Stephan Schwarz

Gibt's dafür auch eine App?

Datenschutzrechtliche Anforderungen an mobile Bibliotheks-Apps und Leitfaden für die Praxis

kassel university press

Stephan Schwarz

Gibt's dafür auch eine App?

Datenschutzrechtliche Anforderungen an mobile Bibliotheks-Apps und Leitfaden für die Praxis

kassel university press

Die vorliegende Arbeit wurde vom Fachbereich Wirtschaftswissenschaften der Universität Kassel als Masterarbeit zur Erlangung des akademischen Grades Master of Public Administration (MPA) angenommen.

Erster Gutachter: Dr. iur. Rainer Biskup
Zweiter Gutachter: PD Dr. iur. Margrit Seckelmann

Tag der mündlichen Prüfung: 25. Juni 2016

Dr. Stephan Schwarz ist Mitarbeiter der Bayerischen Staatsbibliothek in München, derzeit als Leiter des Referats Informationsdiente und Ortsleihe sowie als stellvertretender Leiter der Abteilung Benutzungsdienste.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

ISBN 978-3-7376-0294-5 (print)
ISBN 978-3-7376-0295-2 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783737602952
URN: http://nbn-resolving.de/urn:nbn:de:0002-402959

Printed in Germany

Vorwort

Mobile Apps für Smartphones und Tablet-Computer erfreuen sich immer größerer Beliebtheit. Die Downloadzahlen der verschiedenen App-Stores erklimmen täglich neue Höhen. Man findet kaum noch ein Unternehmen, das nicht mit mindestens einer App im Markt präsent ist. Da ist es nicht verwunderlich, dass auch zahlreiche öffentliche Institutionen und Körperschaften bemüht sind, von diesem Trend zu profitieren und sich die Vorteile mobiler Apps im Bereich des E-Government zunutze zu machen.

Sehr frühzeitig haben Bibliotheken diesen Trend erkannt und aufgegriffen. Als gefragte und innovative Informationsdienstleister ist es ihnen ein wichtiges Anliegen, ihre digitalen Bestände und zentralen Services in moderner und kundenorientierter Weise zur Verfügung stellen. Neben technischen und vertraglichen Gesichtspunkten sind bei mobilen Bibliotheks-Apps auch zahlreiche datenschutzrechtliche Fragestellungen zu beachten. Smartphone- und Tablet-Nutzer speichern nämlich oft erhebliche Mengen an personenbezogenen Daten (Adressdaten, Bankdaten, Standortinformationen, Fotos und Videos) auf ihren mobilen Geräten.

Die datenschutzrechtlichen Anforderungen an mobile Bibliotheks-Apps sind vielfältig und komplex. Die vorliegende Arbeit hat das Ziel, die entsprechenden Rechtsgrundlagen zu analysieren und so zusammenzufassen (Kapitel 3), dass sie auch für interessierte Bibliotheksmitarbeiterinnen und -mitarbeiter ohne vertiefte rechtliche Kenntnisse nachvollziehbar sind. Besonderes Gewicht liegt auf der Entwicklung eines Praxisleitfadens (Kapitel 4) mit Empfehlungen und einer Checkliste, der den Projektverantwortlichen in den Bibliotheken praxisgerecht vermittelt, was bei der Konzeption, der technischen Realisierung und dem Produktiveinsatz mobiler Bibliotheks-Apps aus datenschutzrechtlicher Sicht zu beachten ist. Die Checkliste (Kapitel 4.2) ist so konzipiert, dass sie die Projektverantwortlichen in 100 sehr detaillierten Schritten durch den App-Entwicklungsprozess begleitet und immer wieder auf die in den einzelnen Phasen wichtigen datenschutzrechtlichen Fragestellungen aufmerksam macht, die sich auch bei Änderungen der gesetzlichen Grundlagen in gleicher Weise stellen werden.

Die Arbeit ist primär auf den Bibliotheksbereich ausgerichtet. Da es bisher keine vergleichbaren Handlungsempfehlungen gibt, können wesent-

liche Teile des Praxisleitfadens auch von anderen Einrichtungen der öffentlichen Verwaltung genutzt werden.

