Sven Venzke-Caprarese

Standortlokalisierung und personalisierte Nutzeransprache mittels Bluetooth Low Energy Beacons

Datenschutzrechtliche Rahmenbedingungen einer möglicherweise bald alltäglichen Datenverarbeitung

Nur wenigen neuen Technologien wird derzeit das Potential zugetraut, unseren Alltag in Zukunft langfristig beeinflussen und verändern zu können. Eine dieser Technologien verspricht Unternehmen die Möglichkeit, den Standort von Kunden in den eigenen Räumlichkeiten zu erfassen, die erfassten Kunden zu individualisieren und standort- bzw. kundenspezifisch über elektronische Medien anzusprechen. Unter dem Begriff Bluetooth Low Energy Beacon hat es ein potentieller Technologie-Mega-Trend geschafft, sich bisher relativ unbemerkt zu entwickeln. Dieser Artikel beschreibt, worum es sich bei den genannten Beacons handelt, wie diese eingesetzt werden können und bewertet die datenschutzrechtlichen Rahmenbedingungen der jeweiligen Einsatzmöglichkeiten.

1. Funktionsweise

Um die Funktionsweise von Bluetooth Low Energy Beacons zu verstehen, müssen drei Dinge betrachtet werden: Bluetooth Low Energy Beacons an sich, bluetoothfähige Smartphones sowie die auf dem Smartphone installierten Applikationen.

1.1 Bluetooth Low Energy Beacons

Bei Bluetooth Low Energy Beacons handelt es sich in der Regel um kleine, etwa zweifingergroße Geräte mit Batteriebetrieb, die kontinuierlich über Bluetooth 4.0 ein Signal mit gleichbleibenden Informationen aussenden. Die gesendeten Informationen bestehen dabei aus einer festen Zeichenfolge, die vom Betreiber des Beacons festgelegt werden kann und die eine eindeutige Identifikation des Beacons ermöglicht. Der bekannteste Standard für Bluetooth Low Energy Beacons stammt von Apple und nennt sich iBeacon. Ein iBeacon überträgt grundsätzlich vier Informationen. Zum einen die sog. UUID[1] – eine mehrstellige Zeichenfolge, die als übergeordnetes Zuordnungsmerkmal verwendet werden kann. Zum anderen die beiden Zahlenwerte Major und Minor.[2] Aus diesen drei Zeichenfolgen in Kombination ergibt sich die jeweilige Beacon-ID. Schließlich wird auch noch ein Indikator für die Sendeleistung des Beacons übertragen.[3]

Ein solcher Beacon kann an einem bestimmten Ort platziert werden, um diesen fortan zu markieren, indem die Beacon-ID und die Sendeleistung mittels eines dauerhaften Bluetooth-Funkfeuers ausgesendet werden. Die Reichweite dieses Funkfeuers umfasst im Freien einen Umkreis von bis zu 100 Metern. Über weitere Funktionen verfügt der Beacon nicht – insbesondere werden keine Daten empfangen und keine Kopplungen mit anderen Bluetoothgeräten durchgeführt.[4] Auch eine Einstellung der Sig-

Sven Venzke-Caprarese

Rechtsanwalt und Berater bei der datenschutz nord GmbH mit dem Schwerpunkt Datenschutz in neuen Medien

E-Mail: svenzke@datenschutz-nord.de

1 Der Universally Unique Identifier besteht regelmäßig aus 32 Zeichen, die durch Bindestriche in 5 Gruppen aufgeteilt werden (z. B.: „f0018b9b-7509-4c31-a905-1a27d39c003c"). Dieser Wert kann vom Beaconbetreiber konfiguriert werden.

2 Die Werte Major und Minor bestehen regelmäßig aus jeweils 5 Zahlen (z. B. „35545" und „27531") und können vom Beaconbetreiber ebenfalls konfiguriert werden. In der Praxis werden diese Werte oftmals genutzt, um verschiedene Gruppen und Untergruppen zu bilden.

3 Die Sendeleistung wird als sog. TX Power Level bezeichnet und in Dezibel Milliwatt (dBm) angegeben. Die Sendeleistung kann oftmals vom Beaconbetreiber eingestellt sowie ein Indikator für die Sendeleistung kalibriert werden (measured power at a distance of one meter). Diese Werte ändern sich danach nicht mehr.

4 Im Rahmen der Einrichtung und Wartung ist es allerdings möglich, sich nach Eingabe einer PIN-Nummer mit dem Beacon zu verbinden und insbesonde-

nalrichtung ist nicht unmittelbar möglich. Das Signal verbreitet sich in alle Richtungen, wird mit zunehmender Entfernung schwächer und durch Gegenstände zusätzlich abgeschwächt.[5] Lediglich durch die Einstellung der Sendeleistung des Beacons und seine Platzierung kann der vom Signal erfasste Bereich eingegrenzt werden.

1.2 Smartphones

Die vom Beacon ausgehenden Signale können von aktuellen Smartphones mit aktivierter Bluetoothverbindung empfangen werden. Das Smartphone ist somit in der Lage zu erkennen, welche Beacon-IDs sich derzeit in der Nähe befinden und mit welcher Ausgangsleistung die jeweiligen Beacons senden. Und noch eine weitere, ganz entscheidende Information ist verfügbar: die sekündlich vom Smartphone gemessene Stärke des empfangenen Signals.[6] Diese weicht aufgrund der Entfernung des Smartphones zum Beacon von dessen ursprünglicher Sendeleistung ab.

