DÜSSELDORFER KREIS
Aufsichtsbehörden für
den Datenschutz im
nicht-öffentlichen Bereich

Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter

Die Orientierungshilfe richtet sich an Entwickler und Anbieter mobiler Applikationen (Apps). Sie zeigt datenschutzrechtliche und technische Anforderungen auf und macht diese anhand plakativer Beispiele verständlich.

Redaktionelle Bearbeitung:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27, 91522 Ansbach

E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de
Tel.: 0981/53-1300
Fax: 0981/53-5300

Hinweis:
Dieser Orientierungshilfe wurde im Umlaufverfahren vom Düsseldorfer Kreis am 16. Juni 2014 zugestimmt.

Stand: 16. Juni 2014

Inhaltsverzeichnis

1. Zielgruppe und Ziel

Zielgruppe dieser Orientierungshilfe sind Entwickler und Anbieter[1] mobiler Applikationen (Apps) im nicht-öffentlichen Bereich[2], die als Telemediendienst zu qualifizieren sind und auf die ganz oder auf Teil-Dienste der App die datenschutzrechtlichen Regelungen der §§ 11 ff. des Telemediengesetzes (TMG) vollumfänglich Anwendung finden.[3] Nicht im Fokus dieser Orientierungshilfe stehen somit App-Angebote, deren Dienst ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht bzw. Rundfunk (i.S.d. § 2 des Rundfunkstaatsvertrages-RStV) darstellen oder die offline[4] betrieben werden. Auch werden Apps, welche Teil des jeweiligen Betriebssystems sind und Besonderheiten von Apps[5], die für spezielle Endgeräte wie z. B. Smart-TVs oder Smart-Watches entwickelt und angeboten werden, nicht im Rahmen dieses Dokumentes berücksichtigt.[6] Die Orientierungshilfe bezieht sich ausschließlich auf (Online-) Apps für Smartphones und Tablets.

App-Entwickler sollten bereits in der Entstehungs- und Entwicklungsphase einer App die datenschutzrechtlichen Vorgaben kennen und durch datenschutzgerechte Gestaltung („privacy by design“) sowie datenschutzfreundliche Voreinstellungen („privacy by default“) dafür Sorge tragen, dass die App später ohne datenschutzrechtliche Mängel angeboten werden kann. Soweit der Entwickler in der Anwendungsphase[7] (z.B. im Rahmen von Fehlermeldungen) personenbezogene Daten erhält und verwendet[8], ist er selbst Adressat datenschutzrechtlicher Anforderungen und muss diese kennen und umsetzen.

Wird eine App nicht datenschutzkonform angeboten, weil unzulässig personenbezogene Daten erhoben und verwendet werden, können insbesondere den **App-Anbieter** als verantwortliche Stelle aufsichtsrechtliche Maßnahmen oder Bußgelder treffen.

---

[1] Die Trennung wird vorgenommen, da für die Entwicklung einer App häufig externe Dienstleister beauftragt werden. Soweit die App vom App-Anbieter selbst entwickelt wird, fallen beide Eigenschaften zusammen, so dass von diesem die vorgestellten Regelungen sowohl in der Entwicklung als auch während des Produktivbetriebes zu beachten sind.

[2] Die Orientierungshilfe findet nur für nicht-öffentliche Stellen direkte Anwendung. In Kapitel 9.4 wird ein knapper Hinweis für öffentliche Stellen gegeben.

[3] Die § 11 ff. TMG finden vollumfänglich Anwendung, soweit es sich um einen Telemediendienst handelt, der nicht überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht (vgl. § 11 Abs. 3 TMG).

[4] Entscheidend dabei ist nicht der Verwendungszweck der App, sondern ob tatsächlich Daten übermittelt werden. Dies ist für den Nutzer allerdings nur schwer zu erkennen.

[5] Die in dieser Orientierungshilfe dargestellten Grundsätze gelten jedoch auch für solche Apps, soweit diese als Telemedien gelten.

[6] Somit gilt die Orientierungshilfe grundsätzlich direkt für alle Apps, die
- keinen Messenger-Dienst oder VoIP-Dienst anbieten,
- keinen Rundfunk anbieten (Radio, TV) und
- eine Online-Verbindung bei der Nutzung benötigen (vgl. Fn.4).

[7] Unter Anwendungsphase ist der Produktivbetrieb der App zu verstehen.

[8] Der Begriff „Verwenden“ personenbezogener Daten wird in den § 11 ff. TMG verwendet. Er umfasst das Verarbeiten und Nutzen personenbezogener Daten i.S.d. § 3 Abs. 4 und Abs. 5 BDSG. Entsprechend wird dieser Begriff vorliegend einheitlich (sowohl im Anwendungsbereich des BDSG als auch des TMG) verwendet.

Um dieser Verantwortung gerecht zu werden, muss bei der Entwicklung und bei dem Angebot einer App beachtet werden, dass die Erhebung und Verwendung personenbezogener Daten datenschutzrechtlichen Regelungen unterliegt. Um aufzuzeigen, in welchem datenschutzrechtlichen Rahmen sich App-Anbieter und ggf. auch App-Entwickler bewegen, geht die Orientierungshilfe nach einer kurzen Darstellung der Grundlagen auf den anzuwendenden Rechtsrahmen (Kapitel 2), die Verantwortlichkeiten (Kapitel 3), auf die Erlaubnistatbestände und die allgemein zu beachtenden Datenschutzgrundsätze (Kapitel 4) sowie die Nutzerrechte (Kapitel 5) ein. Im Anschluss daran werden grundlegende Anforderungen an den technischen Datenschutz (Kapitel 6) und die Problematik eines erhöhten Schutzbedarfs bei dem Umgang mit besonderen Arten personenbezogener Daten (Kapitel 7) besprochen. Zuletzt werden die mit dieser Orientierungshilfe angesprochenen Akteure auf die Konsequenzen eines unzulässigen Datenumgangs und auf Besonderheiten hingewiesen (Kapitel 8 und 9).

2. Anwendbarkeit deutschen Datenschutzrechts

2.1. Räumlicher Anwendungsbereich

App-Anbieter und weitere datenverarbeitende Stellen müssen sich gem. § 1 Bundesdatenschutzgesetz (BDSG) an die deutschen Datenschutzgesetze halten, soweit diese ihren Sitz bzw. eine datenverarbeitende Niederlassung in der Bundesrepublik Deutschland (BRD) haben. Befindet sich weder der Sitz des App-Anbieters noch eine datenverarbeitende Niederlassung desselben innerhalb der BRD, ist danach zu unterscheiden, ob sich der Sitz bzw. eine datenverarbeitende Niederlassung innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR, umfasst zusätzlich zu den Mitgliedsstaaten noch Island, Norwegen, Liechtenstein) befindet. Trifft dies zu, ist das jeweils nationale Datenschutzrecht des Mitgliedstaats oder Vertragsstaats anzuwenden. Liegen der Sitz und etwaige Niederlassungen ausschließlich außerhalb der EU bzw. des EWR, ist der Anwendungsbereich des deutschen Datenschutzrechts eröffnet, wenn personenbezogene Daten im Inland (BRD) mittels der App erhoben und verwendet werden.[9]

Beispiele:

- Ein App-Anbieter mit Sitz/Niederlassung in München erhebt mittels seiner App personenbezogene Daten: Deutsches Datenschutzrecht findet Anwendung.
- Ein amerikanisches Unternehmen mit einer für die Datenverarbeitung relevanten Niederlassung in Irland (und nicht in Deutschland) erhebt mittels seiner App personenbezogene Daten bei Bewohnern Deutschlands: Irisches Datenschutzrecht findet Anwendung.
- Ein Unternehmen mit Sitz in China ohne weitere Niederlassung in Europa erhebt mittels einer App personenbezogene Daten bei Bewohnern Deutschlands: Deutsches Datenschutzrecht findet Anwendung.

[9] Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten der Artikel 29 Gruppe, WP 202, Ziffer 3.1 , vgl. auch Stellungnahme 8/2010 zum anwendbaren Recht der Artikel 29 Gruppe, WP 179, Kapitel III.4 und IV.2

2.2. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich des Datenschutzrechts ist eröffnet, soweit es um den Umgang mit personenbezogenen Daten geht. Ein personenbezogenes Datum i.S.d. § 3 Abs. 1 BDSG ist gegeben, soweit eine Information, direkt oder auch nur mit Hilfe von Zusatzwissen (Bestimmbarkeit), auf eine Person zurückgeführt werden kann. Die Bestimmbarkeit einer Person im Zusammenhang mit mobilen Geräten und Apps ist insbesondere bei folgenden Informationen zu bejahen[10]:

- **IP-Adresse** des Nutzers, welche in der Regel als personenbezogenes Datum gilt. Dieser bedarf es auch bei Apps notwendigerweise für die Internetkommunikation.
- Eindeutige **Geräte- und Kartenkennungen**, die dauerhaft mit dem Gerät bzw. der Karte verbunden sind, können regelmäßig durch verschiedene Stellen einer Person zugeordnet werden. So werden die Kennungen mitunter von den Netzbetreibern gemeinsam mit dem Namen etc. einer Person gespeichert oder die Kennungen in Verbindung mit einer Registrierung der registrierten Person zugeordnet.
  Die bekanntesten Kennungen sind die:
  - IMEI: International Mobile Equipment Identity (=Gerätenummer)
  - UDID: Unique Device ID (=Gerätenummer eines iOS-Gerätes)
  - IMSI: International Mobile Subscriber Identity (=Kartennummer)
  - MAC-Adresse: Media AccessControl-Adresse (=Hardware-Adresse eines Netzwerkadapters)
  - MSISDN: Mobile Subscriber ISDN-Number (=Mobilfunknummer)
- **Name des Telefons**, soweit ein Nutzer sein Telefon unter Verwendung des eigenen Namens benennt.
- **Standortdaten** können zumeist ebenfalls einer bestimmbaren Person zugeordnet werden, da oftmals zu dem Standortdatum ein weiteres Datum, wie z.B. die IP-Adresse oder eine anderweitige eindeutige Kennung mitgesandt wird. Darüber hinaus kann eine Person bei Kumulierung mehrerer Standortdaten aufgrund eines Bewegungsprofils identifizierbar sein, wenn hierdurch ein bestimmtes, individuelles Bewegungsverhalten erfasst wird (z.B. Weg zur Arbeit).
- **Audiodaten** mit Stimmaufnahmen stellen ebenfalls personenbezogene Daten dar, da durch einen Stimmabgleich die Person, der die Audiodaten zuzuordnen sind, eindeutig identifiziert werden kann. Dies gilt entsprechend für **Foto- und Filmaufnahmen** einer Person.

[10] Vgl. hierzu auch: Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten der Artikel 29 Gruppe, WP 202, Ziffer 3.1

- **Daten für biometrische Erkennungsverfahren** wie der Fingerabdruck, die Iris und die Gesichtsgeometrie sollen gerade dazu dienen, eine einzelne Person eindeutig zu identifizieren und stellen somit personenbezogene Daten dar.

- **Informationen über die App-Nutzung**: Welche App wurde z.B. wann durch den Nutzer genutzt.

Neben diesen, besonders hervorgehobenen personenbezogenen Daten, können zahlreiche weitere Informationen, die auf dem mobilen Gerät gespeichert sind, von diesem generiert oder durch den Nutzer eingegeben werden, unter die o.g. Definition der personenbezogenen Daten fallen. Hierzu gehören bspw. Kontaktdaten im Adressbuch, Kalendereinträge, Registrierungsdaten, Anruflisten, Nachrichten (z.B. SMS, E-Mails), Namen, Adressen und Kontoverbindungsdaten.

