerechtfertigt sein kann, ist im Einzelfall zu prüfen. Bei der reinen Übersendung von Angebotshinweisen wird dies in der Regel wohl nicht ausreichen.

Um ein Double-Opt-In-Verfahren mit einer ausdrücklichen Einwilligung des Users wird der Anbieter von Marketing-Aktionen via Beacon-Technologie aber kaum umhinkommen – selbst wenn die Erhebung von personenbezogenen Geo-Daten mit dem Zweck der Vertragserfüllung gerechtfertigt werden könnte.

5.2 Beacon-Technologie & Wettbewerbsrecht

Natürlich macht das Wettbewerbsrecht auch vor den Beacons nicht halt. Und nach § 7 Abs. 2 Nr. 3 UWG stellt nun mal „Werbung unter Verwendung [...] elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt“ eine unzumutbare Belästigung dar. Und eine „unzumutbare Belästigung“ ist wettbewerbswidrig. Darüber hinaus stellt sie auch noch einen Eingriff in das Persönlichkeitsrecht eines jeden Einzelnen dar, der dann wiederum einen Unterlassungsanspruch gegenüber dem Absender der Werbung hat. Das heißt, für eine derartige Direct Message bedarf es eben der ausdrücklichen Zustimmung des Nutzers, denn dass Gerichte eine Push-Nachricht ebenfalls unter dem Begriff der elektronischen Post subsumieren, ist nahezu sicher.

Spannend ist die Frage, wie die Google-Technologie hier in einiger Zeit von den Gerichten bewertet werden wird. Denn wenn keine App mehr notwendig ist, sondern via Eddystone z. B. ein Overlay in den Browser gelegt werden kann, der einem die aktuellen Angebote des lokalen Umfeldes anzeigt, ist das keine elektronische Post im bisherigen Sinne, sondern eine „plötzlich auftretende Werbeanzeige“. Dass sich diese Umsetzung durchsetzt, vermag ich allerdings aus anderen Gründen kaum zu glauben: Die User nutzen schon jetzt AdBlocker-Software und wollen sicher nicht eine Werbeanzeige sehen, obwohl sie eigentlich gerade einen Spiegel-Online-Artikel lesen und nur zufällig vor einem lokalen Geschäft stehen.

Davon einmal ab gilt aber natürlich auch für die Werbeanzeigen und Rabatt-Gutscheine das Wettbewerbsrecht im Übrigen. Neben den schon unter Ziffer 4 aufgeworfenen Grundsätzen heißt das auch, dass der Verbraucher nicht unter unmäßigen Kaufdruck gesetzt werden darf. Etwa durch den Hinweis „Angebot nur noch 5 Minuten gültig“ o. ä.

5.3 Fazit zur Beacon-Technologie

Letztlich gilt für denjenigen, der mit der Beacon-Technologie arbeiten möchte, nichts anderes als für jeden anderen App-Betreiber auch: Die rechtlichen Anforderungen sollten in der Planungsphase geprüft und bei der technischen Realisierung direkt berücksichtigt werden. Damit lassen sich die rechtlichen Risiken minimieren und gegebenenfalls auch das eine oder andere Verbrauchervertrauen langfristig gewinnen.

6 Fazit

Die vorstehenden Punkte enthielten zum Teil Worst-Case-Szenarien. Aber zum einen ist es der Job des Anwalts, das Worst-Case-Szenario kommen zu sehen – und zwar um es beurteilen, dessen Eintritt verhindern bzw. das bestehende Risiko vermindern und Lösungen aufzeigen zu können. Zum anderen lässt sich alles drehen und wenden, wie man will: Mobile Business ist ein Business. Jedes Business hat Regeln. Man kann sich entscheiden mit den oder gegen die Regeln zu spielen. Jedoch sollten zumindest die Risiken der Entscheidung bekannt sein. Um sich bewusst entscheiden zu können – dafür oder dagegen.

In diesem Sinne – auf ein erfolgreiches Mobile Business.

Die Autorin

Rechtsanwältin Nina Diercks, M.Litt (University of Aberdeen) führt die Anwaltskanzlei Diercks, ist Gründerin des Social Media Recht Blog und anerkannte Datenschutz-Sachverständige (genau genommen: „Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IT-Produkte (rechtlich)“). In ihrer täglichen Arbeit beschäftigt sie sich mit all den juristischen Fragen, mit denen sich Unternehmen im Zusammenhang mit der digitalen Welt auseinandersetzen müssen. Ihre Tätigkeitsschwerpunkte liegen in der Beratung, Vertragsgestaltung und Vertretung auf dem Gebiet des IT-, Medien-, Datenschutz- und Arbeitsrechts.

<http://www.springer.com/978-3-658-16603-8>

Social goes Mobile - Kunden gezielt erreichen

Mobile Marketing in Sozialen Netzwerken

Scholz, H. (Hrsg.)

2017, XIII, 227 S. 29 Abb., 19 Abb. in Farbe. Book +

eBook., Softcover

ISBN: 978-3-658-16603-8