Die vorliegende Masterarbeit wurde im Rahmen des berufsbegleitenden Studiengangs „Öffentliches Management“ an der Management School der Universität Kassel (UNIKIMS) zur Erlangung des Abschlusses Master of Public Administration (MPA) angefertigt. Sie fußt einerseits auf den Studieninhalten des MPA-Studiengangs und der Auswertung der einschlägigen rechts- und verwaltungswissenschaftlichen Fachliteratur, andererseits auf meinen praktischen Erfahrungen aus der Mitarbeit bei verschiedenen App-Projekten im Rahmen meiner Tätigkeit an der Bayerischen Staatsbibliothek in München. Für die Veröffentlichung wurden die Statistikdaten zur Nutzung mobiler Endgeräte sowie zur App-Nutzung aktualisiert.

Mein besonderer Dank gilt Herrn Dr. iur. Rainer Biskup für die sowohl in fachlicher als auch menschlicher Hinsicht exzellente Betreuung dieser Masterarbeit sowie für die Erstellung des Erstgutachtens. Ebenso danken möchte ich Frau Priv.-Doz. Dr. iur. Margrit Seckelmann für die Übernahme des Zweitgutachtens.

München, im Februar 2017 Stephan Schwarz

Inhaltsverzeichnis

1 Einleitung

Smartphones und Tablet-Computer prägen derzeit wie kaum eine andere moderne Technologie das Leben vieler Menschen. Sie sind omnipräsent und mit ihnen die mobilen Apps, also kleine Anwendungsprogramme, die auf den mobilen Endgeräten installiert werden und deren Funktionsumfang erheblich erweitern. Aktuellen Erhebungen des Branchenverbands Bitkom[1] zufolge besaßen im Jahr 2016 etwa 53 Millionen der über 14-jährigen Deutschen und damit 76 Prozent dieser Bevölkerungsgruppe ein Smartphone.[2] Im Jahr 2015 waren es noch 65 Prozent. Dies entspricht einer Steigerungsrate von 17 Prozent. Bei den 14-29-Jährigen ist praktisch niemand mehr ohne Smartphone.[3] Im Bereich der Tablet-Computer sind die Zuwächse sogar noch deutlicher: Laut Umfrage steigerte sich der Anteil der Tablet-Nutzer in den letzten zwei Jahren von 28 auf 41 Prozent der befragten Bevölkerungsgruppe, was einer Steigerungsrate von gut 46 Prozent entspricht.[4] Im Gegensatz dazu fiel der Anteil der genutzten Desktop-PCs in den letzten Jahren kontinuierlich.[5] Der Trend ist demnach eindeutig vorgezeichnet: Weg von klassischen Geräten wie dem Desktop-PC und Laptop und weg vom stationären Internet über Kabel oder WLAN, hin zu mobilen Endgeräten wie Smartphone und Tablet bzw. hin zum mobilen Internetzugang über das Mobilfunknetz (LTE, 4G und 5G).[6]

Die Fülle der mobilen Apps ist mittlerweile nur noch schwer überschaubar. In den beiden führenden App-Stores (Google Play und Apples App-Store) zusammen wurden im August 2016 über 4,3 Millionen verschiedene Apps zum Download angeboten.[7] In Deutschland haben die meisten Smartphone-Nutzer bereits eine oder mehrere Apps installiert. Etwa zwei Drittel geben an, dass sie sogar zehn oder mehr Apps installiert haben.[8] Zu nahezu jedem beliebigen Thema sind Apps vorhanden: Wettervorhersage, Einkaufen, Terminplanung, Spielen, Aktienkurse, Gesundheit, Social Media, Bildung, Bücher, Tageszeitungen, Sport und derglei-

1 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

2 Bitkom (2016), S. 15.

3 Bitkom (2016), S. 15

4 Bitkom (2016), S. 19.

5 Initiative D21 (2016), S. 8-11 und 57.

6 IfD Allensbach (2016); Pfeiffenberger (2010), S. 14-18.

7 AppBrain/TechCrunch (2016).

8 ForwardAdGroup (2016).

chen mehr. Zwischen Juni 2015 und Juni 2016 wurden allein aus Apples App-Store etwa 30 Milliarden Apps heruntergeladen.[9] Mittlerweile stellen Apps einen enormen Wirtschaftsfaktor dar. So setzte Apple im Jahr 2016 24 Milliarden US-Dollar und Google 12 Milliarden US-Dollar mit dem Verkauf von mobilen Apps um.[10]