1.3 Applikationen des Beaconbetreibers

Auf dem Smartphone installierte Apps, die Zugriff auf die über Bluetooth empfangenen Daten nehmen können, sind durch Auswertung der gemessenen Signalstärke in der Lage, mehr oder weniger genau abzuschätzen, wie groß die Entfernung des Smartphones zum jeweiligen Beacon ist. Die Werte sind dabei nicht hochpräzise. Zum einen kann anhand der geschätzten Entfernung kein genauer Standpunkt identifiziert werden, sondern lediglich ein Umkreis, in dem sich ein Beacon befindet. Zum anderen kann die Signalstärke nicht nur durch Entfernung, sondern auch durch andere, sich verändernde Gegebenheiten beeinflusst werden – etwa durch Kundenverkehr oder Störsignale. Je näher das Smartphone dem Beacon allerdings kommt, desto genauer stimmt der geschätzte Umkreis regelmäßig mit der echten Entfernung überein. Zudem ist durch den Einsatz von mehreren, sich in der Reichweite überschneidenden Beacons auch eine genauere Schätzung des Standpunktes möglich.[7]

Der Beaconbetreiber kann die geschätzte Entfernung des Smartphones zu einem bestimmten Beacon nutzen, um durch die App bei Über- oder Unterschreitung der Entfernung vordefinierte Aktionen ausführen zu lassen. Je nach Betriebssystem des Smartphones ist es hierzu noch nicht einmal erforderlich, dass die App geöffnet ist.[8]

2. Einsatzmöglichkeiten

Sofern ein Beaconbetreiber Nutzer dazu bringt, die von ihm angebotene App zu installieren, Bluetooth zu aktivieren und den Zugriff auf Standortdaten freizugeben, stehen ihm vielfältige Möglichkeiten offen: Der App des Beaconbetreibers ist in diesem Fall regelmäßig bekannt, welche Standorte durch die empfangenen Beacon-IDs markiert werden und in welcher ungefähren Entfernung sich der Nutzer zu dem jeweiligen Beacon befindet. Dieses Wissen kann dazu genutzt werden, um ab einer bestimmten Entfernung zum Beacon verschiedene Aktionen auszulösen – etwa eine Push Notification zu versenden, Daten an den Unternehmensserver zu übermitteln, Daten abzufragen, Steuerbefehle abzusetzen etc. Die geringe Sendereichweite des Beacons ist dabei eher ein Vor- als ein Nachteil. Denn insbesondere in Innenräumen, in denen eine klassische Ortung mittels GPS mangels Sichtverbindung zum Satelliten keinen Erfolg verspricht, bieten Beacons mit relativ wenig Aufwand und Kosten[9] eine sehr gute Präsenzerkennung.

2.1 Rein standortbezogene Aktionen

Beacons können in Verbindung mit Apps vielfältig genutzt werden. So könnten Museen ihren Besuchern etwa empfehlen, die museumseigene App vor dem Museumsbesuch herunterzuladen, um auf dem Smartphone Informationen über die jeweiligen Exponate anzubieten, sobald sich ein Besucher einem Exponat auf z. B. einen Meter nähert. Zu dieser standortbasierten Nutzeransprache wäre während des Besuchs noch nicht einmal zwingend eine Internetverbindung erforderlich, sofern die jeweiligen Beacon-IDs, alle aktionsauslösenden Regeln und sämtliche Inhalte in der App hinterlegt wären.

Die Möglichkeiten gehen dabei über das Anzeigen von statischen Inhalten hinaus. Stattet z. B ein Retail-Shop seine Verkaufsflächen mit Beacons aus, könnten Besucher bei Betreten des Shops mittels einer durch die App ausgelösten Push Notification über tagesaktuelle Angebote und Verkaufsaktionen informiert werden. Hier wäre jedoch eine Internetverbindung erforderlich, um die tagesaktuellen Angebote abzufragen.

Durch den Einsatz von Beacons ergeben sich auch neue Analysemöglichkeiten. Der Betreiber eines Retailshops könnte sich über seine App alle Standortdaten auf seine Server übermitteln lassen und diese auswerten. Eine Möglichkeit, die bereits genutzt wird, ist das Erstellen von sog. Heatmaps. Hierbei handelt es sich um eine – bisher eher im Online-Bereich verbreitete – Visualisierung, welche Standorte bzw. Umkreise insgesamt wie häufig betreten wurden. Aber auch die Auswertung des Bewegungsverhaltens eines einzelnen Besuchers ist möglich – insbesondere, wenn viele Beacons feinmaschig eingesetzt werden und sich die Sendereichweite von benachbarten Beacons überschneidet.

Bei allen bisher dargestellten Möglichkeiten ist zu beachten, dass der Beaconbetreiber keine Kenntnis haben muss, wer genau angesprochen bzw. analysiert wird.

re die drei Werte UUID, Major, Minor sowie die Sendeleistung des Beacons zu ändern. So kann es z. B. sinnvoll sein, die Sendeleistung des Beacons zu verringern, um einen bestimmten Bereich noch enger einzugrenzen.

5 Eine gute Übersicht der technischen Hintergründe bietet insgesamt: https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf (zuletzt abgerufen am 5.10.2014).

6 Genau genommen kann das Sendeintervall individuell vom Beaconbetreiber vorgegeben werden und sich auch im 100 Millisekundenbereich bewegen.