3. Verantwortlichkeiten

Adressat datenschutzrechtlicher Vorgaben für den Datenumgang ist vorliegend[11] grundsätzlich der App-Anbieter, als diejenige Stelle, die die personenbezogenen Daten für sich selbst erhebt (vgl. § 3 Abs. 7 HS. 1 BDSG). Dies gilt auch, soweit der App-Anbieter seine App nicht selbst entwickelt hat, sondern diese „nur" anbietet. Auch in diesem Fall obliegt es dem App-Anbieter als verantwortliche Stelle, sich über den Datenumgang, welcher mittels der App stattfindet, zu informieren und die Einhaltung der einschlägigen datenschutzrechtlichen Anforderungen zu überprüfen. Bei einer Überprüfung des App-Angebotes durch die Aufsichtsbehörde kann nicht auf den App-Entwickler verwiesen werden. Auch für den Nutzer der App ist der App-Anbieter die Anlaufstelle für seine Nutzerrechte (z. B. Auskunft, Löschung etc.).

Auch wenn die personenbezogenen Daten von einer Stelle im Auftrag des App-Anbieters erhoben und verwendet werden, ist der App-Anbieter weiterhin als verantwortliche Stelle Adressat der datenschutzrechtlichen Anforderungen (vgl. § 3 Abs. 7 HS. 2 BDSG). Durch die Vergabe der Datenverarbeitung an einen Dienstleister wird er zum Auftraggeber, der Dienstleister wird Auftragnehmer. Bei der Auftragsdatenverarbeitung ergeben sich für den App-Anbieter vielfältige Sorgfalts- und Kontrollverpflichtungen, welche in § 11 BDSG dargestellt und geregelt sind. Die Erfüllung der Vorgaben zur Auftragsdatenverarbeitung erfordert zum einen eine geeignete und rechtssichere Ausgestaltung der Verträge mit dem Auftragnehmer. Weiterhin ergeben sich für den Auftraggeber fortwährende Kontrollpflichten. So soll er z.B. durch das Führen von Protokollen über Vor-Ort-Kontrollen beim Auftragnehmer jederzeit die Ausübung der ihm obliegenden Sorgfalts- und Kontrollverpflichtungen

[11] Die vorliegende Orientierungshilfe richtet sich ausschließlich an App-Anbieter und App-Entwickler, nicht jedoch an weitere mögliche Akteure wie z.B. Werbenetzwerkbetreiber und Nutzer.

nachweisen können. Unter Umständen können geeignete Zertifizierungen bzw. Gütesiegel eine Vor-Ort-Kontrolle ersetzen.[12]
Der Auftragnehmer ist hingegen verpflichtet, streng weisungsgebunden zu agieren und die personenbezogenen Daten einzig für die Zwecke der verantwortlichen Stelle zu erheben und zu verwenden.[13] Obwohl er verpflichtet ist, die Weisungen des Auftraggebers zu befolgen, obliegt es ihm, den Auftraggeber unverzüglich darauf hinzuweisen, soweit eine Weisung gegen Datenschutzbestimmungen verstößt.

Beispiele:

- Wird die App auftragsgemäß über den Server eines Dienstleisters betrieben und werden die personenbezogenen Daten dort gespeichert, so ist der App-Anbieter als Auftraggeber die datenschutzrechtlich verantwortliche Stelle.
- Wird ein Verfahren zur Reichweitenmessung eingesetzt und die Auswertung durch einen Dienstleister durchgeführt, ist der App-Anbieter als Auftraggeber die datenschutzrechtlich verantwortliche Stelle.

Auch wenn Dienstleister für den technischen Betrieb einer App eingesetzt werden, konkret Cloud-Anbieter, welche unentgeltlich oder gegen Bezahlung Datenverarbeitungsressourcen wie Speicherplatz oder Rechenleistung bereitstellen, trifft ebenfalls der datenschutzrechtliche Sachverhalt der Auftragsdatenverarbeitung zu.

Bei Cloud-Diensten sitzt der Auftragnehmer häufig nicht im Inland und nicht innerhalb eines Mitgliedstaats der EU oder eines Vertragsstaats des EWR und/oder findet die Datenverarbeitung ganz oder teilweise im außereuropäischen Raum statt, beispielsweise in den USA oder in Asien. Somit liegt regelmäßig eine Datenübermittlung[14] in Drittstaaten vor. Zu den Pflichten bei der Auftragsdatenverarbeitung kommen dann weitere Anforderungen hinzu. So muss z.B. im Rahmen der Vertragsgestaltung die Zulässigkeit der Datenverarbeitung und die Zweckbindung der verarbeiteten Daten explizit thematisiert und definiert werden.[15]

[12] Vgl. Orientierungshilfe „Cloud-Computing der Arbeitsgruppen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26.09.2011, Kapitel 3.2. Abrufbar unter https://www.datenschutz.rlp.de/downloads/oh/ak_oh_cloudcomputing.pdf

[13] Weitere Informationen zur Auftragsdatenverarbeitung: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Auftragsdatenverarbeitung.pdf

[14] Im Gegensatz zum innereuropäischen Datenumgang liegt ein Übermittlung an einen Dritten vor, vgl. § 3 Abs. 8 S. 1 BDSG. Neben der datenschutzrechtlichen Erlaubnis zur Übermittlung bedarf es in einer zweiten Stufe eines angemessenen Datenschutzniveaus.

[15] Weitere Informationen zum Thema Nutzung von Cloud-Diensten und der hierbei entstehenden Verantwortung und Kontrolle durch den Auftraggeber liefert die "Orientierungshilfe Cloud Computing" der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, erhältlich unter http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf (Version 01, 29.09.2011)

Beispiel:
Die Daten, welche über die Endgeräte der App-Nutzer erhoben werden, werden je nachdem an welchem Ort Speicherplatz vorhanden ist, in Frankreich, in den USA oder auf Indonesien gespeichert.

Neben dem App-Anbieter kann es weitere Verantwortlichkeiten geben:

- Sobald ein App-Entwickler rechtswidrig agiert, indem er z.B. entgegen den Weisungen des Auftraggebers personenbezogene Daten erhebt und verwendet bzw. über den Umfang einer Weisung oder eines (Entwickler-) Auftrages hinaus datenverarbeitend tätig wird oder personenbezogene Daten ohne Erlaubnis und somit unzulässigerweise eigenständig erhebt und verwendet, kann der App-Entwickler selbst zu einer verantwortlichen Stelle werden.
  Der App-Entwickler als Auftragnehmer ist streng weisungsgebunden und muss den Auftraggeber auf Weisungen, die gegen datenschutzrechtliche Bestimmungen verstoßen hinweisen, während der Auftraggeber den Auftragnehmer kontrollieren muss, um einen weisungswidrigen Datenumgang zu verhindern (vgl. auch oben).
  Der App-Entwickler als verantwortliche Stelle ist an den Grundsatz des Verbots mit Erlaubnisvorbehalt gebunden und bedarf für jegliche Datenerhebung und -verwendung einer Erlaubnis.

  Beispiel:
  Eine App sendet bei einem Fehler automatisiert eine entsprechende Meldung an den App-Entwickler, ohne dass der App-Anbieter eine Fehlerkontrolle angeordnet bzw. von einer solchen Kenntnis hat. Da die Datenerhebung und -verwendung außerhalb eines Auftrages stattfindet und keine Rechtsgrundlage für die Erhebung und Verwendung der personenbezogenen Daten (zumindest die IP-Adresse wird übertragen) ersichtlich ist, handelt der App-Entwickler widerrechtlich.

- Der Betreiber eines App-Stores kann die für die Datenverarbeitung verantwortliche Stelle sein, soweit er (zusätzlich zum Anbieter der App) zu eigenen Zwecken personenbezogene Daten des Endnutzers erhebt oder verwendet und den Umfang der Datenerhebung und -verwendung festlegt.

  Beispiele:
  - Ein Nutzer muss sich bei einem App-Store anmelden, um hierüber eine bestimmte App herunterladen zu können. Die bei dem App-Store angegebenen Daten werden von diesem zu (eigenen) Abrechnungszwecken erhoben und verwendet.

- Verwaltung von Abonnenten einer Zeitungs-App durch den App-Store, ohne dass der App-Betreiber die Abonnentendaten mitgeteilt bekommt bzw. Zugriff darauf nehmen kann. Der App-Store ist für die Verwaltung der Abonnenten verantwortliche Stelle.

4. Erlaubnistatbestände und Datenschutzgrundsätze

4.1. Erlaubnistatbestände

Im Datenschutzrecht gilt der Grundsatz des Verbotes mit Erlaubnisvorbehalt. Dies bedeutet, dass die Erhebung und Verwendung personenbezogener Daten grundsätzlich verboten ist, es sei denn, es existiert eine Erlaubnis dazu. Eine solche Erlaubnis kann sich einerseits aus einer Rechtsvorschrift oder aus einer Einwilligung[16] des Nutzers bzw. der betroffenen Person ergeben.

Während das BDSG als allgemeines Datenschutzgesetz gilt, sind u.a. die datenschutzrechtlichen Regelungen des TMG (§§ 11 ff. TMG) bereichsspezifische Rechtsvorschriften, welche den allgemeinen Datenschutzgesetzen vorgehen. So finden die Vorschriften des TMG immer dann Anwendung, wenn es um den Datenumgang auf der Diensteebene geht, d.h. bei einem Umgang mit Daten, die zur Bereitstellung des Dienstes erhoben und verwendet werden. Im Fokus sind einerseits die Bestandsdaten (vgl. § 14 TMG) und andererseits die Nutzungsdaten (vgl. § 15 TMG). Hiervon zu unterscheiden sind die Inhaltsdaten, also u. a. die Daten, die durch die App beim Anwender abgefragt werden – für diese Daten gelten in der Regel die allgemeinen Datenschutzgesetze (im nicht-öffentlichen Bereich das BDSG).
Soweit personenbezogene Daten zur Bereitstellung des Telemedienangebots erhoben und verwendet werden sollen, bedarf es entweder einer Erlaubnis dazu in einer Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht oder einer Einwilligung des Nutzers, um die personenbezogenen Daten zulässigerweise erheben und verwenden zu können (vgl. § 12 Abs. 1 TMG).

Auf die im vorliegenden Kontext relevanten Erlaubnisse und Anforderungen an eine wirksame Einwilligung wird im Folgenden eingegangen:

4.1.1. Erlaubnisse aus dem TMG

Die datenschutzrechtlichen Regelungen des TMG finden sich in den §§ 11 ff.. In diesen Regelungen wird die Erhebung und Verwendung der Bestands- und Nutzungsdaten sowohl durch öffentliche als auch durch nicht-öffentliche Stellen (§ 1 Abs. 1 S. 2 TMG) behandelt.[17]

[16] Soweit eine solche in Betracht kommt, vgl. Kapitel 4.1.3
[17] Im Gegensatz dazu muss auf der Inhaltsebene zwischen dem öffentlichen und dem nicht-öffentlichen Bereich unterschieden werden (vgl. Kapitel 4.1.2).

4.1.1.1. Bestandsdaten

Gem. **§ 14 TMG** darf ein Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Welche personenbezogenen Daten konkret für diese Zwecke erforderlich sind, wird durch den jeweiligen Nutzungsvertrag bestimmt, der zwischen dem Diensteanbieter und dem Nutzer abgeschlossen wird. Zu den Bestandsdaten können insbesondere Name, Anschrift, Rufnummer, Registrierungsdaten und Zahlungsdaten zählen.

Nicht unter die Bestandsdaten sind die personenbezogenen Daten zu fassen, welche zwar über eine App erhoben werden, jedoch nicht zur Nutzung des Telemediums „App“ erforderlich sind, sondern für weitere, außerhalb des Telemediendienstes liegende Zwecke erhoben und verwendet werden (vgl. dazu unter Kapitel 4.1.2).

Beispiele:

- App eines sozialen Netzwerks oder Online-Portals:
  Die Zulässigkeit der Erhebung und Verwendung der bei der Registrierung angegebenen Daten ist nach dem TMG zu bewerten (= Bestandsdaten).
- Bestellung eines Buches bei einem Online-Versandhaus über die Versandhaus-App: Die für die Abwicklung des Kaufvertrags und die Lieferung des bestellten Buches erforderlichen personenbezogenen Daten sind als sogenannte Inhaltsdaten unter die Vorgaben des BDSG zu fassen. Der Telemediendienst an sich kann grundsätzlich auch ohne Vornahme einer Bestellung und Angabe der Adress- und Zahlungsdaten genutzt werden.