Sehr frühzeitig haben Bibliotheken, sowohl wissenschaftliche als auch öffentliche,[11] den Trend zum mobilen Internet erkannt und aufgegriffen. Als wichtige Diensteanbieter im Web in den Bereichen Information, Forschung und Wissenschaft sowie Bildung und Kultur müssen und wollen sie zentrale Angebote – wie den Online-Katalog, elektronische Datenbanken, E-Journals und E-Books, ihre digitalisierten Buch- oder Kartenbestände wie auch die virtuellen Auskunftsangebote – im mobilen Internet aktiv zur Verfügung stellen und die darin vorhandenen Chancen und Möglichkeiten für ihre Kunden nutzbar machen.[12] Der „NMC Horizon Report – Edition Bibliotheken", der kurz-, mittel- und langfristige Trends untersucht, an denen sich Bibliotheken strategisch ausrichten sollten, um im Informationsmarkt weiterhin bestehen zu können, nennt in seiner Ausgabe aus dem Jahr 2014 als kurzfristigen Trend und damit als Aufgabe für die nächsten ein bis zwei Jahre die Priorisierung von mobilen Inhalten und deren Bereitstellung: „Durch die verstärkte Nutzung mobiler Inhalte erwarten Nutzerinnen und Nutzer, Lehrende, Forscherinnen und Forscher sowie Studierende, auf Bibliotheksinhalte immer und überall zugreifen zu können. Um dieser steigenden Nachfrage zu entsprechen, integrieren Hochschul- und Forschungsbibliotheken mobile Optionen für ihre Inhalte und deren Bereitstellung in ihr Serviceangebot."[13] Eine besondere Rolle in Deutschland spielte in diesem Zusammenhang die Bayerische Staatsbibliothek in München. Seit 2010 stellt

---

9 Apple/TechCrunch (2016).

10 Statista (2017).

11 Unter wissenschaftlichen Bibliotheken werden im deutschen Bibliothekswesen traditionell diejenigen Bibliotheken verstanden, die dem wissenschaftlichen Studium, der Forschung und Lehre dienen (z.B. Universitätsbibliotheken, National- und Landesbibliotheken sowie wissenschaftliche Spezialbibliotheken). Davon abgegrenzt werden die öffentlichen Bibliotheken, die sich zumeist in kommunaler oder kirchlicher Trägerschaft befinden. Sie stehen der breiten Öffentlichkeit zur Verfügung und dienen in Abgrenzung zu wissenschaftlichen Bibliotheken in der Regel der allgemeinen Information, der Unterhaltung und der allgemeinen Bildung (z.B. Stadt- oder Gemeindebüchereien), Böttger (2009), S. 35; Gantert (2015), S. 9-13.

12 Ceynowa/Hermann (2013), S. 360.

13 Johnson/Adams-Becker/Estrada/Freeman (2014) S. 8.

sie sukzessive ihre wichtigsten netzbasierten Informationsdienste und vielfältigen digitalen Angebote auch in Form mobiler Applikationen bereit. Als eine der führenden Einrichtungen im Bereich der Digitalisierung hat sie – Ceynowa/Hermann zufolge – „[…] einige Angebote entwickelt, die auf paradigmatische Weise die Möglichkeit nutzen, die das mobile Internet für eine zeitgemäße Präsentation digitaler Kulturgüter bietet."[14]

1.1 Problemaufriss und Abgrenzung des Gegenstandsbereichs

Der zunehmende Verbreitungsgrad von mobilen Apps wirft zahlreiche Rechtsfragen auf, die aus den spezifischen Charakteristika mobiler Apps resultieren. Sie reichen von Besonderheiten bei der Gestaltung entsprechender Software-Entwicklungsverträge und Vertriebswege über urheberrechtliche und wettbewerbsrechtliche Problemstellungen bis hin zu Fragen der Haftung oder Umsatzsteuer.[15] Die vorliegende Arbeit konzentriert sich auf die datenschutzrechtlichen Aspekte. Smartphone- und Tablet-Nutzer speichern oft eine erhebliche Menge an personenbezogenen Daten (Adressdaten, Bankdaten, Standortinformationen, Fotos und Videos) auf ihren Geräten. Der Zugriff auf diese Daten ist für die installierten Apps relativ leicht und erfolgt vielfach ohne Zustimmung der Benutzer.[16] Deren Umgang mit den eigenen Daten oder auch den persönlichen Daten anderer, die auf dem mobilen Endgerät gespeichert sind (z.B. in Adressbüchern), ist in der Regel relativ leichtfertig. Bei Apps ist es um den Datenschutz und Datensicherheitsaspekte nicht gut bestellt. Verantwortlich sind hierfür mit Sicherheit auch Kostengründe, denn die Entwicklung hochwertiger Apps ist eine teure Angelegenheit. Wichtig ist den App-Anbietern zunächst einmal ein schickes Design und gutes Funktionieren der App.[17] Außerdem existiert eine Art Tauschtheorie, die von vielen App-Anbietern zumindest implizit vertreten wird. Dabei wird der Zugriff auf die personenbezogenen Daten und deren Nutzung durch das Unternehmen, das die App anbietet, regelmäßig als Ausgleich für das unentgeltliche Angebot der App angesehen.[18] Als größte Risiken für den Datenschutz lassen sich die fehlende Transparenz und die mangelnde Kenntnis der von einer App ausgeführten Verarbeitungen sowie das