7 Etwa durch Lateration. Empfängt ein Smartphone das Signal von einem Beacon und errechnet dabei eine ungefähre Entfernung, so kann der mögliche Standort lediglich durch einen Kreis beschrieben werden. Werden aber gleichzeitig Signale von zwei Beacons erfasst, liegt der mögliche Standpunkt an den beiden Schnittpunkten von zwei sich überschneidenden Kreisen. Kommt ein drittes Beaconsignal hinzu, kann ein konkreter Standpunkt am Schnittpunkt der drei Kreise vermutet werden.

8 So ermöglicht iOS z. B. Hintergrundaktualisierungen. Empfängt ein Smartphone bestimmte UUIDs, werden im Vorfeld zugeordnete Apps im Hintergrund aktiviert und die Informationen an die App durchgereicht. Die App kann daraufhin mit der Datenverarbeitung beginnen – sogar wenn das Smartphone gerade gesperrt ist und sich bspw. in der Hosentasche befindet.

9 Ein Beacon kostet derzeit für Privatanwender ca. 20 Euro. Für Unternehmen, die Beacons in großen Massen verwenden wollen, werden die Kosten nur einen Bruchteil betragen.

2.2 Personalisierte Aktionen

Die Datenverarbeitungsmöglichkeiten beschränken sich jedoch nicht auf standortbezogene Aktionen. Zentrale Bedeutung kommt insoweit der Gestaltung der App und der vorhandenen Kundendatenbank des Beaconbetreibers zu. Sofern die App des Beaconbetreibers in der Lage ist, den Smartphonenutzer zu identifizieren,[10] ist es möglich, dass die App eventuell vorhandene Zusatzinformationen aus der Kundendatenbank des Beaconbetreibers abfragt und diese Information genutzt wird, um den Nutzer des Smartphones personalisiert anzusprechen.

So könnte der Nutzer z. B. per Push Notification im Retail Store namentlich begrüßt und ihm ein Angebot in einer Produktgruppe angeboten werden, für die sich der Kunde in der Vergangenheit schon interessierte. Es wäre auch möglich, ein Bonussystem zu entwickeln, welches Kunden dafür belohnt, dass sie besonders häufig die Shops des Beaconbetreibers besuchen.

Derzeit sind Beacons auch für Betreiber von Sportstadien oder Theater interessant. Erhält eine App z. B. Zugriff auf das elektronische Ticket des Besuchers, kann dieser zu seinem Platz navigiert werden. Die Beacons weisen insoweit den Weg.

Die durch die App ausgelösten Aktionen können sogar über das Bereitstellen von Informationen auf dem Smartphone hinausgehen. Bedenkt man, dass sich der Beacon grundsätzlich in einem Bereich befinden wird, auf den der Beaconbetreiber Einfluss hat, ist es sogar möglich, den Kunden über andere Wege als sein Smartphonedisplay anzusprechen. So könnten elektronische Displays oder Lautsprecher im Shop des Beaconbetreibers genutzt werden, um personalisierte Inhalte bereitzustellen, wenn ein bestimmter Kunde an diesen vorbeigeht. Die App könnte insoweit zu einer umgehenden Personalisierung der Umgebung des Kunden führen, ohne dass dieser auch nur sein Smartphone in die Hand nehmen müsste oder von der im Hintergrund ausgelösten Datenverarbeitung etwas mitbekommen würde. Was wäre hierzu erforderlich? Der Beacon müsste seine Beacon-ID aussenden, die vom Smartphone empfangen und an die App des Beaconbetreibers weitergereicht werden würde. Die App würde daraufhin eine Verbindung zum Unternehmensserver aufbauen und die Beacon-ID, die errechnete Entfernung sowie Identifikationsdaten des Nutzers mitteilen. Auf dem Unternehmensserver müsste eine Art Kontaktmanagementsoftware betrieben werden, die den aktuellen Standort des Kunden abfragt und erkennt, dass dieser sich z. B. in einem bestimmten Ladengeschäft in der Nähe eines bestimmten Bildschirms oder Lautsprechers befindet. Gleichzeitig könnte die Kontaktmanagementsoftware über eine Schnittstelle zur Kundendatenbank abfragen, ob der Nutzer bereits Kunde ist und Kaufinteressen gespeichert wurden. Ist dies der Fall, würde die Kontaktmanagementsoftware passende Medieninhalte auswählen, die an den mit einem Medienserver verbundenen Bildschirm oder Lautsprecher im Ladengeschäft übertragen werden. Der Kunde erhielte so personalisierte Werbung im Vorbeigehen, ohne von der im Hintergrund ablaufenden Datenverarbeitung etwas bemerkt zu haben, ohne die App zu öffnen und sogar ohne sein Smartphone in die Hand nehmen zu müssen. Die möglichen Anwendungsszenarien werden mit der Verbreitung des sog. „Internet der Dinge" künftig noch erheblich zunehmen.[11]

Auch die Analysemöglichkeiten werden sich durch die Verwendung von Beacons, insbesondere im Falle der Identifikation des Smartphonenutzers, erheblich erhöhen. Fragen, die im Online-Bereich alltäglich sind, werden plötzlich auch für den Retail-Bereich denkbar: Welcher Kunde war wann im Shop? Ist der Besuch des Kunden im Shop auf eine vorhergehende Werbeaktion zurückzuführen und erhöht insofern deren Conversion-Rate? Wie hat sich der Kunde im Shop bewegt und wie wurde auf personalisierte Ansprachen reagiert?