4.1.1.2. Nutzungsdaten

4.1.1.2.1. Inanspruchnahme des Dienstes

Als Nutzungsdaten werden gem. **§ 15 Abs. 1 TMG** hingegen diejenigen personenbezogenen Daten bezeichnet, die erforderlich sind, um die Inanspruchnahme des Dienstes zu ermöglichen. Das Gesetz zählt dabei

- Merkmale zur Identifikation des Nutzers,
- Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
- Angaben über die vom Nutzer in Anspruch genommenen Telemedien auf.

Bei dieser Aufzählung handelt es sich nicht um eine abschließende Aufzählung. Zu den Nutzungsdaten zählen somit alle personenbezogenen Daten, welche notwendigerweise zur Nutzung der App durch den Diensteanbieter erhoben und verwendet werden müssen, wie z.B. die IP-Adresse oder – soweit im Einzelfall erforderlich - eindeutige Kennnummern oder der Standort. Für die Erbringung des Dienstes ist die Erhebung und Verwendung dieser Nutzungsdaten zulässig.

Beispiel:
Bedarf es für das Funktionieren der App des aktuellen Standortes, z.B. um die Wegstrecke zu einer angegebenen Adresse berechnen zu können, so darf das Standortdatum für diesen konkreten Zweck erhoben und verwendet werden.

4.1.1.2.2. Nutzungsprofil unter Pseudonym

§ 15 Abs. 3 TMG gestattet dem Diensteanbieter die Erstellung von Nutzungsprofilen auf der Basis von Nutzungsdaten für Zwecke der Werbung, der Marktforschung und zur bedarfsgerechten Gestaltung von Telemedien unter Pseudonym, soweit der Nutzer nicht widerspricht.[18]

Die Regelungen des § 15 Abs. 3 TMG berechtigen nur den Diensteanbieter selbst oder seine Auftragnehmer[19] zur Erstellung pseudonymisierter Nutzerprofile zu Werbezwecken. Eine Verwendung von Nutzungsdaten durch Dritte kann nicht auf diese Regelungen gestützt werden. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen jedoch anonymisierte Nutzungsdaten übermittelt werden (§ 15 Abs. 5 S. 3 TMG).

Der Nutzer muss vom Diensteanbieter auf die Erstellung eines solchen Nutzungsprofils und die Möglichkeit dieser zu widersprechen hingewiesen werden. Dies muss zumindest im Rahmen der Datenschutzerklärung (vgl. Kapitel 5.2) geschehen.
Eindeutige Geräte- und Kartenkennungen wie die IMEI-Nummer (vgl. Kapitel 2.2) oder auch die IP-Adresse stellen kein Pseudonym dar. Diese Daten dürfen auch nicht in das Nutzungsprofil einfließen, da die Zusammenführung pseudonymer Nutzungsprofile mit Daten über den Träger des Pseudonyms unzulässig ist (Verstoß gegen § 15 Abs. 3 S. 3 TMG, § 13 Abs. 4 Nr. 6 TMG).

Die Widerspruchsmöglichkeit muss effektiv und angemessen sein. Es sollte daher eine direkte Opt-Out Möglichkeit (Link, Möglichkeit des Auskreuzens) für den Nutzer vorgehalten werden, welche mit möglichst einem Klick aktiviert werden kann. Der bloße Hinweis auf bestimmte Einstellungsmöglichkeiten am Gerät etc. genügt nicht. Stattdessen ist zumindest eine konkrete Anleitung, welche die Vornahme der entsprechenden Einstellungen geräteangepasst Schritt für Schritt darstellt, erforderlich. Auch die Möglichkeit per E-Mail oder postalisch einer Nutzungsprofilerstellung gem. § 15 Abs. 3 TMG zu widersprechen, genügt nicht, da bei einem Widerspruch per E-Mail oder per Post eine Zuordnung aufgrund des Medienbruches im Allgemeinen nicht erfolgen kann. Der Widerspruch gegen

[18] Soweit Art. 5 Abs. 3 der ePrivacy-Richtlinie (2002/58/EG in der Fassung 2009/136/EG) künftig Anwendung findet, ist bei der Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind (u.a. beim Einsatz von Cookies), grundsätzlich eine Einwilligung des Nutzers einzuholen.
[19] Die Einschaltung von Dienstleistern innerhalb der EU/ des EWR ist im Rahmen der Bestimmungen zur Auftragsdatenverarbeitung nach § 11 BDSG unter den dort genannten Voraussetzungen möglich.

die automatisierte Nutzungsprofilbildung unter Pseudonym kann im Regelfall auf technischer Ebene effektiv umgesetzt werden (z.B. Opt-Out-Cookie).[20]

Widerspricht der Betroffene der Profilbildung unter Pseudonym, so sind etwa vorhandene Profildaten zu löschen oder wirksam zu anonymisieren.

Im Zusammenhang mit Apps wird die soeben dargestellte Erlaubnis insbesondere in den folgenden Konstellationen benötigt:

- **Reichweitenmessung**
  Eine Nutzungsprofilerstellung unter Pseudonym gem. § 15 Abs. 3 TMG findet insbesondere zur Reichweitenmessung statt. Mittels einer Reichweitenmessung kann ein App-Anbieter feststellen, in welchem Umfang und auf welche Weise sein App-Angebot genutzt wird.

  Auf die Voraussetzungen für die „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ wurde vom Düsseldorfer Kreis mit Beschluss vom 26./27. November 2009 hingewiesen.[21] Diese Voraussetzungen sind auch bei einem Einsatz solcher Verfahren in Apps entsprechend einzuhalten:
  - Anonymisierung der IP-Adresse (z.B. durch Kürzen oder Überschreiben der IP-Adresse),
  - Vorhalten einer Widerspruchsmöglichkeit und wirksame Umsetzung von Widersprüchen,
  - keine Zusammenführung des Pseudonyms mit Daten über Träger des Pseudonyms,
  - Unterrichtung über Erstellung pseudonymer Nutzungsprofile und über die Widerspruchsmöglichkeit und
  - soweit ein Dienstleister eingesetzt wird, Abschluss eines Auftragsdatenverarbeitungsvertrages gem. § 11 BDSG.

  Soweit etablierte Verfahren zur Reichweitenmessung eingesetzt werden, ist beim Einbau von Standardwiderspruchslösungen über die oben dargestellten Anforderungen an die Angemessenheit einer Widerspruchsmöglichkeit darauf zu achten, dass ein ausgeübter Widerspruch effektiv ist. Dies bedeutet z.B., dass ein im nativen Teil einer App gesetzter Widerspruch auch im Webview einer App, sofern vorhanden, wirksam ist.

- **Werbefinanzierte Apps**
  Viele Apps können gebührenfrei genutzt werden. Allerdings werden diese Angebote vielfach durch eine Verarbeitung von Nutzungsdaten zu Werbezwecken finanziert. Dazu können bei-

[20] Eine solche Möglichkeit zum Opt-out kann technisch jedoch erst innerhalb der App, d.h. nach deren Installation realisiert werden. Dies ist insbesondere dann zu beachten, wenn die Widerspruchsmöglichkeit in der Datenschutzerklärung enthalten ist, welche bereits innerhalb des App-Stores bzw. vor dem Start der App zum Abruf bereitgestellt werden muss (vgl. Kapitel 5.2).

[21] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“, abrufbar unter http://www.lda.bayern.de/onlinepruefung/Beschluss_Reichweitenmessung.pdf

spielsweise auch die jeweiligen Aufenthaltsorte (Standortdaten) der Betroffenen verwendet werden, um ihnen möglichst passgenaue Werbung zu präsentieren. Werden Standortdaten für die Bewerbung erhoben und verwendet, so ist dies nur mit einer gesetzlichen Erlaubnis oder der Einwilligung des Nutzers möglich, soweit es sich bei den Standortdaten um personenbezogene Daten handelt (vgl. Kapitel 2.2).

Soweit die Erhebung und Verwendung der Nutzungsdaten von § 15 Abs. 3 TMG gedeckt ist, ist den Betroffenen ein wirksames Widerspruchsrecht einzuräumen. Signalisiert der Nutzer durch besondere Einstellungen auf seinem Endgerät, dass er eine Verarbeitung seiner Nutzungsdaten für Werbezwecke nicht wünscht, so ist auch[22] diese Erklärung als Widerspruch zu werten und durch den Diensteanbieter zu beachten.

Über die oben beschriebene Erstellung von Nutzungsprofilen unter Pseudonym hinaus ist die Verarbeitung von Nutzungsdaten für Werbezwecke nur gestattet, wenn eine gesetzliche Erlaubnis (§ 15 Abs. 1 TMG) vorliegt oder der Nutzer wirksam in diese Verwendung der Nutzungsdaten für diesen Zweck eingewilligt hat.

4.1.1.3. Verwendung zu Abrechnungszwecken

Soweit die Nutzungsdaten durch den App-Anbieter bzw. App-Store-Betreiber für die Abrechnung kostenpflichtiger App-Angebote verwendet werden, handelt es sich um Abrechnungsdaten, deren Verwendung in den §§ 15 Abs. 2, 4 ff. TMG geregelt wird. Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, wenn es für Zwecke der Abrechnung mit dem Nutzer erforderlich ist.

4.1.2. Erlaubnisse aus dem BDSG

Soweit es nicht um eine Datenerhebung und -verwendung auf der Anwendungsebene, sondern um eine Datenerhebung und -verwendung auf der Inhaltsebene geht, findet grundsätzlich das BDSG Anwendung. Ein Datenumgang auf der Inhaltsebene ist dann anzunehmen, wenn online Daten zwischen dem Nutzer und dem App-Anbieter ausgetauscht werden, um ein Vertrags- oder Leistungsverhältnis zu begründen, das selbst keinen Telemediendienst darstellt („Offline-Vertrag“) oder aber solche, die ein Nutzer selbst in die App eingibt (ausgenommen sind Bestandsdaten, s. unter Kapitel 4.1.1.1). Zwar werden die Daten unter Anwendung des Telemediendienstes „App“ eingegeben und übermittelt, ermöglicht wird jedoch eine Verwendung außerhalb des Anwendungsbereichs des TMG.

[22] Einstellungen auf dem Endgerät können unter Umständen eine wirksame Widerspruchsmöglichkeit darstellen, wenn durch den App-Anbieter die Wirksamkeit des Widerspruchs tatsächlich sichergestellt werden kann. Ist dies nicht möglich, so entbindet die Möglichkeit, bestimmte Einstellungen an den Endgeräten vornehmen zu können, den App-Anbieter nicht von der Verpflichtung eine (zusätzliche) wirksame Widerspruchsmöglichkeit anzubieten.

Bei der Erhebung und Verwendung personenbezogener Daten durch nicht-öffentliche Stellen sind die §§ 27 ff. BDSG anzuwenden. Darüber hinaus können im konkreten Einzelfall spezielle Datenschutzregelungen vorrangig anzuwenden sein.

Beispiele:

- App eines Pizzadienstes, mittels welcher man Speisen und Getränke bestellt:
  Die Zulässigkeit der Erhebung und Verwendung der bei der Bestellung angegebenen Daten durch den Pizzadienst als verantwortliche Stelle ist nach dem BDSG zu bewerten, da die Umsetzung der Bestellung offline ausgeführt wird. Daten über z. B. den Zeitpunkt des Aufrufs der App oder das Klickverhalten in der App sind hingegen Nutzungsdaten im Sinne des TMG.
- Daten, die in ein Kontaktformular eingegeben werden, bspw. um eine Beschwerde anzubringen, soweit sie sich auf ein durch die App ermöglichtes Leistungsverhältnis außerhalb der App beziehen.
- Bei einer Kalender-App zählen die Daten über Termine oder bei einer Adress-App die Namen und Telefonnummern der Freunde zu den Inhaltsdaten.
- Bei der App eines sozialen Netzwerkes zählen die Profildaten eines persönlichen Profils und die Inhalte der Kommunikation zu den Inhaltsdaten.[23]

4.1.3. Einwilligung

Existiert kein gesetzlicher Erlaubnistatbestand, sind die Erhebung und Verwendung personenbezogener Daten dennoch im Regelfall mit einer wirksamen Einwilligung der betroffenen Person bzw. des Nutzers möglich.
Soweit eine Einwilligung in Betracht kommt, sind die Voraussetzungen für eine wirksame Einwilligung - je nachdem ob das das TMG Anwendung findet oder nicht - in § 4a BDSG und § 13 Abs. 2, 3 TMG geregelt.