[14] Ceynowa/Hermann (2013), S. 360.

[15] Hoffmann (2013), S. 632-635.

[16] Hladjk (2013), S. 92.

[17] Kramer (2014), S. 155.

[18] Kramer (2014), S. 155.

Fehlen einer expliziten Einwilligung der Benutzer vor der Verarbeitung identifizieren, ebenso unzureichende Sicherheitsmaßnahmen, ein offenkundiger Trend zur Datenmaximierung und die ungenaue Festlegung der Zwecke, für die personenbezogene Daten erfasst werden.[19]

Aufgrund des hohen Komplexitätsgrades datenschutzrechtlicher Fragestellungen muss eine Einschränkung vorgenommen werden. Im Mittelpunkt stehen Bibliotheks-Apps, also mobile Apps, die von Bibliotheken angeboten werden. Grundsätzlich gelten für Bibliotheks-Apps die gleichen datenschutzrechtlichen Anforderungen wie für Wetter-, Navigations-, Shopping- oder Spiele-Apps. Bei Bibliotheken muss allerdings berücksichtigt werden, dass es sich bei ihnen in der Regel um öffentliche Stellen im Sinne des § 2 des Bundesdatenschutzgesetzes (BDSG) handelt. Daher kann bei ihnen je nach Bibliotheksträger neben den bereichsspezifischen Gesetzen wie dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG) auch landesspezifisches Datenschutzrecht zu Anwendung kommen.

1.2 Relevanz des Themas

Wenn man die aktuelle Berichterstattung in der Presse etwas im Auge behält, wird schnell deutlich, welches Spannungsfeld sich zwischen Apps und Datenschutz auftut.[20] Da ist beispielsweise die Rede davon, dass Apple im Oktober 2015 mehr als 250 „Schnüffel"-Apps aus seinem App-Store entfernt hat. Es handelte sich dabei um Apps, die ein Software Development Kit (SDK) einer chinesischen Firma enthielten, mit dessen Hilfe ohne Wissen der Betroffenen Hunderttausende von privaten Daten wie E-Mail-Adressen, Gerätebezeichnungen, Adressen etc. gesammelt und zu Erstellung von Werbeprofilen an eben diese chinesische Firma gesandt wurden.[21] Zu zweifelhaftem Ruhm gelangte eine Taschenlampen-App für Android-Smartphones, die unerlaubt Daten über Aufenthaltsort und Geräteidentifikationsnummer der Nutzer speicherte und wiederum zu Werbezwecken an Dritte weiterleitete.[22] Die Prüfberichte des Bayerischen Landesamtes für Datenschutzaufsicht, das in den Jahren 2013 und 2014 jeweils 30 Apps aus dem nicht-öffentlichen Be-

[19] Artikel-29-Datenschutzgruppe (2013), S. 7.

[20] Haar (2013).

[21] Beiersmann (2015).

[22] Scherschel (2013); Odrich/Mörer-Funk (2013).

reich in datenschutzrechtlicher Hinsicht überprüft hatte,[23] kommen zu dem ernüchternden Ergebnis, dass es um den Datenschutz der nach dem Zufallsprinzip überprüften Apps nicht gut bestellt ist.[24] Der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Thomas Kranig, stellte resigniert fest: „Die schlechte datenschutzrechtliche Bewertung insbesondere der bayerischen iOS-Apps zeigt, dass die datenschutzrechtlichen Anforderungen durch bayerische App-Anbieter nicht ausreichend wahrgenommen werden. Für uns folgt hieraus, dass nach dieser eher allgemeinen Prüfung eine noch intensivere Prüfung von Apps nach den Maßstäben deutscher Datenschutzgesetze und eine Ahndung von Verstößen notwendig ist."[25]