3. Aktuelle Verbreitung und Prognose

Technologieanalysten sehen Beacons als eine der kommenden Top-Technologien[12] und gehen davon aus, dass in den nächsten fünf Jahren 60 Millionen Beacons weltweit genutzt werden[13].

Tatsächlich erfahren insbesondere iBeacons schon derzeit vor allem in den USA eine größere Verbreitung. So kündigte etwa Macy's, der größte Kaufhausbetreiber in den USA, im September 2014 an, alle seine Kaufhäuser mit iBeacons auszustatten und in diesem Rahmen über 4.000 iBeacons zu installieren.[14] Zudem sind seit kurzem nahezu alle Sportstadien der Major League Baseball mit Beacontechnologie ausgestattet,[15] ebenso wie über 250 Apple Stores. Auch Fluggesellschaften und Flughafenbetreiber bereiten sich auf den großflächigen Einsatz von iBeacons vor.[16] In Europa kommen iBeacons z. B. an Flughäfen in London (LGW und LTN) sowie Paris (CDG) zum Einsatz.[17] Auch in Deutschland werden die ersten iBeacons eingesetzt, etwa in Schnellrestaurants.[18]

Es wird zu beobachten sein, ob und wie sich die durch iBeacons ausgelösten Datenverarbeitungen entwickeln und ob iBeacons zum Mega-Trend werden oder lediglich ein kurzzeitiges Phänomen darstellen. Für die Entwicklung zum Mega-Trend spricht allerdings, dass die Einsatzmöglichkeiten enorm sind und Datenverarbeitungen, die bisher nur auf Internetseiten und Online-Shops denkbar waren, plötzlich auch in Ladengeschäften vor Ort möglich sind. Auch der Datenhunger, den viele Unternehmen im Online Bereich in der Vergangenheit gezeigt haben, spricht dafür, dass iBeacons – oder vergleichbare Beacon-Technologien – in Zukunft alltäglich werden. Möglicherweise werden sich auch die Hürden, die Beaconbetreiber momentan noch zu nehmen haben, in Zukunft reduzieren. So ist es in Zukunft vielleicht nicht mehr erforderlich, dass Beaconbetreiber den Smartphone-

10 Etwa weil eine personalisierte Anmeldung erforderlich ist oder weil ein über die App angebotener und genutzter Online-Gutschein den Nutzer bereits in der Vergangenheit identifiziert hat etc.

11 Neben Unternehmen mit lokalem Kundenkontakt sind Betreiber von Hausautomationslösungen schon heute eine weitere Zielgruppe von Beaconherstellern.

12 Gartner, Gartner Identifies Top 10 Mobile Technologies and Capabilities for 2015 and 2016,http://gtnr.it/1fmWolA (zuletzt abgerufen am 5.10.2014).

13 ABI Research, iBeacon/BLE Beacon Shipments to Break 60 Million by 2019, http://bit.ly/1s2JnTC (zuletzt abgerufen am 5.10.2014).

14 Washington Post, Is the new technology at Macy's our first glimpse of the future of retail? http://wapo.st/1ro57J2 (zuletzt abgerufen am 5.10.2014).

15 Techcrunch, MLB's iBeacon Project Enters Phase Two With Interactive Ballpark Attractions, http://tcrn.ch/TWqHX4 (zuletzt abgerufen am 5.10.2014).

16 Sita Aero, Sita shows the way for iBeacon Technology at airports, http://bit.ly/1iQkVlY (zuletzt abgerufen am 5.10.2014).

17 EasyJet Twitter Pressemitteilung, http://t.co/C0a5yDZTmX (zuletzt abgerufen am 5.10.2014).

18 Wirtschafts Woche, McDonald´s probiert Beacon-Funktechnik aus, http://bit.ly/1mEGPIQ (zuletzt abgerufen am 5.10.2014).

nutzer dazu bringen müssen, dass dieser ihre App installiert und sich „bestenfalls" durch Angabe von Namen oder E-Mail-Adresse auch identifiziert. Vielmehr ist es denkbar, dass Betreiber weit verbreiteter und betriebssystemübergreifender Apps den Beaconbetreibern anbieten, bei Empfang bestimmter Beacon-IDs die vom Beaconbetreiber festgelegten Aktionen auszuführen oder Informationen weiterzuleiten. Dies könnte insbesondere ein Geschäftsmodell für Betreiber von Apps werden, deren Apps die Nutzer nicht nur identifizieren, sondern vielfältiges Zusatzwissen zu diesen gespeichert haben.[19] Insbesondere für Betreiber von sozialen Netzwerken zeichnet sich möglicherweise ein neues, interessantes Geschäftsfeld ab.

4. Rechtliche Rahmenbedingungen

Um die rechtlichen Rahmenbedingungen für den Einsatz von iBeacons bestimmen zu können, müssen neben den iBeacons auch die auf dem Smartphone und die innerhalb der jeweiligen App stattfindenden Datenverarbeitungen bewertet werden.