Während § 4a BDSG neben der Freiwilligkeit und Informiertheit der Einwilligung grundsätzlich die Schriftform fordert, erlaubt und regelt das TMG für Telemedien die Einholung einer elektronischen Einwilligung.

Eine Einwilligung kann gegenüber dem Telemedienanbieter[24] elektronisch erklärt werden, wenn die Vorgaben des § 13 Abs. 2 und Abs. 3 TMG eingehalten werden. Hiernach wird verlangt, dass

[23] Vgl. Orientierungshilfe „Soziale Netzwerke“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14.03.2013, Kapitel 4.2.1

[24] § 4a Abs. 1 S. 3 BDSG sieht eine Ausnahme vom Schriftformerfordernis vor, wenn wegen besonderer Umstände eine andere Form angemessen ist. Solche besonderen Umstände liegen nicht generell dann vor, wenn eine Einwilligung (außerhalb des TMG) bei der Nutzung einer App eingeholt werden soll. Im Regelfall ist deshalb gem. § 126 Abs. 3 i.V.m. § 126a BGB eine qualifizierte elektronische Signatur nach dem Signaturgesetz zu verlangen. Eine entsprechende Anwendung des § 13 Abs. 2, 3 TMG auf Einwilligungen außerhalb des TMG ist umstritten, so dass es entweder der Schriftform, der elektronischen Form gem. § 126a BGB oder besonderer Umstände, welche zur Angemessenheit einer anderen Form als der Schriftform führt, bedarf.

- der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat (z.B. durch Ankreuzen einer vorformulierten Einwilligung)[25],
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.[26] Hierauf ist der Nutzer bereits vor Erteilung der Einwilligung hinzuweisen.

Die Einwilligung muss freiwillig durch den Nutzer abgegeben worden sein.

4.2. Datenschutzgrundsätze

4.2.1. Grundsatz der Direkterhebung

Gem. § 4 Abs. 2 S. 1 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Ausnahmen bestehen nach § 4 Abs. 2 S. 2 BDSG nur dann, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte für die Beeinträchtigung eines überwiegend schutzwürdigen Interesses der betroffenen Person besteht. Die betroffene Person soll wissen, wer welche Daten zu welchen Zwecken über sie erhebt, verarbeitet und nutzt. Die personenbezogenen Daten müssen somit nicht nur bei ihr direkt, sondern auch unter Mitwirkung erlangt werden. Diese Mitwirkung kann sowohl aktiv als auch passiv durch die betroffene Person geschehen. In beiden Fällen muss die betroffene Person allerdings über die Datenerhebung Bescheid wissen. Findet eine Datenerhebung heimlich statt, so wird der Grundsatz der Direkterhebung verletzt, soweit nicht eine der genannten Ausnahmen greift.

Im Rahmen eines App-Angebotes ist es daher notwendig, den Nutzer konkret über die Erhebung und Verwendung seiner personenbezogenen Daten zu informieren.

Werden Daten von Dritten z. B. bei Adressbuch-Apps oder Apps mit Verbindung zu sozialen Netzwerken (Freundesliste) über eine App erhoben und verwendet, stellt sich die Frage, inwieweit dies zulässig ist. So hat das KG Berlin (Urteil vom 24.01.2014 - 5 U 42/12) im Zusammenhang mit der Erstellung einer Freundesliste und der Möglichkeit des Versands von Einladungs-E-Mails entschieden, dass es „an einer E-Mail-Werbung des Unternehmens fehlen [kann], wenn das Unternehmen zwar Nutzer auffordert, anderen Verbrauchern Einladungs-E-Mails zu übersenden, das Unternehmen da-

[25] Eine bewusste und eindeutige Einwilligung kann nicht über eine Opt-out-Lösung erlangt werden, bei der der Nutzer erst die entsprechende Voreinstellung abwählen muss, indem er z.B. ein bereits aktiviertes Kreuzchen deaktivieren muss.

[26] Es handelt sich nicht um eine wirksame Einwilligung, wenn der Nutzer entweder den Dienst „so nehmen muss, wie er ist“ oder den Dienst nicht in Anspruch nehmen kann und ein Widerruf der „Einwilligung“ nur durch Beendigung des Nutzungsvertrages möglich ist.

bei aber nur technische Hilfe leistet, damit die Nutzer bequem eine solche eigene persönliche Einladungs-E-Mail an Verwandte, Freunde und Bekannte versenden können.“[27]

Eine solche Einladungs-E-Mail ist allein dem privaten Nutzer zuzurechnen, wenn dieser sich in Kenntnis aller wesentlichen Umstände -und damit eigenverantwortlich- zur Versendung dieser E-Mails entschließt. Der auch für das Unternehmen werbende Effekt wird dabei durch den privaten Zweck der Einladungs-E-Mails verdrängt. Denn dem Nutzer geht es dabei allein darum, mit den von ihm Eingeladenen ebenfalls über das soziale Netzwerk und die von diesem gebotenen Vorteile kommunizieren zu können. Es muss keinem Verbraucher verwehrt werden, Freunden und Bekannten in einer E-Mail einen konkreten Hinweis auf ein von ihm für gut befundenes Produkt zu geben."

4.2.2. Grundsatz der Datenvermeidung und der Datensparsamkeit

Nach dem in § 3a BDSG normierten Grundsatz der Datenvermeidung und der Datensparsamkeit sollten so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden. Diesem Ziel kann auch eine Pseudonymisierung i.S.d. § 3 Abs. 6a BDSG oder Anonymisierung i.S.d. § 3 Abs. 6 BDSG von Daten dienen. Aus diesem Grund ist bereits bei der Entwicklung einer App darauf zu achten, dass durch diese später nur diejenigen personenbezogenen Daten erhoben und verwendet werden, die erforderlich sind.

4.2.3. Grundsatz der anonymen und pseudonymen Nutzung

Soweit es dem Diensteanbieter technisch möglich und zumutbar ist, hat der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung gem. § 13 Abs. 6 TMG anonym oder unter Pseudonym zu ermöglichen. Über diese Möglichkeit ist der Nutzer zu informieren. Dem Nutzenden muss z.B. bei Apps zur Nutzung sozialer Netzwerke jedenfalls die Möglichkeit gegeben werden unter Pseudonym zu agieren, wenngleich eine Offenlegung der Identität gegenüber dem Diensteanbieter zur Erschwerung von Missbrauch hingenommen werden kann.[28]

4.2.4. Grundsatz der Zweckbindung

Jeder Umgang mit personenbezogenen Daten muss einen bestimmten, legitimen Zweck verfolgen. Eine Datensammlung ohne Verfolgung eines konkret festgelegten Zwecks ist genauso wenig zulässig wie die Änderung eines Zweckes und der Verwendung der bis dahin gesammelten Daten für diesen neuen Zweck, ohne dass auch für diesen Datenumgang eine Erlaubnis existiert. Soweit der verfolgte Zweck wegfällt, sind die personenbezogenen Daten grundsätzlich zu löschen. Bei Vorhandensein von Aufbewahrungsfristen (etwa nach Vorgaben der Abgabenordnung oder des Handelsgesetzbuches) o.ä. sind die Daten zu sperren und damit von den aktuellen Produktivdaten zu trennen.

[27] Vgl. Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke der Artikel-29-Datenschutzgruppe, WP 163, Ziff. 3.8 Abs. 2, Seite 12

[28] Vgl. Kapitel 4.5 der Orientierungshilfe „Soziale Netzwerke“ der Konferenz der Datenschutzbeauftragten und der Länder vom 14.03.2013

Der Grundsatz der Zweckbindung spielt im Zusammenhang mit der Einholung von Berechtigungen und der damit zusammenhängenden Möglichkeit, Zugriff auf zahlreiche Daten nehmen zu können, eine besondere Rolle, sofern die Plattformen ein Berechtigungskonzept unterstützen. Dabei gelten die folgenden Anforderungen:

- Es dürfen nur die für die App erforderlichen Berechtigungen vom Nutzer angefordert werden. Dabei sind die Möglichkeiten, die die Plattform für die Rechtevergabe bietet, auszuschöpfen. Einige Betriebssysteme bieten Berechtigungen nur in festen Kombinationen an, welche neben dem erforderlichen Recht auch nicht benötigte enthalten.[29] Soweit das durch die Begrenzung auf neuere Betriebssystemversionen vermieden werden kann, ist dies bei Entwicklung der App zu berücksichtigen. Lässt sich eine unnötige Berechtigungsgewährung nicht vermeiden, sollte der Anbieter in der Datenschutzerklärung (siehe Kapitel 5.2.4) über diesen Umstand aufklären und sich gegenüber dem Nutzer dazu verpflichten, von dem nicht erforderlichen Recht keinen Gebrauch zu machen.
- Auch wenn ein Nutzer bei der Installation einer App pauschale Berechtigungen erteilt, darf die verantwortliche Stelle dennoch lediglich auf diejenigen Daten zugreifen, die für den verfolgten legitimen Zweck benötigt werden. So ist z.B. ein Zugriff auf das gesamte Adressbuch des Geräts mit all den darin hinterlegten persönlichen Informationen des Nutzers und seiner Kontakte und deren Verwendung nicht zulässig, wenn lediglich z.B. eine Adresse für die Navigation mit einer App benötigt wird.

4.2.5. Grundsatz der Erforderlichkeit

Sofern Möglichkeiten bestehen, personenbezogene Daten durch Verarbeitungsschritte so zu verändern, dass der Informationsgehalt auf das erforderliche Mindestmaß begrenzt wird, ist dies entsprechend umzusetzen, sofern keine anderen Kriterien dies verhindern.

Beispielsweise sollten Standortdaten nur so genau übertragen werden wie es tatsächlich erforderlich ist. Dies spielt insbesondere bei Umkreissuchen eine wichtige Rolle. Hierbei ist es häufig nicht notwendig, dass der Standort des Nutzers metergenau erhoben und verwendet wird.

Zudem muss sich auch die Speicherdauer eines jeden personenbezogenen Datums am Grundsatz der Erforderlichkeit messen lassen.

[29] Z.B. lässt sich bei Android bis zur Version 4.03 der Zugriff auf das Kontaktverzeichnis nicht erteilen, ohne gleichzeitig Zugriffsrechte auf den Anrufverlauf zu bekommen. Diese Berechtigungskoppelung kann nur umgangen werden, indem die Unterstützung älterer Android-Versionen gezielt ausgeschlossen wird (siehe http://developer.android.com/reference/android/Manifest.permission.html#READ_CALL_LOG).

5. Unterrichtung des Nutzers und Nutzerrechte

Der App-Anbieter muss zunächst ein Impressum (vgl. § 5 TMG) vorhalten und der Nutzer ist durch den App-Anbieter bereits zu Beginn des Nutzungsvorgangs ohne ein vorhergehendes eigenes Tätigwerden über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu informieren (vgl. § 13 Abs. 1 TMG). Daneben stehen dem Nutzer weitere Rechte zu, deren Erfüllung er teilweise aktiv verlangen muss.