Neben privatwirtschaftlichen Unternehmen bieten immer mehr öffentliche Stellen wie Ministerien, Städte und Gemeinden, Museen, Theater und Bibliotheken mobile Apps an. Die Bayerische Staatsbibliothek beispielsweise stellt ihren Nutzerinnen und Nutzern aktuell sieben mobile Apps zur Verfügung: 1) Famous Books, 2) Ludwig II. – Auf den Spuren des Märchenkönigs, 3) Bayern in historischen Karten, 4) Dichterwege – Auf den Spuren Jean Pauls, 5) Bavarikon3D, 6) Deutsche Klassiker in Erstausgaben, 7) BSB-Navigator.[26] Auch zahlreiche andere Bibliotheken, wie z.B. die Staatsbibliothek zu Berlin, Preußischer Kulturbesitz,[27] die Sächsische Landesbibliothek – Staats- und Universitätsbibliothek Dresden,[28] die Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft,[29] die Bibliothek der Hochschule der Medien in Stuttgart[30] oder die Bücherhallen Hamburg[31] haben mobile Apps in ihrem Dienstleistungsspektrum. Mit zunehmendem Verbreitungsgrad rücken auch die Apps öffentlicher Stellen vermehrt in den Fokus der entsprechenden Datenschutzaufsichtsbehörden. In ähnlicher Weise wie das Bayerische Landesamt für Datenschutzaufsicht ausgewähl-

---

23 Bayerisches Landesamt für Datenschutzaufsicht (2015), S. 29 und 51 f.

24 Bayerisches Landesamt für Datenschutzaufsicht (2013); Bayerisches Landesamt für Datenschutzaufsicht (2014); Reimer (2013), S. 549.

25 Bayerisches Landesamt für Datenschutzaufsicht (2014).

26 https://www.bsb-muenchen.de/recherche-und-service/apps/ (Letzter Zugriff: 15.02.2017).

27 http://staatsbibliothek-berlin.de/de/extras/allgemeines/mediathek/24-kulturschaetze-als-app/ (Letzter Zugriff: 15.02.2017).

28 https://www.slub-dresden.de/recherche/slub-app/ (Letzter Zugriff: 15.02.2017).

29 http://www.zbw.eu/de/recherchieren/econbiz-mobile/ (Letzter Zugriff: 15.02.2017).

30 https://www.hdm-stuttgart.de/bibliothek/angebot/Apps (Letzter Zugriff: 15.02.2017).

31 https://www.buecherhallen.de/app/ (Letzter Zugriff: 15.02.2017).

te Apps im nicht-öffentlichen Bereich überprüfte, begann beispielsweise der Bayerische Landesbeauftragte für den Datenschutz, der gemäß Art. 30 Abs. 1 BayDSG im Freistaat Bayern für die öffentlichen Stellen zuständig ist, im Jahr 2014 kontinuierlich mit der Überprüfung von Apps aus unterschiedlichen Bereichen der bayerischen Staatsverwaltung.[32]

1.3 Ziel der Arbeit

Vor dem Hintergrund der hohen Relevanz des Themas besteht das Ziel der vorliegenden Arbeit in der Analyse und systematischen Aufarbeitung der datenschutzrechtlichen Fragestellungen rund um mobile Bibliotheks-Apps sowie der Erarbeitung eines Praxisleitfadens für Bibliotheken. Dieser soll den mit der App-Entwicklung befassten Bibliotheksmitarbeiterinnen und -mitarbeitern praxisgerecht vermitteln, was aus datenschutzrechtlicher Sicht bei der Konzeption, der technischen Realisierung und dem Produktiveinsatz mobiler Bibliotheks-Apps zu beachten ist. Der Praxisleitfaden ist primär auf den Bibliotheksbereich ausgerichtet. Da es bisher keine vergleichbaren Handlungsempfehlungen gibt, können wesentliche Teile des Leitfadens auch von anderen Einrichtungen der öffentlichen Verwaltung nachgenutzt werden.