4.1 Verwendung von iBeacons

Betrachtet man den Beacon an sich, ist festzustellen, dass dieser lediglich seine eigene Beacon-ID nebst Ausgangssendeleistung überträgt und keinerlei Daten empfängt. Sofern der Beacon lediglich dafür genutzt wird, bestimmte Orte zu markieren und keine Personen oder mobile Gegenstände[20], stellt weder die Beacon-ID ein personenbezogenes Datum dar, noch findet eine Verarbeitung personenbezogener Daten durch den Beacon statt. Die Installation eines solchen Beacons ist daher frei von datenschutzrechtlichen Restriktionen. Selbst eine Hinweispflicht auf den Einsatz von Beacons besteht somit nicht. Hieran ändert auch die Tatsache nichts, dass sich Smartphonebesitzer mit aktivierter Bluetoothverbindung nicht gegen den Empfang der Beacon-IDs wehren können. Denn ob daraufhin eine personenbezogene Datenverarbeitung erfolgt oder nicht, hängt ausschließlich vom Funktionsumfang des Betriebssystems des Smartphones bzw. der darauf installierten Apps ab. Dieser Funktionsumfang ist es, der letztlich über die datenschutzrechtliche Zulässigkeit entscheidet.

4.2 Signalempfang durch das Smartphone

In dem Moment, in dem die Beacon-IDs vom Smartphone empfangen werden, stellen sie personenbezogene Daten dar, selbst wenn sie zu diesem Zeitpunkt noch gar nicht an die App weitergereicht wurden. Denn die Kenntnis, welche Beacon-IDs vom Smartphone empfangen wurden, erlaubt Dritten, die sowohl die Bedeutung der Beacon-ID kennen, als auch wissen, in wessen Besitz sich das Smartphone befindet, einen Rückschluss auf den Standort des Besitzers. Adressat etwaiger datenschutzrechtlicher Pflichten ist in diesem Stadium jedoch nicht der Beacon- oder Appbetreiber, sondern der Smartphone- bzw. Betriebssystemhersteller. Dieser dürfte z. B. die empfangenen Beacon-IDs nicht abrufen und zu eigenen Zwecken verwenden.[21]

4.3 Datenverarbeitung durch die App

Rechtlich besonders relevant ist jedoch die Datenverarbeitung, die innerhalb der App stattfindet bzw. durch diese angestoßen wird. Sofern Apps personenbezogene Daten verarbeiten, kann der Anwendungsbereich des BDSG eröffnet sein. Stellen diese Apps zudem einen Telemediendienst dar, findet auch das TMG Anwendung.

4.3.1. Apps ohne Onlineanbindung

Es ist durchaus denkbar, dass eine App mit iBeacon-Funktionalität gänzlich ohne Internetverbindung auskommt. Dies ist etwa dann der Fall, wenn mit der erstmaligen Installation der App alle relevanten Informationen geladen werden – also alle benötigten Beacon-Informationen sowie alle damit verknüpften lokalen Aktionen, anzuzeigenden Inhalte etc. Ein Beispiel für eine Offline-App ist die App eines Museums, welche unmittelbar vor dem Besuch geladen werden kann und anschließend weder Inhalte herunterladen noch übermitteln muss. In diesem Fall ist das TMG mangels Onlineanbindung nicht anwendbar.[22] Anwendbar kann aber weiterhin das BDSG sein. Jedoch finden sich für Apps ohne Onlineanbindung kaum klare datenschutzrechtliche Vorgaben. Es spricht sogar vieles dafür, dass der Anwendungsbereich des BDSG nicht eröffnet ist, wenn eine App zwar vom App-Anbieter angeboten und vom Nutzer heruntergeladen wird, dann aber keine Onlineverbindung mehr aufbaut und auch dem App-Anbieter keine Daten mehr übermittelt. In diesem Falle fehlt es genau genommen an einer datenverarbeitenden Stelle i.S.d. § 1 Abs. 2 Nr. 3 BDSG. Denn der App-Anbieter gäbe im Falle einer App, die autark auf dem Smartphone des Nutzers zu dessen ausschließlich persönlicher Nutzung abläuft und dort lediglich lokal personenbezogene Daten verarbeitet, jede Einflussmöglichkeit ab.[23] Sofern der Anwendungsbereich des BDSG nicht eröffnet ist, findet für den App-Anbieter nicht einmal der Grundsatz der Datensparsamkeit aus § 3a BDSG Anwendung. Gleichwohl wäre der Nutzer der App in seiner informationellen Selbstbestimmung gefährdet. Zum einen könnten Anbieter von Offline-Apps auf eine besonders extensive Datenverarbeitung abzielen. Zum anderen würde insbesondere eine Speicherung von Standort- und sonsti-

19 Z. B. könnten Betreiber sozialer Netzwerke anbieten, gegen eine Gebühr die durch die eigene App empfangenen „fremden" Beacon-IDs zu verarbeiten, mit eigenen Informationen anzureichern und über die eigene App vom Beaconbetreiber vorgegebene Werbung anzuzeigen bzw. Push-Notifications auszulösen. Denkbar ist es sogar, den Beaconbetreibern in Echtzeit zu empfehlen, wann welche Werbeinhalte auf sich im Ladengeschäft befindlichen Bildschirmen angezeigt werden sollten. Wird die Präsenz mehrerer Kunden in der Nähe eines Bildschirms erkannt, wäre es sogar möglich, anhand von vorgegebenen Algorithmen zu berechnen, welche Werbung am erfolgversprechendsten ist.

20 In diesen Fällen wäre die Beacon-ID regelmäßig ein personenbeziehbares Datum, da die Beacon-ID mit der Person bzw. dem Besitzer des Gegenstandes und einem Standort in Verbindung gebracht werden könnte.