5.1. Impressum

Nach § 5 TMG haben Telemedienanbieter und somit diejenigen App-Anbieter, welche unter das TMG fallen, für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien bestimmte Angaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu veröffentlichen. Ein geschäftsmäßig angebotenes Telemedium kann nur bei rein privaten Angeboten verneint werden. Ein privates Angebot wird jedoch kaum vorliegen, soweit eine App über einen App-Store angeboten wird. Die Geschäftsmäßigkeit erfordert nicht zwingend eine Gewinnerzielungsabsicht, allerdings wird eine gewisse Nachhaltigkeit und somit ein auf einen längeren Zeitraum ausgerichtetes Angebot verlangt. Apps im Anwendungsbereich dieser Orientierungshilfe (s. Kapitel 1) sind danach grundsätzlich als geschäftsmäßiger Telemediendienst einzuordnen.
Handelt sich bei dem App-Angebot um kommerzielle Kommunikation (Begriffsbestimmungen in § 2 Abs. 5 TMG), die Telemedien oder Bestandteile von Telemedien sind, sind gem. § 6 TMG weitere Voraussetzungen zu beachten.

5.2. Datenschutzerklärung

5.2.1. Pflichten des App-Anbieters

Der App-Anbieter hat gemäß § 13 Abs. 1 S. 1 TMG den Nutzer „zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten [außerhalb der EU bzw. des EWR] (...) in allgemein verständlicher Form zu unterrichten". Nach Satz 3 des § 13 Abs. 1 TMG muss der Inhalt der Unterrichtung für den Nutzer jederzeit abrufbar sein. Zudem ist der Nutzer zu Beginn eines automatisierten Verfahrens, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, hierüber zu informieren (vgl. § 13 Abs. 1 S. 2 TMG). Letztere Unterrichtungspflicht zielt insbesondere auf den Einsatz von Cookies ab, betrifft jedoch nicht nur diese. Auch sollte die Datenschutzerklärung das Datum ihrer Erstellung enthalten.

5.2.2. Hinweise zum Nutzungsbeginn

Eine frühzeitige Verankerung dieser Datenschutzhinweise ist im Gegensatz zu einer Webseite nicht erst nach dem Aufruf des Dienstangebotes möglich, sondern bereits in dem Moment, in welchem die App in einem App-Store eingestellt wurde und vom Nutzer installiert werden kann oder auch vor dem eigentlichen Start der App auf dem Gerät des Nutzers. Die Datenschutzerklärung muss somit

entweder im App-Store oder nach dem Herunterladen und vor dem Start der App für den Nutzer zum Abruf bereitgehalten werden. Die größten App-Stores empfehlen App-Anbietern bereits beim Einstellen der App in den jeweiligen App-Store von dieser Möglichkeit Gebrauch zu machen, um den Nutzer umfassend über die Datenverarbeitung zu informieren.[30]

5.2.3. Jederzeit abrufbereite Unterrichtung

Unabhängig davon, auf welche Weise ein App-Anbieter zu Beginn des Nutzungsvorgangs informiert, muss der Nutzer zusätzlich jederzeit die Datenschutzerklärung abrufen können, so dass eine weitere Verankerung in der App zwingend erforderlich ist. Die Unterrichtung muss dabei jeweils leicht auffindbar platziert werden, so dass dem Nutzer die Kenntnisnahme der Informationen ohne Hindernisse möglich ist. Innerhalb der App kann so z.B. ein Informationsbutton „i“ oder sonstige leicht erreichbare und auffindbare Lösungen, wie „Rechtliches“, „Datenschutzhinweis“ oder „Datenschutzerklärung“ eingebaut werden. Inwieweit sich die Informationen innerhalb der App befinden oder lediglich verlinkt sind, ist grundsätzlich irrelevant. Soweit im Offline-Betrieb einer App personenbezogene Daten auf dem Gerät o.ä. abgelegt werden, um diese bei einem späteren Online-Betrieb zu übertragen, genügt eine Verlinkung auf eine Datenschutzerklärung unter Umständen nicht.

5.2.4. App-spezifische Datenschutzerklärung

Eine einfache Verknüpfung mit den Datenschutzhinweisen eines ähnlichen oder alternativen Webangebotes des gleichen Anbieters genügt nicht den Ansprüchen an eine Unterrichtung nach den Vorschriften des TMG zu dem konkreten Dienst, da es - auch soweit gefühlt der gleiche Dienst angeboten wird - erhebliche Unterschiede geben kann:

Im Gegensatz zu dem Aufruf einer Webseite werden bei der Installation von Apps Berechtigungen bei dem Nutzer eingeholt, mittels derer der App-Anbieter über die Schnittstellen auf die Funktionen des Gerätes und somit auch auf Daten, welche auf dem Gerät gespeichert sind, eingegeben oder generiert werden, zugreifen kann. Während eine App somit auf Funktionen des Geräts potentiell zugreifen kann, wie z. B. Kamera, Mikrofon, Kontaktbuch, Standort, Telefon, SMS etc., ist es durch das bloße Aufrufen einer Webseite für den Webseitenanbieter im Allgemeinen nicht ohne Nutzerbetätigung möglich, über den Internetbrowser auf das Gerät des Nutzers in dieser weitgehenden Form zuzugreifen. Etliche Berechtigungen werden gerade dazu benötigt, personenbezogene Daten zu erheben oder zu verwenden, so dass eine konkrete Unterrichtung des Nutzers zu Art, Umfang und Zweck des Datenumgangs zwingend erforderlich ist. Soweit Berechtigungen sichtbar eingeholt werden, sind

[30] Google legt in Ziffer 4.3 des Android Developer Distribution Agreement (zuletzt abgerufen am 05.02.2014) gegenüber den App-Anbietern fest „Sie sind zudem verpflichtet, den betreffenden Nutzern rechtlich einwandfreie Datenschutzhinweise sowie einen entsprechenden Schutz zu bieten (http://play.google.com/intl/ALL_de/about/developer-distribution_-agreement.html). Apple fordert in Ziffer 3.1 (b) des iOS Developer Program License Agreement (Version 1-22-10) „All information provided by You and Apple or Your end users in connection with this agreement or Your Application, including without limitation Licensed Application Information, will be current, true, accurate and complete (…)“ (https://www.eff.org/files/20100127_iphone_dev_agr.pdf).

hierbei die jeweilige Berechtigung und die konkret stattfindenden Zugriffe (vgl. Kapitel 4.2.4) zu benennen.[31] Um nicht den Eindruck einer unvollständigen Information entstehen zu lassen, sollte darüber hinaus auch über Berechtigungen unterrichtet werden, welche einen Zugriff zwar ermöglichen, aber nicht für den Zweck der Datenerhebung vom App-Anbieter eingeholt und genutzt werden. Dem Nutzer muss sich beim Lesen der Datenschutzinformation erschließen, zu welchen Zwecken bestimmte Berechtigungen eingeholt werden.[32] Als nicht ausreichend ist eine negative Beschreibung anzusehen, bei der der App-Anbieter ausschließlich darstellt, was er nicht macht. Dem Nutzer ist der Umfang einer Berechtigung im Regelfall nicht bekannt; er kann somit nicht abschätzen, ob es sich um eine abschließende Darstellung handelt oder ob lediglich einige Datenumgänge herausgegriffen werden.

Eine weitere Abweichung zwischen App und Webseite besteht auch bei den Einstellungsmöglichkeiten für den Nutzer. Während bei gängigen Internetbrowsern gezielt Einstellungen zur Privatsphäre und zum Datenschutz vorgenommen werden können, wie z. B. das Löschen von Tracking-Cookies, ist es dem App-Nutzer über Betriebssystemmittel in der Regel nicht möglich, solch gezielte Maßnahmen selbst zu ergreifen. Werden diese allerdings in der Datenschutzerklärung unter Bezugnahme auf die Webseite dargestellt, so dienen diese Informationen nicht dem App-Nutzer. Er muss folglich davon ausgehen, dass die Datenschutzerklärung allgemein auf die Nutzung der App keine Anwendung findet.

5.2.5. Lesbarkeit

Wegen der beschränkten Display-Größe mobiler Endgeräte sind die Datenschutzhinweise vom App-Anbieter derart zu gestalten, dass der Nutzer jederzeit ohne großen Aufwand die gewünschten Informationen erhalten kann. Als besonders benutzerfreundlich hat sich dabei die Einteilung in Kapitel, welche einzeln geöffnet werden können, herausgestellt. Darüber hinaus kann es auch genügen, die wesentlichen Inhalte der Datenschutzerklärung wiederzugeben und für darüber hinausgehende Informationen gut sichtbar auf weitere Erläuterungen sowie die vollständige Datenschutzerklärung zu verlinken. Was die wesentlichen Inhalte der Datenschutzerklärung sind, bestimmt sich anhand des Funktionsumfangs der App. Zu den wesentlichen Inhalten können insbesondere Kontaktinformationen des Anbieters (Firmensitz), Beschreibung der Datenarten, die von der App erhoben werden (z.B. Standortdaten, Netzkommunikation, Kalender, Adressbuch, etc.), Erläuterung der Zwecke, für die diese Daten erhoben werden, Speicherdauer, Bezeichnung der Dritten, an die Nutzerdaten übermittelt werden, und der Zweck der Übermittlung an Dritte zählen.

[31] Die standardmäßigen Berechtigungsbeschreibungen genügen aufgrund ihrer Abstraktheit nicht für eine hinreichende Information des Nutzers.

[32] Sobald eine Berechtigung für das Nutzen einer App nicht benötigt wird, sollte vermieden werden, diese vom Nutzer einzufordern, da sonst das Risiko besteht, dass bei künftigen Updates der App die bislang ungenutzte Berechtigung ohne Wissen des Nutzers verwendet wird und ggf. personenbezogene Daten des Nutzers erhoben, verarbeitet oder genutzt werden. Stattdessen muss beim Hinzufügen einer neuen Berechtigung beim Update einer App die Einwilligung des Nutzers eingeholt werden, sofern personenbezogene Daten des Nutzers durch die neue App-Berechtigung berührt werden.

5.2.6. Kontaktmöglichkeiten

Um dem Nutzer die unkomplizierte Wahrnehmung seiner Nutzerrechte (vgl. Kapitel 5.3) zu ermöglichen, ist eine einfache Kontaktmöglichkeit (z.B. postalische Adresse, E-Mail Adresse) zu einer bei dem Anbieter für datenschutzrechtliche Fragen zuständigen Stelle in der Datenschutzerklärung zu hinterlegen. Hier kann der App-Anbieter dem Nutzer die Gelegenheit geben, an zentraler Stelle seine Nutzerrechte geltend zu machen.

5.3. Nutzerrechte

Jeder Nutzer, dessen personenbezogene Daten erhoben und verwendet werden, hat gem. § 34 BDSG (ggf. i.V.m. § 13 Abs. 7 TMG) das Recht, Auskunft über die durch die verantwortliche Stelle zu seiner Person gespeicherten Daten zu verlangen. Gemäß § 35 BDSG kann er die Berichtigung, Löschung und Sperrung von Daten verlangen. Diese Ansprüche bestehen auch bei Nutzung einer App für den Nutzer. App-Anbieter sollten deshalb wie auch bei anderen Verarbeitungen von Nutzerdaten (Bestands-, Nutzungs- und Inhaltsdaten) auf entsprechende Anfragen von Nutzern vorbereitet sein, um bei Bedarf zeitnah reagieren zu können.

6. Technischer Datenschutz

Eine zentrale Rolle bei der datenschutzgerechten Gestaltung spielt die Sicherheit einer App. Bereits im Entwicklungsprozess sollte zur Vermeidung erhöhter Entwicklungs- und Nachbesserungskosten darauf hingewirkt werden, kritische Schwachstellen von vornherein zu vermeiden und das Sicherheitsniveau der App auf ein Niveau zu setzen, das den datenschutzrechtlichen Anforderungen entspricht. Bei Verarbeitung personenbezogener Daten ergeben sich die notwendigen technischen Anforderungen an eine App aus den „Technischen und organisatorischen Maßnahmen“ nach § 9 BDSG (und der dazugehörigen Anlage) und aus § 13 Abs. 4 TMG. Nachfolgend werden zentrale Themenbereiche daraus vorgestellt:

6.1. Anmeldedaten

Im Rahmen einer **Authentifizierung** innerhalb der App ist zu berücksichtigen, dass im Falle einer Passwortauswahl ausreichend komplexe Passwörter entweder erzwungen oder durch explizite Darstellung der Passwortstärke empfohlen werden. Es muss dabei geprüft werden, ob ein Verfahren mit Benutzername und Passwort als Anmeldekennung ausreicht oder ob das App-Angebot ein höheres Schutzniveau erfordert, das z. B. über eine Zwei-Faktor-Authentifizierung (z. B. über QR-Code, Zertifikate,…) erreicht werden kann. Bei der Passworteingabe sollte dabei die Möglichkeit bestehen, das durch den Nutzer eingetippte Passwort zu maskieren, um die Gefahr sog. Shoulder-Surfing-Angriffe zu minimieren.