1.4 Bisherige wissenschaftliche Bearbeitung des Themas

Obwohl das Thema Datenschutz mittlerweile in der Mitte der bibliothekswissenschaftlichen Diskussion angekommen ist, sind Bibliotheks-Apps bisher noch nicht im datenschutzrechtlichen Kontext behandelt worden. Im Focus stehen eher grundsätzliche Fragen der Benutzerdatenverwaltung, des ASP-Providings und des Cloud-Computings sowie Fragen rund um die Web-Auftritte und Social Media-Aktivitäten von Bibliotheken.[33] Auch liegt kein Praxisleitfaden zur datenschutzkonformen Gestaltung von Bibliotheks-Apps vor. Jüngere bibliothekswissenschaftliche Arbeiten[34] setzen sich zwar durchaus mit mobilen Apps auseinander, aber eher unter den Aspekten der technischen Realisierung, des App-Designs, der Nützlichkeit und der Kundenorientierung. Rechtliche Fragen bleiben weitgehend ausgespart. Lediglich die im September

---

[32] Der Bayerische Landesbeauftragte für den Datenschutz (2015), S. 40.

[33] International Federation of Library Associations and Institutions (2015), S. 2-3; Katzenberger/Talke (2015), S. 684; Schmitz (2015), S. 697 f.; Nietzer (2015), S. 695; Nentwich (2015), S. 691-693; Deutscher Bibliotheksverband (2013), S. 1.

[34] Goltz (2014); Hennig (2014); Lehnard-Bruch (2012); Pohla (2011); Pfeifenberger (2010).

2015 in zweiter Auflage erschienene Studie „Mobile Applikationen für Bibliotheken im deutschsprachigen Raum“ von Julia Goltz gibt auf drei Seiten ein paar kurze Hinweise zum Thema Bibliotheks-Apps und Datenschutz.[35] In der rechts- und verwaltungswissenschaftlichen Literatur spielen Bibliotheks-Apps keine Rolle. Hier stehen Auseinandersetzungen mit mobilen Apps im Allgemeinen sowie im Kontext der Omnipräsenz mobiler Endgeräte im Mittelpunkt. Einen Aufsatz gibt es zum Thema mobile Apps der öffentlichen Verwaltung. Bei diesem wird bereits im Titel ein expliziter Bezug zum „Mobile Government“ (M-Government) hergestellt.[36]

1.5 Zur verwendeten Literatur

Die datenschutzrechtliche Auseinandersetzung mit mobilen Apps begann erst vor wenigen Jahren. Dennoch konnte bei der Anfertigung der vorliegenden Arbeit auf zahlreiche rechtswissenschaftliche Veröffentlichungen zurückgegriffen werden. Neben zwei größeren Abhandlungen[37] existieren mehrere Aufsätze in den einschlägigen Zeitschiften zum Datenschutz-, Internet- oder Multimediarecht. Selbst die Beacons-Technologie zur Navigation in geschlossenen Räumen (also dort, wo keine Signale von GPS-Satelliten empfangen werden können) ist bereits Gegenstand rechtswissenschaftlicher Bearbeitung geworden. Auch die aktuellsten Ausgaben der datenschutzrechtlichen Kommentare und Handbücher enthalten vereinzelt Informationen zur App-Thematik. Entsprechende Gerichtsurteile liegen dahingegen noch nicht vor. Dafür gibt es mehrere Empfehlungen deutscher Datenschutzbehörden und solcher der Europäischen Union. Zu nennen sind hier die Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter des „Düsseldorfer Kreises“,[38] eines Zusammenschlusses der deutschen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, sowie die Stellungnahmen der „Artikel-29-Datenschutzgruppe“.[39] Diese ist ein unabhängiges Beratungsgremium der Europäischen Union in Datenschutzfragen und wurde gemäß Artikel

---

[35] Goltz (2015), S. 13-15. In der ersten Auflage der Studie, Goltz (2014), fand der Datenschutz noch keinerlei Erwähnung.

[36] Hoffmann (2013).

[37] Baumgartner/Ewald (2016); Solmecke/Taeger/Feldmann (2013).

[38] Düsseldorfer Kreis (2014).

[39] Artikel-29-Datenschutzgruppe (2011); Artikel-29-Datenschutzgruppe (2013).

29 der EU-Datenschutzrichtlinie 95/46/EG eingesetzt.[40] Die Empfehlungen und Stellungnahmen sind zwar nicht rechtlich bindend, aber sie zeigen, in welche Richtung sich die maßgeblichen Datenschutzinstitutionen bewegen und wie sie gegebenenfalls ihre Aufsichts- und Kontrolltätigkeit gestalten werden.[41]

[40] Taeger (2014), Kap. I Rn. 31.

[41] Lober/Falker (2013), S. 361.