21 Vgl. hierzu insgesamt auch Beschluss des Düsseldorfer Kreises vom 4./5. Mai 2011, Datenschutzgerechte Smartphone-Nutzung ermöglichen!

22 So auch *Feldmann*, Mobile Apps: Zivilrecht – Telemedienrecht – Datenschutz, DSRI-Tagungsband 2011, S. 60, der treffend formuliert, dass ein „bloßes Stück Software" ohne Interaktionsmöglichkeiten nicht unter Begriff des Telemediums fällt; *Baumgartner/Ewald*, Apps und Recht RN 148, 149, 154, 203; Orientierungshilfe des Düsseldorfer Kreises zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Stand 16. Juni 2014, Ziffer 1.

23 Vgl. auch *Dammann* in Simitis BDSG, 7. Aufl. 2011, § 3 RN 225. Zu einem anderen Ergebnis könnte man gelangen, wenn man den Begriff der Datennutzung sehr weit auslegen und eine Datennutzung auch dann annehmen würde, wenn zwar weder eine Rückübermittlung von Daten vorgesehen ist noch eine Einflussnahmemöglichkeit auf die Datenverarbeitung besteht, aber eine Offline-App derart mit Regelwerken zur Datenverarbeitung „betankt" wird, dass diese die Handlungsweise des Betroffenen zu Gunsten eines Dritten beeinflussen soll.

gen personenbezogenen Daten durch die App detaillierte Rückschlüsse auf den Nutzer zulassen, sofern Dritte auf die Daten Zugriff nehmen könnten. An dieser Stelle zeigt sich möglicherweise eine Schutzlücke des BDSG. Das Prinzip der Datensparsamkeit und das daraus folgende Prinzip „Privacy by Design" erstreckt sich nicht unmittelbar auf Anbieter von Offline-Apps, sondern auf die für den Einsatz verantwortliche Stelle.[24] Fehlt es jedoch an einer solchen, wird das Prinzip der Datensparsamkeit letztlich ausgehöhlt.

Teilweise wird die Frage aufgeworfen, ob App-Anbieter dem Anwendungsbereich des § 6c BDSG unterliegen.[25] Demnach bestehen bei der Ausgabe mobiler personenbezogener Speicher- und Verarbeitungsmedien für die ausgebende Stelle u. a. besondere Informationspflichten. Dies wäre insbesondere bei Apps ohne Onlineanbindung wünschenswert, um den Nutzer über die Gefahren einer Datenverarbeitung zu informieren, die durch das Herunterladen der App und die darauffolgende autarke Datenverarbeitung ausgelöst wird. Allerdings ist wie bereits gezeigt der Anwendungsbereich des BDSG nicht eröffnet. Zudem stellt die Gesetzesbegründung zu § 3 Abs. 10 BDSG klar, dass unter den Begriff „mobile personenbezogene Speicher- und Verarbeitungsmedien" weder Mobiltelefone noch tragbare Personalcomputer fallen.[26] Zur Begründung wird angeführt, dass der Benutzer die Verarbeitungsvorgänge dieser Geräte auf vielfältige Weise steuern kann.[27] Zwar wird zum einen Unverständnis an dieser engen Sichtweise geäußert.[28] Teilweise wird sogar angenommen, dass Mobiltelefone dann von § 3 Abs. 10 BDSG umfasst sind, sofern diese über Soft- bzw. Hardwarebereiche verfügen, die der Kontrolle des Nutzers entzogen sind.[29] Allerdings ist eine solche Auslegung mit der Gesetzesbegründung nicht vereinbar. Zudem besteht im Hinblick auf Apps regelmäßig die Möglichkeit, den Zugriff auf Standortdienste zu deaktivieren. Obwohl § 6c BDSG geeignet wäre, die informationelle Selbstbestimmung auch bei der Nutzung von Offline-Apps zu schützen, findet die Rechtsvorschrift keine Anwendung.

Im Ergebnis bleibt festzustellen, dass eine personalisierte und standortbezogene Nutzeransprache durch eine Offline-App unter Verwendung von iBeacons datenschutzrechtlich ohne weiteres möglich ist.

4.3.2. Apps mit Onlineanbindung

Sofern ein App-Anbieter bzw. eine dritte Stelle die Datenverarbeitung durch die App auch nach deren Herunterladen beeinflussen kann oder personenbezogene Daten von der App versendet werden, findet das BDSG und regelmäßig auch das TMG[30] Anwendung. Im Hinblick auf die Verarbeitung personenbezogener Daten gilt somit das Verbot mit Erlaubnisvorbehalt aus § 4 Abs. 1 BDSG bzw. § 12 Abs. 1 TMG. Es bedarf daher entweder einer Einwilligung des betroffenen Nutzers oder einer Rechtsvorschrift, welche die Datenverarbeitung erlaubt. Als Rechtsvorschriften, die eine Datenverarbeitung legitimieren können, kommen für Inhaltsdaten etwa § 28 Abs. 1 S. 1 Nr. 1 BDSG und im Bereich der Telemedien für Bestandsdaten § 14 Abs. 1 TMG sowie für Nutzungsdaten § 15 Abs. 1 TMG in Betracht.[31] Im Hinblick auf die Bildung pseudonymisierter Nutzerprofile ist zudem an die privilegierende Rechtsvorschrift des § 15 Abs. 3 TMG zu denken.