Die Speicherung eines Passworts in Klartext lokal auf dem Gerät sollte vermieden werden, da dieses im Falle eines unberechtigten Zugriffs (z.B. durch Verlust, Schadsoftware,…) entwendet werden kann. Stattdessen sollte bei der ersten Anmeldung einer App am App-Server ein Zugangstoken, der für eine App und das eingesetzte Gerät eindeutig ist, zur Authentifizierung erzeugt werden. Zusätzlich sollte es die Möglichkeit geben, diesen Zugangstoken (z.B. bei Verlust des Geräts) über die Webseite des Diensteanbieters sperren zu können. Sofern Passwörter dennoch auf dem Gerät gespeichert werden, ist auf den Einsatz von starken kryptographischen Verfahren nach dem Stand der Technik[33] zu achten.

Bei erhöhtem Schutzbedarf ist eine Speicherung der Zugangsdaten im Allgemeinen nicht zulässig, da mit dieser Funktion, die meist als Komfortmerkmal zur App-Bedienung eingesetzt wird, das notwendige Schutzniveau bei Verlust des Gerätes nicht erreicht werden kann. Zusätzlich ist in diesem Fall darauf zu achten, dass eine Auto-Logout Funktion umgesetzt wird, die nach einer gewissen Zeit der Inaktivität (z.B. 5 Minuten) den Benutzer von der App (und ggf. dem App-Dienst) abmeldet.

Gerätekennungen wie IMEI-Nummern oder MAC-Adressen (oder auch davon abgeleitete Hashwerte) sollten nicht zur Authentifizierung verwendet werden, da diese mit wenig Aufwand gefälscht oder entwendet werden können.

Bei der Realisierung einer Passwort-Vergessen-Funktion ist darauf zu achten, dass das neue Passwort nicht im Klartext an den App-Nutzer übertragen wird. Stattdessen ist, wie bei Webapplikationen üblich, ein zeitlich befristeter Zugangslink (mit z.B. 10 Minuten Gültigkeitsdauer) an den Nutzer zu senden. Bei erhöhtem Schutzbedarf muss ein Passwort verschlüsselt oder über alternative Kommunikationswege (z.B. Telefonhotline mit Geheimwort) übermittelt werden.

Die Rechtevergabe einer App im Rahmen einer **Autorisierung** sollte serverseitig erfolgen, da das Risiko einer Umgehung von App-seitig umgesetzten Sicherheitsmechanismen sehr hoch ist.

6.2. Eindeutige Kennungen

App-Entwickler müssen zudem verstärkt darauf achten, keine eindeutigen Daten als Identifizierungswerte im Hintergrund zu übertragen. Werden eindeutige Kennungen, wie z.B. die IMEI-Nummer oder die UDID (vgl. Kapitel 2.2), übertragen, gelten entsprechende Hinweis- und Zweckbindungspflichten (vgl. Kapitel 5.2) zur Datenschutzerklärung.

Sofern für das Nutzen der App eine eindeutige Kennung erforderlich sein sollte, wird empfohlen, eine zufallsgenerierte eindeutige Nummer (ein Token) zu erzeugen, die im Rahmen der App-Nutzung

[33] BSI – Technische Richtlinie. Kryptographische Verfahren und Schlüssellängen. Version 2014-01. Abrufbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

zwar eindeutig ist, außerhalb der App oder bei Neuinstallation jedoch keinen Bezug mehr zum Gerät bzw. Nutzer ermöglicht. Durch solche zufallsgenerierte Token wird die Möglichkeit der App-übergreifenden Nachverfolgung von Nutzern eingeschränkt. Nach Möglichkeit sollte dieser Token regelmäßig ausgewechselt werden.

6.3. Sichere Datenübertragung

Regelmäßig kommuniziert die App auf dem Gerät des Nutzers mit den Server-Backends des Anbieters oder sonstiger Dritter. Um sicherzustellen, dass personenbezogene Daten mit **normalem Schutzbedarf** während des Transports nicht unbefugt gelesen oder verändert werden, sollte sowohl beim Versand als auch beim Empfang entsprechender Daten die Kommunikationsverbindung mit dem Backend durch eine Transportverschlüsselung abgesichert sein. Die App und auch das Backend müssen daher so konfiguriert sein, dass eine sichere Verbindung auf Grundlage einer dem Stand der Technik entsprechenden Protokollvariante nach den Vorgaben des BSI oder höher ausgehandelt wird (zurzeit bspw. TLS 1.1 oder höher). Sollten diese Protokolle etwa aus Kompatibilitätsgründen nicht nutzbar sein, dürfen unsichere Varianten, wie bspw. SSL 3.0 bzw. TLS 1.0, allenfalls für einen kurzen Übergangszeitraum genutzt werden. Das Server-Backend sollte bei der Aushandlung der Verschlüsselung nur starke Chiffren (>= 128 Bit, bspw. 3DES, AES) verwenden und ausreichend große Schlüssellängen (>= 2048 Bit) einsetzen. Dabei sollten nur vertrauenswürdige Zertifikate, also solche, die von einer bekannten Zertifizierungsstelle ausgestellt wurden, zum Einsatz kommen.

Personenbezogene Daten dürfen auch bei der Nutzung von Transportverschlüsselung nicht in der URL bzw. im GET-Parameter der https-Anfrage übermittelt werden, da es durch Protokollierung der Aufrufe auf Seiten der App oder des Backend-Servers (etwa durch den Serverbetreiber) trotz Verschlüsselung zur Offenbarung personenbezogener Daten kommen kann.

Durch den Einsatz kurzlebiger Sitzungsschlüssel (Perfect Forward Secrecy) ist sicherzustellen, dass ein Angreifer aufgezeichnete Verbindungen selbst bei Brechen der Verschlüsselung einer Verbindung nicht nachträglich entschlüsseln kann. Zudem sollte darauf geachtet werden, dass die zum Einsatz kommenden Softwarebibliotheken zumindest mit FIPS-140-2 Zertifizierung Stufe 1 kompatibel sind.

Werden durch oder an die App Daten mit **erhöhtem Schutzbedarf**, wie z.B. Gesundheits- oder Kreditkartendaten übertragen, so muss mittels Zertifikats- oder Public-Key-Pinning zusätzlich sichergestellt werden, dass Angreifer nicht durch Unterschieben vermeintlich valider Zertifikate die Verbindung kompromittieren können. Die zum Einsatz kommenden kryptographischen Algorithmen und Schlüssellängen müssen sich an der Dauer der Schutzwürdigkeit der personenbezogenen Daten orientieren (z.B. kann eine notwendige Schlüssellänge von bis zu 15360-Bit bei RSA-Verfahren[34] bei Ge-

[34] ENISA, Algorithms, Key Sizes and Parameters Report, 2013 recommendations. Abrufbar unter https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

sundheitsdaten höhere Anforderungen nach sich ziehen, als aktuell eingesetzte Standardverfahren anbieten).

6.4. Lokale Datenspeicherung

Im Rahmen der App-Nutzung werden meist Daten auf dem Gerät lokal gespeichert. Dies können Benutzernamen, Zugangstoken, Cookies, Standortdaten, Adressen und app-spezifische-Daten in lokalen Datenbanken und Einstellungsdateien sein. Hierbei sollten nur diejenigen personenbezogenen Daten gespeichert werden, die unbedingt für den Betrieb der App notwendig sind. Auch die Speicherdauer muss sich an dieser Notwendigkeit orientieren. Diese Daten müssen ausreichend vor unbefugtem Zugriff geschützt werden. Dabei muss davon ausgegangen werden, dass ein Zugriff auf das Dateisystem des Geräts von Seiten eines Angreifers erfolgen kann, auch wenn dieser den Gerätenutzern aufgrund der Plattformbeschränkungen im Allgemeinen nicht möglich ist. Dies gilt insbesondere auch dann, wenn personenbezogene Daten auf der SD-Karte oder einem anderem leicht austauschbaren Datenträger des Geräts gespeichert werden.

Findet eine lokale Datenspeicherung durch eine App statt, ist dafür Sorge zu tragen, dass nach einem Deinstallieren der App auch die lokal gespeicherten personenbezogenen Daten des Nutzers gelöscht werden. Sollte es sich dabei um Daten handeln, die ggf. anderen Apps auf dem Gerät zur Nutzung zur Verfügung gestellt werden, so sollte der Nutzer gezielt bei der Deinstallation gefragt werden, ob er diese persönlichen Daten löschen oder auf dem Gerät belassen möchte.

Bei Speicherung von Daten mit **erhöhtem Schutzbedarf** müssen diese zusätzlich zu den Schutzmechanismen der Geräteplattform (z.B. Sandboxing) mit starken kryptographischen Verfahren nach aktuellem Stand der Technik[35] (z.B. Stand 2014: AES-256) abgesichert werden. Statt einer dauerhaften verschlüsselten Speicherung ist es empfehlenswert, die besonderen personenbezogenen Daten auch nur für die Dauer der Anwendung vom Server zur Darstellung an die App zu übertragen – auf eine entsprechend der Speichertechnologien der mobilen Endgeräte geeignete Implementierung wie z.B. wirksame Löschung der verwendeten Speicherbereiche ist dabei zusätzlich zu achten.

6.5. Logging

Die Protokollierung von Fehlermeldungen und Systemereignissen spielt gerade im Entwicklungszustand einer App eine wichtige Rolle. Sobald die App jedoch produktiv und somit im App Store für den Nutzer abrufbar ist, sollte das sogenannte Logging möglichst nicht oder nur eingeschränkt eingesetzt werden. Abhängig von der eingesetzten Logging-Variante besteht zum Beispiel bei Android die Gefahr, dass personenbezogene Daten in das Systemlog geschrieben und durch andere Apps mit der entsprechenden Berechtigung ausgelesen werden können.

[35] BSI – Technische Richtlinie. Kryptographische Verfahren und Schlüssellängen. Version 2014-01. Abrufbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Sofern Daten nicht nur an den App-Anbieter, sondern auch an den Entwickler der App geschickt werden, z. B. Fehler-Reports zur App, so ist darauf zu achten, dass keine personenbezogenen Daten übertragen werden. Eine Erhebung und Verwendung personenbezogener Daten des Nutzers einer App ist auf Entwicklerseite in der Regel nicht erforderlich und müsste deshalb im Einzelfall begründet werden und von einem Erlaubnistatbestand gedeckt sein.

6.6. Einbindung von Webseiten

Werden im Rahmen der App-Nutzung Inhalte von Webseiten eingebunden, besteht die Gefahr, dass dadurch auch das ggf. unberechtigte Laden von Drittanbieter-Inhalten datenschutzrechtliche Verstöße wie z.B. eine Reichweitenmessung ohne wirksame Widerspruchsmöglichkeiten nach sich zieht. Es ist technisch möglich, durch einen In-App-Browser ganze Webinhalte in der App zu integrieren, ohne dass es dem Nutzer ersichtlich ist, dass eine Internetseite innerhalb der App aufgerufen wird. Entsprechend ist es hierbei erforderlich, dass bei der Einbindung von Webseiteninhalten in der App darauf geachtet wird, welcher Webseitencode geladen wird. Durch Einstellungen seitens des Entwicklers wie Deaktivierung von JavaScript und Plug-ins kann beispielsweise bereits die Ausführung eines Teils des geladenen Webseitencodes technisch unterbunden werden. Des Weiteren müssen die Drittanbieterinhalte bei der Ausgestaltung der rechtlichen Anforderungen (z.B. der Datenschutzerklärung) beachtet werden.