Sofern eine Einwilligung im Anwendungsbereich des TMG elektronisch erklärt werden soll, muss diese den Anforderungen des § 13 Abs. 2 TMG entsprechen, also bewusst und eindeutig erteilt worden sein sowie protokolliert werden. Der Nutzer muss den Inhalt der Einwilligung zudem jederzeit abrufen und die Einwilligung mit Wirkung für die Zukunft widerrufen können. Schließlich muss eine App, die in den Anwendungsbereich des TMG fällt, den Nutzer in einer Datenschutzerklärung nach § 13 Abs. 1 TMG u. a. über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten informieren und über ein Impressum nach § 5 TMG verfügen. Die dargestellten Rechtsvorschriften des BDSG und des TMG bieten grundsätzlich einen ausreichenden Schutz vor unzulässiger Datenerhebung und übermäßiger Datenverarbeitung. Eine besondere Gefahr besteht jedoch im Hinblick auf die Nutzung von mobilen Standortdaten zur Nutzerprofilbildung.

Zwar bedarf das Erstellen von Nutzerprofilen und deren Zusammenführung mit Identifikationsmerkmalen grundsätzlich einer Einwilligung des betroffenen Nutzers. Die Art. 29 Datenschutzgruppe fordert sogar über das gesetzlich vorgeschriebene Maß hinaus weitere Mindestvoraussetzungen, die bei der Verarbeitung von mobilen Standortdaten einzuhalten sind.[32] So muss eine Einwilligung nicht nur freiwillig, für den konkreten Fall und in Kenntnis der Sachlage erfolgen, sondern dürfe auch nicht an die Nutzung der App gekoppelt und nicht über Allgemeine Geschäftsbedingungen eingeholt werden. Insgesamt sei ein ausdrückliches Opt-In in die Datenverarbeitung zu fordern. Auch sei es wichtig, die Aktivierung der Standortlokalisierung dauerhaft anzuzeigen – etwa durch die Einblendung entsprechender Symbole. Empfehlenswert sei es zudem, eine einmal eingeholte Einwilligung nach einem Jahr erneut abzufragen bzw. dem Nutzer die Möglichkeit zu geben, diese leicht zu widerrufen.[33] Trotz der Empfehlung der Art. 29 Gruppe verbleibt mangels einer klaren gesetzlichen Regelung zur Verarbeitung mobiler Standortdaten aber die Gefahr, dass App-Betreiber versuchen werden, Einwilligungen in extensive Datenverarbeitungen z. B. über Allgemeine Geschäftsbedingungen einzuholen. Hier könnte eine entsprechende gesetzliche Regelung zur Verarbeitung mobiler Standortdaten Abhilfe schaffen.

Es ist auch denkbar, dass App-Anbieter versuchen werden, Nutzerprofile unter der Privilegierung des § 15 Abs. 3 TMG zu erstellen. Solche pseudonymisierten Nutzungsprofile dürfen nach § 15 Abs. 3 S. 3 und § 13 Abs. 4 Nr. 6 TMG keinesfalls mit Daten

24 Vgl. auch *Schulz* in BeckOK DatenSR, 9. Edition, § 3a RN 22; *Dammann* in Simitis BDSG, § 3a RN 25, 26.

25 *von der Heide*, i-Beacon – Technischer Hintergrund und datenschutzrechtliche Aspekte, PinG 2014, S. 165, 166.

26 BT-Drs. 14/5793Zu III 2, Seite 60.

27 BT-Drs. 14/5793Zu VI 3, Seite 63.

28 *Schild* in BeckOK DatenSR, § 3 RN 155.

29 *Scholz* in Simitis BDSG, § 3 RN 277.

30 Es sei denn, bei der App handelt es sich ausnahmsweise um einen reinen Telekommunikationsdienst oder ein Rundfunkangebot.

31 Einen guten Überblick hierzu geben *Sachs/Meder*, Datenschutzrechtliche Anforderungen an App-Anbieter – Prüfungen am Beispiel von Android-Apps, ZD 2013, S. 306; Orientierungshilfe des Düsseldorfer Kreises zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Ziffer 4; *Baumgartner/Ewald*, Apps und Recht, RN 243 ff.

32 *Art. 29 Gruppe*, WP 185 Opinion 13/2011 on Geolocation services on smart mobile devices, Ziffer 5.2.1. und 6.3.

33 Weniger restriktiv scheint hingegen die Orientierungshilfe des Düsseldorfer Kreises zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Ziffer 6.7. zu sein, obwohl auch hier eine Freigabe des Zugriffs auf Standortdaten vom Nutzer gefordert wird, selbst wenn eine Einwilligung im konkreten Fall nicht erforderlich wäre.

über den Träger des Pseudonyms zusammengeführt werden. Aufsichtsbehörden gehen jedoch davon aus, dass Standortdaten „zumeist" einer bestimmbaren Person zugeordnet werden können. Dies sei etwa dann der Fall, wenn kumulierte Standortdaten – etwa der Weg vom Wohnsitz zur Arbeitsstelle – betroffen sind.[34] Da es sich bei der Standortlokalisierung mittels iBeacons jedoch regelmäßig um eine Innenraumlokalisierung handelt, werden selbst kumulierte Standortdaten an sich nicht immer einen Rückschluss auf eine einzelne Person zulassen,[35] sofern diese von Identifikationsmerkmalen getrennt gespeichert werden. Auch an dieser Stelle ist eine Klarstellung des Gesetzgebers zum Umgang mit mobilen Standortdaten wünschenswert.