6.7. Standortdaten

Sofern durch die App auf Standortdaten des Geräts zugegriffen wird, muss darauf geachtet werden, dass dies nur im zulässigen Umfang geschieht. Hierbei gilt es zu berücksichtigen, dass nur in der unbedingt nötigen Auflösung auf die Geodaten zugegriffen werden sollte, d. h. dass eine gezielte Verwaschung des Standorts erfolgt (z. B. statt „München Bahnhofsplatz 1“>„München Stadtmitte“). Dies kann z.B. durch Nullung von Dezimalstellen in den GPS-Koordinaten innerhalb der App vor Versand an den Backend-Server erreicht werden.

Des Weiteren sollten Standortdaten, soweit für die Anwendung möglich, nur lokal auf dem Gerät verarbeitet werden. In Kombination mit einer Standortlogik, die auf verwaschenen Koordinaten beruht, können standortgenaue Dienste ohne Übermittlung des genauen Standorts an den App-Anbieter realisiert werden. Wird z.B. der Standort „München Stadtmitte“ für die Suche nach Geldautomaten an den App-Anbieter übermittelt, so kann Karten- und Automatenstandortmaterial zu diesen verwaschenen Koordinaten an die App geliefert werden. Durch eine lokale Auswertung der genauen Standortdaten in Bezug auf das gelieferte Kartenmaterial können innerhalb der App individuelle Routen für den App-Nutzer ermittelt werden.

Eine Speicherung von Standortdaten auf dem Gerät darf nur dann stattfinden, wenn dies für die Funktionalität der App notwendig ist, da mit diese Daten bei unberechtigtem Zugriff Bewegungsprofile erstellt werden können.

Sofern Standortdaten von der App an das Backend des App-Anbieters gesendet werden, dürfen diese nur in dem Abtastintervall erhoben werden, das entsprechend dem Nutzungszweck der App notwendig ist. So wäre es für die Ermittlung von einer Liste von Geldautomaten nach Drücken auf einen „Suche"-Button nicht erforderlich, alle 10 Sekunden, auch ohne Nutzeraktion, den aktuellen Standort an den App-Anbieter zu übermitteln.

Die Zulässigkeit einer Weitergabe und Nutzung von Standortdaten (auch nach der „Verwaschung") an den App-Betreiber oder Dritte ist nur zu bejahen, wenn dies entweder erforderlich für die Erbringung des Dienstes ist oder eine Einwilligung des Nutzers vorliegt. Grundsätzlich sollte die Erhebung und Verwendung von Standortdaten jedoch vorher von dem Nutzer freigegeben werden müssen- auch soweit eine ausdrückliche Einwilligung des Nutzers nicht notwendig ist. Zudem wird empfohlen, dem Nutzer zu ermöglichen, die Lokalisierung abzuschalten, auch wenn dann u.U. ein Teildienst (z.B. die Restaurantsuche im Umkreis) nicht genutzt werden kann und ihm eine aktive Lokalisierungsfunktion anzuzeigen.

6.8. Server-Backend

Neben Schutzmechanismen auf Seite der App müssen die beteiligten Server- bzw. Cloud-Dienste ausreichend abgesichert sein. Bei Ermittlung von möglichen Bedrohungen und Risiken muss davon ausgegangen werden, dass ein Angreifer sämtliche in der App hinterlegten Daten wie URL, Passwörter, Tokens und Datenstrukturen in Erfahrung bringen kann (z.B. durch Reverse Engineering der App). Die Schutzmechanismen des Backends müssen vergleichbar wie bei Webapplikationen gegen Möglichkeiten des unbefugten Datenzugriffs wie z.B. durch Injection-Angriffe, Authentifizierungs- und Autorisierungsmanipulationen, Zugriffe auf Daten über Objektreferenzen absichern[36]. Ebenso müssen die beteiligten Systeme auf Netzwerkebene durch eine geeignete Netzwerk- und Firewall-Architektur sowie ein konsequent umgesetztes Patch-Management geschützt werden.

6.9. Spezielle Pflichten des Telemedienanbieters

Weitreichende Pflichten zur technisch-organisatorischen Ausgestaltung eines Dienstes ergeben sich für einen Telemedienanbieter auch aus § 13 Abs. 4 TMG. Der Diensteanbieter hat danach durch technische und organisatorische Vorkehrungen sicherzustellen, dass

[36] Ausführliche Informationen zu diesem Themenfeld finden sich z.B. bei den „OWASP Top 10 „ – Stand 2013 (abrufbar unter www.owasp.org) oder beim BSI Baustein „B 5.21 Webanwendungen" – Stand 2013 (abrufbar unter www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05021.html)

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,

2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des § 13 Abs. 4 Satz 2 („soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen“) gesperrt werden,

3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,

4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,

5. Daten nach § 15 Abs. 2 TMG nur für Abrechnungszwecke zusammengeführt werden können (vgl. Kapitel 4.1.1.3) und

6. Nutzungsprofile nach § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

Hieran erkennt man den Willen des Gesetzgebers, dass durch die Nutzung entstehende personenbezogene Daten in der Regel umgehend nach der Beendigung des Dienstes gelöscht werden müssen (vgl. Nr. 2), es sei denn, sie werden für Abrechnungszwecke benötigt (vgl. Nr. 5). Nicht erfasst hiervon werden Inhaltsdaten, die für die App selber erforderlich sind (z. B. Kalendereinträge bei einer Kalender-App).
Aber auch die Absicherung der Kommunikation etwa durch Einsatz von (SSL-) Verschlüsselung wird durch das Gesetz gefordert (vgl. Nr. 3). Dies gilt insbesondere, wenn personenbezogene Daten über das Internet übertragen werden.
Nr. 4 ist vor allem für Anbieter wichtig, die mehrere Dienste anbieten (etwa über eine gemeinsame App oder über mehrere Apps). Diese Daten müssen getrennt verwendet werden, so dass vermieden wird, dass in den Datenbanken gemeinsame Profile über die Nutzungen entstehen. Und hat der Betreiber des Dienstes (in der Regel der App-Anbieter) sich entschieden, Profile über seine Nutzer im Rahmen des § 15 Abs. 3 TMG zu erstellen (vgl. Kapitel 4.1.1.2.2), dann muss dieses nicht nur unter Pseudonym und mit Einräumung eines Widerspruchsrechts erfolgen, sondern auch durch den Betreiber verhindert werden, dass die Pseudonyme aufgedeckt werden.

Nach § 13 Abs. 6 TMG schließlich ist dem Nutzer die Weitervermittlung zu einem anderen Diensteanbieter anzuzeigen. Das bedeutet, dass der Nutzer erkennen können muss, wenn etwa über einen Link oder eine andere Verknüpfung ein Dienst von Dritten aufgerufen wird.

7. Erhöhter Schutzbedarf

Verarbeitet eine App Daten mit erhöhtem Schutzbedarf, bspw. besondere Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG, also Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, sind als Konsequenz zusätzliche Sicherheitsmaßnahmen erforderlich. Diese Maßnahmen sind gem. der Anlage zu § 9 BDSG je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien zu treffen.

Bei Apps aus dem Gesundheitsbereich werden regelmäßig Gesundheitsdaten verarbeitet. Dies können Daten über den physischen und psychischen Gesundheitszustand des Nutzers sein, aber auch Angaben zu einzelnen Krankheiten, deren ärztliche Begleitung sowie einzunehmende Medikamente. Ggf. können auch sogenannte Fitness-Apps, die Werte über den Blutdruck, das Gewicht oder Ausdauer eines Nutzers speichern, darunter fallen.
Um sicherzustellen, dass die Daten mit erhöhtem Schutzbedarf vor unberechtigtem Zugriff geschützt sind, sind sowohl auf dem Endgerät des Nutzers als auch –falls die Daten zum Anbieter oder an andere berechtigte Dritte übermittelt werden - für den Übertragungsweg und den Speicherort Sicherungsmaßnahmen zu ergreifen. So ist der Zugriff auf die App - und damit auf die dort gespeicherten besonderen Daten - mit einer gesonderten Authentifizierung zu versehen, die dem Schutzbedarf entspricht (vgl. Kapitel 6.2 zu Zugangsdaten). Die auf dem Endgerät gespeicherten Daten sind verschlüsselt abzulegen, um sie im Falle eines Geräteverlustes vor dem Zugriff Unbefugter zu schützen.
Werden die Daten zwischen der App und einem (berechtigten) Dritten übermittelt, ist die Datenübertragung entsprechend des Schutzbedarfes zu gestalten (vgl. Kapitel 6.3 zur sicheren Datenübertragung).

Generell gilt, dass bei der Bereitstellung von Apps, die Daten erhebt und verwendet, welche der Geheimhaltungspflicht des § 203 StGB (etwa Ärzte, Anwälte) unterliegen und bei der eine Offenbarung (etwa an Betreiber des App-Stores, der App-Infrastruktur oder Vertreiber des Betriebssystems) und damit ein Straftatbestand nicht ausgeschlossen werden kann, eine gesonderte Einwilligung (ggf. Schweigepflichtentbindungserklärung) der Nutzerin bzw. des Nutzers einzuholen ist.

8. Konsequenzen unzulässigen Datenumgangs

Die Datenschutzaufsichtsbehörden sind gem. § 38 Abs. 5 BDSG befugt, Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anzuordnen. Eine solche Anordnung kann bei Nichtbefolgung mittels eines Zwangsgeldes erzwungen werden. Führt dies nicht zum Erfolg, so kann ein Datenumgang oder der Einsatz einzelner Verfahren untersagt werden. In bestimmten Fällen kann daneben die Begehung einer Ordnungswidrigkeit oder sogar einer Straftat im Raum stehen: Daten-

schutzrechtliche Bußgeldtatbestände sind insbesondere in § 16 TMG und § 43 BDSG aufgezählt und können mit einer Geldbuße bis zu 50.000 Euro, zum Teil sogar bis zu 300.000 Euro geahndet werden. In § 44 BDSG wird geregelt, in welchen Fällen eine Straftat vorliegt, die mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft wird.

Adressat aufsichtsrechtlicher Maßnahmen ist jeweils die verantwortliche Stelle, während Adressat der Ordnungswidrigkeitenvorschriften jeweils diejenige natürliche Person ist, welche den Verstoß begangen hat. Allerdings kommt unter bestimmten, in § 30 des Ordnungswidrigkeitengesetzes (OWiG) geregelten Voraussetzungen auch eine Geldbuße gegen Unternehmen als solche in Betracht. Voraussetzung hierfür ist - vereinfacht gesprochen - ein Versäumnis einer Leitungsperson, infolge dessen es im Unternehmen zu einer (z.B. datenschutzrechtlichen) Ordnungswidrigkeit gekommen ist. Häufiger Anwendungsfall hiervon ist das sog. Organisationsverschulden, auch in der Form einer mangelhaften Aufsicht: die Geschäftsleitung ist grundsätzlich dafür verantwortlich, dass das Unternehmen im Zuge seiner wirtschaftlichen Betätigung alle geltenden einschlägigen Anforderungen der Rechtsordnung einhält, somit auch diejenigen des Datenschutzrechts. Die Geschäftsleitung muss hierfür, insbesondere durch geeignete Organisation und Aufsicht im Unternehmen, Sorge tragen. Ist insoweit einer Leitungsperson ein (organisatorisches) Versäumnis vorzuwerfen, kann eine Geldbuße gegen das Unternehmen in Betracht kommen.