Schließlich könnten App-Betreiber versuchen, einzelne Datenverarbeitungen dem Anwendungsbereich des BDSG und des TMG durch Anonymisierung zu entziehen. So könnten die aktuell erfassten Einzelstandorte anonym und nicht miteinander verknüpft an einen Unternehmensserver übermittelt werden, um dort Heatmaps zu erstellen. Nicht ausgeschlossen ist auch, dass App-Betreiber versuchen werden, auf dem Smartphone personenbezogene Bewegungsprofile zu bilden, um diese im Anschluss zu anonymisieren und ohne Widerspruchsmöglichkeit des Nutzers zu übertragen. Letztere Möglichkeit begegnet jedoch datenschutzrechtlichen Bedenken. So verstieße eine vorbereitende, personenbezogene Speicherung von Standortdaten, die ausschließlich den Zweck verfolgt, lokale Profile zu bilden, die später anonymisiert übermittelt werden sollen, gegen das datenschutzrechtliche Erforderlichkeitsprinzip und den Zweckbindungsgrundsatz. Die Bildung von Heatmaps anhand von anonymisierten Einzeldaten erscheint hingegen durchaus denkbar, da die Datenverarbeitung insoweit dem Anwendungsbereich des BDSG und des TMG entzogen werden könnte.

5. Fazit

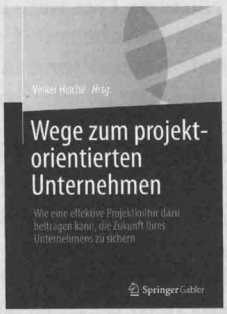
Die Frage, ob ein Unternehmen stationäre Beacons in datenschutzrechtlich zulässiger Weise einsetzt oder nicht, hängt ausschließlich von der durch die App ausgelösten Datenverarbeitung ab. Hier bestehen teilweise Schutzlücken im Hinblick auf reine Offline-Apps. Selbst im Hinblick auf Online-Apps bestehen Regelungslücken in Bezug auf die Verarbeitung mobiler Standortdaten. Obwohl die Beacon-Technologie an sich grundsätzlich datensparsam ausgestaltet ist und insbesondere im Bereich der Innenraumortung im Gegensatz zu anderen Technologien[36] nicht mit einer Übermittlung personenbezogener Daten einhergeht, bestehen durch die mit der Beacon-Technologie verbundene Appgestaltung vielfältige Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen. Trackingmöglichkeiten, die bisher nur im Rahmen des Online-Shoppings denkbar waren, sind nun auch beim Besuch im Ladengeschäft vor Ort möglich. Aufsichtsbehörden werden künftig immer mehr Kompetenzen im Hinblick auf App-Prüfungen benötigen. Insgesamt werden auch betriebliche Datenschutzbeauftragte Apps häufiger bewerten und im Rahmen der Nutzung von Standortdaten ggf. einer datenschutzrechtlichen Vorabkontrolle unterziehen müssen. Es kommt daher darauf an, die mit den Apps verknüpften Technologien zu verstehen. Auch vor dem Hintergrund eines immer weiter vernetzten „Internet der Dinge" hat die Beacontechnologie das Potential, unseren Alltag in einem Maße zu verändern, wie dies Soziale Netzwerke vor einigen Jahren getan haben.

34 Orientierungshilfe des Düsseldorfer Kreises zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Ziffer 2.2.

35 Weil hier Orte wie Wohnsitz oder Arbeitsstelle regelmäßig nicht offenbart werden. Es muss aber im Einzelfall genau geprüft werden, ob z. B. anhand einer vorhandenen Videoüberwachung oder auf Grund des Einsatzes von Kunden- oder gar EC-Karten nicht doch theoretisch ein Personenbezug herstellbar ist – etwa weil neben den Standortdaten auch die Zeitpunkte des jeweiligen Aufenthaltes übermittelt werden.

36 Z. B. im Gegensatz zur Wifi-Ortung, die auf das Aussenden der individuellen MAC-Adresse des Smartphones angewiesen ist – vgl. hierzu: *Art. 29 Gruppe*, WP 185 Opinion 13/2011 on Geolocation services on smart mobile devices, Ziffer 2.3.1.

Mehr Innovationen und Erfolg durch eine effektive Projektkultur im Unternehmen
↗
springer-gabler.de



Volker Hische
Wege zum projektorientierten Unternehmen
Wie eine effektive Projektkultur die Zukunft Ihres Unternehmens sichert
2012. XII, 268 S. mit 78 Abb.
Geb. € (D) 39,95
ISBN 978-3-8349-3244-0

Um als Unternehmen die Zukunft erfolgreich zu gestalten, brauchen Unternehmen Innovationen. Innovation entstehen aus erfolgreicher Projektarbeit. Erfolgreiche Projektarbeit braucht gemeinsame Spielregeln. Effektive Spielregeln ergeben sich aus dem Ansatz der projektorientierten Organisation. Dieses Buch beschreibt anhand von Praxisbeispielen, was eine projektorientierte Organisation auszeichnet und wie sie sich einführen lässt. Ein sehr nützliches Buch, das konkret die Schwierigkeiten und Stolpersteine, aber auch die Vorteile und Anwendungserfolge bei der Einführung einer projektorientierten Kultur und Organisation beschreibt.

Einfach bestellen:
SpringerDE-service@springer.com
Telefon +49 (0)6221 / 345 – 4301
Springer Gabler

Änderungen vorbehalten. Erhältlich im Buchhandel oder beim Verlag.