9. Besonderheiten / Hinweise

9.1. Bezahlvorgänge

Mit Hilfe einiger Apps können heute schon Smartphones zum Bezahlen verwendet werden. Der Bezahlvorgang wird dabei in elektronischer Form und in der Regel kontaktlos abgewickelt. Technisch realisiert wird der kontaktlose Bezahlvorgang z.B. durch die Near Field Communication (NFC). Unterschieden werden kann zwischen zwei Betriebsmodi:

- Das Smartphone kommuniziert über eine App mit einem NFC-Lesegerät, z. B. einem Händlerterminal. In diesem Fall übernimmt das Smartphone die Rolle einer kontaktlosen Smartcard (Card Emulation Modus). Die notwendigen kritischen Operationen (Authentifizierung, Schlüsselberechnung, Speicherung von PIN u.a.) werden dabei auf einem sicheren Element auf dem Smartphone (regelmäßig im NCF-Bauteil oder in der SIM-Karte) durchgeführt.
- Wie im ersten Fall übernimmt das Smartphone die Rolle der Smartcard. Jedoch werden die kritischen Operationen vollständig in der App durchgeführt und das NFC-Bauteil nur zur Übertragung der Daten genutzt (Host Card Emulation Modus).
- Beim Read/Writer-Modus vertauschen sich die Rollen und das Smartphone wird zum NFC-Lesegerät. Mit einer Smartcard lassen sich (kontaktlos) am Smartphone Bezahlvorgänge durchführen.

Bei der Verwendung von Apps als Zahlungssoftware sind verschiedenste Regelungen aus den Bereichen des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG), des Bundesdatenschutzgesetzes (BDSG), des Zahlungsdiensteaufsichtsgesetzes (ZAG), des Kreditwesengesetzes (KWG), des Bürgerlichen Gesetzbuchs (BGB), und der EU-Richtlinien (z.B. Payment Services Directive) zu beachten.

Der Datenumgang ist dem Diensteanbieter im gesetzlichen Rahmen des § 28 Abs. 1 S. 1 Nr. 1 BDSG gestattet. Der Diensteanbieter kann danach personenbezogene Daten der Nutzer (z.B. Name, Kontoverbindungsdaten, Preis, Kaufsache) nur erheben, speichern, verändern oder übermitteln, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Nutzer erforderlich ist. Ein darüber hinausgehender Datenumgang durch den Diensteanbieter ist nur im Umfang einer zuvor einzuholenden Einwilligung der Nutzer zulässig.

Für die im Rahmen eines Zahlungsvorgangs erhobenen personenbezogenen Daten gilt eine strenge Zweckbindung. Die Verwendung der erhobenen Daten zu Zwecken der Direktwerbung ist nur unter den Voraussetzungen des § 28 Abs. 3 BDSG zulässig.

Die Verwendung von Nutzungsdaten zur Erstellung von Nutzungsprofilen zu Zwecken der Marktforschung (Analyse des Nutzerverhaltens) oder zu Werbezwecken ist ohne Einwilligung nur unter den Voraussetzungen des § 15 Abs. 3 TMG zulässig (vgl. Kapitel 4.1.1.2.2).

Bei Bankkontodaten handelt es sich um besonders sensible Daten, deren Kenntnisnahme durch unberechtigte Dritte eine Meldepflicht nach § 42a BDSG nach sich zieht. Die Sicherung der Bankkontodaten durch technisch-organisatorische Maßnahmen, insbesondere einem sicheren Übertragungsweg kommt daher besondere Bedeutung zu.

Bei der Entwicklung von Bezahl-Apps sollte darauf geachtet werden, dass ein Bezahlvorgang nicht ohne Kenntnis und aktive Mitwirkung der Nutzer stattfinden kann. Die Informationen sollten insbesondere Name und Anschrift des Vertragspartners und den zu entrichtenden Preis enthalten. Ferner sollte die App eine nachvollziehbare Authentifizierung und Protokollierung bereitstellen.[37] Wird beim Einsatz einer Bezahlfunktion eine rein softwarebasierte Berechnung und Speicherung der kritischen Nutzerdaten (Authentifizierung, Schlüsselspeicher) eingesetzt, ist die Sicherheit dieser Daten nach dem Stand der Technik zu gewährleisten.

[37]Weitere Informationen zum Mobile Payment finden Sie in der Veröffentlichung zum 3. Verbraucherdialog Rheinland-Pfalz „Mobile Payment“, Empfehlungen der Arbeitsgruppe Zahlungssicherheit (http://www.datenschutz.rlp.de/downloads/misc/mobile_payment/Empfehlungen_der_AG_Zahlungssicherheit.pdf) und Schütte, NFC? Aber sicher, DuD 2014, 20ff.

9.2. Nutzung alternativer Quellen zum Bezug von Apps

Apps finden zu einem überwiegenden Teil über App-Stores der großen Anbieter wie Apple, Microsoft oder Google Verbreitung. Apple bzw. Microsoft sehen für ihre Mobilgeräte, die das Betriebssystem iOS bzw. Windows Phone verwenden, außer der Nutzung des eigenen App-Stores keine weitere Möglichkeit zum Erwerb von Apps vor. Die Verwendung von Software aus alternativen Quellen ist lediglich nach Überwindung technischer Zugangshinderungen möglich (sog. „Jailbreak"). Im Gegensatz dazu bietet Google für Android-Mobilgeräte die Möglichkeit, Apps von anderen Quellen als dem Play Store zu erwerben. Damit können Apps z.B. von Webseiten heruntergeladen und auf den Endgeräten installiert werden. Neben einzelnen Apps können für Android auch ganze alternative App-Stores aus dem Internet geladen und installiert werden.[38]

Bei der Auswahl eines Distributionswegs handelt ein App-Anbieter datenschutzfreundlich, wenn er neben App-Stores, bei denen der Bezug von Apps mit einer Registrierung und weiteren Datensammlungen verbunden ist, den Endnutzern weitere Möglichkeiten zum Erwerb von Apps bietet. Gleiches gilt für die Auswahl von App-Stores, die eine Registrierung unter einem Pseudonym ermöglichen sowie für Angebote, für deren Bezahlung nicht die Angaben von Kreditkarteninformationen erforderlich ist, sondern stattdessen Prepaid-Karten verwendet werden können.

Des Weiteren ist es empfehlenswert, dass die Nutzerin bzw. der Nutzer der App beim Download der App aus dem App-Store erkennen können sollte, ob es sich um eine nicht-manipulierte Version der App handelt. Wünschenswert wäre daher die Generierung von Hashwerten etc. als Fingerprint durch die App, die es sicherheitsbewussten Nutzern erlauben würde, diese mit den entsprechenden Werten auf z. B. der Webseite des Entwicklers zu vergleichen. Dazu ist es notwendig, dass ein geeigneter Algorithmus zur Erzeugung des Fingerprints verwendet wird.

9.3. Apps für Jugendliche und Kinder

Kinder und Jugendliche haben häufig nur ein geringes Verständnis und Wissen in Bezug auf den Umfang und die Sensibilität der Daten, die bei der Verwendung einer App übertragen und möglicherweise an Dritte weitergegeben werden. Daher tragen Anbieter und Entwickler bei App-Angeboten, die sich speziell an die Zielgruppe Minderjähriger richten, besondere Verantwortung im Umgang mit deren Daten.

Zu unterscheiden ist generell weiterhin zwischen dem Datenumgang auf Basis gesetzlicher Erlaubnistatbestände und dem Datenumgang auf Basis einer Einwilligung. In beiden Situationen sind jedoch das besondere Interesse Minderjähriger und deren Einsichtsfähigkeit in die Wertung der datenschutzrechtlichen Zulässigkeit einzubeziehen. Hinsichtlich der Einsichtsfähigkeit stellt das Daten-

[38] Ein Beispiel für einen alternativen Non-Profit App-Store, der auf Free und Open Source Software spezialisiert ist und nach eigenen Angaben keine Nutzungsdaten erhebt, ist F-Droid (https://www.f-droid.org).

schutzrecht nicht auf die Geschäftsfähigkeit (vgl. §§ 104 ff. BGB) ab und legt keine verbindliche Altersgrenze fest, ab der diese Fähigkeit bei Kindern und Jugendlichen generell angenommen werden könnte. Entscheidend ist vielmehr in Anknüpfung an die Berechtigung und Mündigkeit zur Ausübung des Grundrechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, ob ein Kind oder Jugendlicher in der Lage ist, die Konsequenzen des Umgangs mit seinen Daten zu überblicken. Diese Beurteilung kann nur für den Einzelfall erfolgen, da sie abhängig ist vom jeweiligen Entwicklungsstand des Minderjährigen und der beabsichtigten Verwendung der Daten.

Sofern der Minderjährige selbst nicht über die notwendige Einsichtsfähigkeit und geistige Reife verfügt, sind deshalb regelmäßig die Erhebung und Verwendung Daten Minderjähriger nur nach Einwilligung durch die Erziehungsberechtigten rechtmäßig. Bei unter 14-jährigen wird im Allgemeinen die Fähigkeit zur Abschätzung der Tragweite einer Einwilligung in die Verarbeitung der eigenen Daten - insbesondere unter Berücksichtigung der komplexen Datenverarbeitungsprozesse, die der Verwendung von Apps zugrunde liegen - abzulehnen sein. App-Anbieter müssen deshalb bei App-Angeboten, die an die Zielgruppe der unter 14-jährigen gerichtet sind, in diesen Fällen sicherstellen, dass die Einwilligung der Eltern zur Datenverarbeitung vorliegt. In der Praxis wird die Einwilligung der Eltern teilweise durch Bestätigung eines Aktivierungslinks abgefragt, der an die E-Mail Adresse der Eltern versandt wurde. Problematisch an dieser Methode ist jedoch, dass nicht sichergestellt werden kann, dass die Bestätigung des Links tatsächlich durch die Eltern erfolgt ist. Anbieter sind angehalten, effektive Mechanismen zur Altersverifikation und Beteiligung der Eltern zu entwickeln und Missbrauch konsequent zu reglementieren. Generell sind Hinweise und Informationen zur Datenverarbeitung in angemessener und verständlicher Sprache zu formulieren, die sich an den Fähigkeiten der Zielgruppe orientiert, so dass Kinder und Jugendliche die Auswirkung und Konsequenzen der Nutzung begreifen können. Das Einwilligungsrecht der Eltern geht graduell auf das Kind über, d.h. der Entscheidungsspielraum der Eltern nimmt in dem Maß ab, in dem die Einsichtsfähigkeit des Kindes zunimmt.

Unabhängig von der datenschutzrechtlichen Bewertung ist bereits fraglich, ob das einer App-Nutzung durch beschränkt geschäftsfähige Minderjährige im Alter zwischen 7 und 14 Jahren zugrundeliegende Rechtsgeschäft ohne die Zustimmung der Eltern gemäß §§ 104 ff. BGB rechtsverbindlich zustande kommen kann.

9.4. Apps öffentlicher Stellen

Die vorliegende Orientierungshilfe des Düsseldorfer Kreises wurde für den nicht-öffentlichen Bereich erstellt. Der Düsseldorfer Kreis ist ein informeller Zusammenschluss der Aufsichtsbehörden im nicht-öffentlichen Bereich. Handelt es sich bei den Akteuren[39] um öffentliche Stellen, so gelten die Vor-

[39] Denkbar ist auch eine Konstellation, bei der es sich bei dem App-Anbieter um eine öffentliche Stelle, bei dem App-Entwickler oder einem weiteren Akteur jedoch um eine nicht-öffentliche Stelle handelt.

schriften des TMG auch für diese. Daneben ist eine Orientierung an den dargestellten Grundsätzen und rechtlichen Ausführungen möglich. Die Zulässigkeit der Erhebung und Verwendung personenbezogener Daten durch Behörden und andere öffentliche Stellen richtet sich allerdings nach den für diese Stellen maßgeblichen Datenschutzregelungen. Für den öffentlichen Bereich gelten insbesondere die jeweiligen Landesdatenschutzgesetze (es sei denn, es handelt sich um Stellen gem. § 1 Abs. 2 Nr. 1 und Nr. 2 BDSG) oder vorrangig zu beachtende bereichsspezifische Datenschutzvorschriften. Die Einhaltung dieser Regelungen ist jeweils genau zu prüfen und sicherzustellen.