2 Präzisierung des Untersuchungsgegenstandes

2.1 Mobile Apps: Begriffsbestimmung und Charakteristika

Der Begriff „App" ist eine deutsche Kurzform von „Applikation" bzw. eine englische Kurzform von „application", womit zunächst jegliche Art von Anwendungsprogramm gemeint ist.[42] Im Deutschen hat der Begriff mittlerweile eine Bedeutungsverengung erfahren und wird vor allem für kleine Computerprogramme verwendet, die auf mobilen Endgeräten wie Smartphones und Tablet-Computer laufen.[43] Sie unterscheiden sich von klassischen Anwendungsprogrammen für Desktopgeräte dadurch, dass in der Entwicklung und im Betrieb den besonderen Eigenschaften mobiler Endgeräte, beispielsweise einer geringeren Hardwareausstattung, kleinen Displayformaten sowie beschränkten Eingabemöglichkeiten, Rechnung getragen wird.[44] Mobile Apps haben den Sinn, den Funktionsumfang mobiler Geräte, die in einer Basisausfertigung geliefert werden, zu erweitern.[45] Ein wichtiges Charakteristikum mobiler Apps ist dabei ihre enge Verknüpfung mit dem jeweiligen mobilen Betriebssystem wie Apple iOS oder Google Android[46] sowie ihre zentrale Vermarktung über die plattformeigenen App-Stores als zentrale Marktplätze.[47]

Durch die enge Verzahnung mit dem mobilen Betriebssystem können Apps relativ problemlos viele Daten und Funktionalitäten des mobilen Geräts – wie Kontakte aus dem Adressbuch, Fotos, Videos, Standortdaten, verschiedene Sensordaten – erfassen und verarbeiten.[48] Neben den zweifelsohne sehr attraktiven Möglichkeiten und innovativen Diensten, die den App-Nutzern damit geboten werden können, liegt darin aber auch ein im Vergleich zur Internetbenutzung über herkömmliche PCs deutlich erhöhtes Missbrauchsrisiko, wenn eine App neben ihrer eigentlichen Funktionalität beispielsweise unbemerkt die persönlichen Kontakte ausliest und auf einen Server im Ausland überträgt, als digitale „Wanze"

---

42 Maske (2012), S. 106; Marly (2014), Rn. 1157.

43 Ewald, in: Baumgartner/Ewald (2016), Rn. 1; Denker/Hartl/Denker, in: Solmecke/Taeger/Feldmann (2013), Kap. 1, Rn. 14.

44 Maske (2012), S. 107.

45 Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 1; Ewald, in: Baumgartner/Ewald (2016), Rn. 2; Tinnefeld/Buchner/ Petri (2012), S. 419.

46 Schneider (2012), S. 297.

47 Ewald, in Baumgartner/Ewald (2016), Rn. 1; Denker/Hartl/Denker, in: Solmecke/Taeger/Feldmann (2013), Kap. 1, Rn. 14.

48 Artikel-29-Datenschutzgruppe (2013), S. 6.

Gespräche mitschneidet oder mit Hilfe von Standortdaten unerlaubt Bewegungsprofile erstellt.[49] Ein hohes Risiko für den Datenschutz besteht auch aufgrund der zahlreichen Beteiligten im Umfeld der Entwicklung und des Vertriebs von Apps.[50] Zu diesen Beteiligten, zwischen denen ein vielfältiges, manchmal schwer durchschaubares Geflecht unterschiedlicher Vertragsbeziehungen besteht,[51] gehören neben dem Endnutzer und dem App-Anbieter, die App-Entwickler, die Hersteller der mobilen Betriebssysteme mit ihren zentralen Vertriebsplattformen (App Stores) sowie andere Dritte, die an der Erbringung der von der App bereitgestellten Dienstleistung oder an der Erfassung und Verarbeitung personenbezogener Daten beteiligt sind (z.B. Content-Lieferanten oder Anbieter von Analyse- und Werbedienstleistungen).[52] Zu einem besseren Überblick über die Beteiligten und die Vertragsbeziehungen, die sie verbinden, soll folgende Darstellung beitragen:

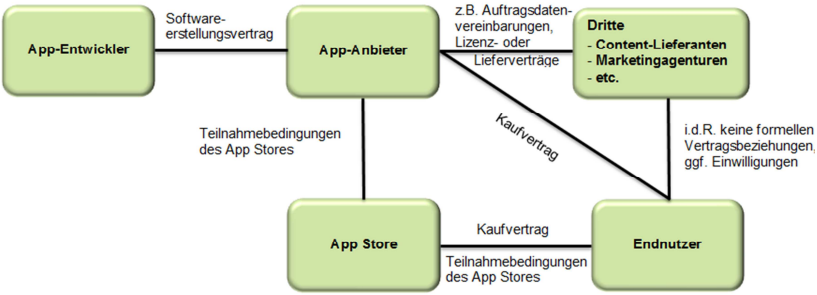

Abbildung 1: Beteiligte im App-Kontext mit Vertragsbeziehungen[53]

2.2 Kategorisierung mobiler Apps: Native Apps und Web-Apps

Mobile Apps im gerade vorgestellten Sinne bezeichnet man als native mobile Apps. Sie heißen nativ, da sie speziell für eine entsprechende

[49] Sachs/Meder (2013), S. 303.

[50] Artikel-29-Datenschutzgruppe (2013), S. 2.

[51] Lachenmann, in: Solmecke/Taeger/Feldmann (2013), Kap. 3, Rnn. 1-7; Marly (2014), Rn. 1168-1178.

[52] Ewald, in: Baumgartner/Ewald (2016), Rnn. 11 f.; Marly (2014), Rn. 1162.

[53] Eigene Darstellung in Anlehnung an Baumgartner, in: Baumgartner/Ewald (2016), Rn. 188.

Zielplattform programmiert wurden und nur dort lauffähig sind.[54] Native Apps werden mit einer Programmiersprache – iPhone-Apps hauptsächlich in Objective-C und Android-Apps in Java – programmiert, mit einem Compiler in einen ausführbaren Code übersetzt und direkt auf dem jeweiligen Betriebssystem des mobilen Geräts ausgeführt.[55] Da native Apps plattformspezifisch implementiert sind, ist sichergestellt, dass alle Schnittstellen zur Hardware einheitlich funktionieren und die Ressourcen des Geräts optimal genutzt werden.[56] Außerdem kann das plattformtypische Look-and-Feel sehr gut umgesetzt werden. Die App fühlt sich dadurch für einen mit der Plattform vertrauten Benutzer sehr intuitiv an, während ein plattformfremder Benutzer sich erst mit der Handhabung vertraut machen muss.[57] Ein wesentlicher Nachteil nativer Apps besteht darin, dass ein Anbieter die App für jedes Betriebssystem getrennt entwickeln muss.[58] Hierdurch ergibt sich ein hoher finanzieller Aufwand.

Von den nativen mobilen Apps unterscheidet man Web-Apps. Darunter versteht man eine speziell programmierte HTML5-Website, die nicht selbstständig lauffähig ist, sondern deren Inhalt im Internet-Browser eines Mobilgeräts dargestellt wird.[59] Web-Apps sind Webseiten, die nativen Apps von der äußeren Erscheinung her durchaus ähneln, in ihrer Funktionalität aber deutlich eingeschränkt sind. Dies betrifft insbesondere die Verwendung der Geräte-Hardware, also beispielsweise der Kamera, des GPS-Empfängers oder der Bewegungssensoren.[60] Um den nativen Apps vom Look-and-Feel her möglichst nahe zu kommen, müssen Web-Apps so programmiert sein, dass sie sich besonders gut in mobilen Browsern bzw. auf kleinen Displays darstellen lassen. Wichtig ist in diesem Fall die Berücksichtigung von Ansätzen des Responsive Webdesign. Dies bedeutet, dass die aufgerufene Website zunächst feststellt, welche Displaygröße bzw. -auflösung auf dem Zielgerät vorliegt, und dementsprechend die optimale Darstellungsweise auswählt. Web-Apps sind also grundsätzlich nichts anderes als für mobile Endgeräte optimierte Web-

---

54 Hildebrandt/Luthiger/Stamm/Yereaztian (2012), S. 27.

55 Hildebrandt/Luthiger/Stamm/Yereaztian (2012), S. 27; Sachs/Meder (2013), S. 303.

56 Marly (2014), Rn. 1159.

57 Hildebrandt/Luthiger/Stamm/Yereaztian (2012), S. 27.

58 Marly (2014), Rn. 1159.

59 Marly (2014), Rn. 1159; Sachs/Meder (2013), S. 303.

60 Ewald, in: Baumgartner/Ewald (2016), Rn. 3; Hildebrandt/Luthiger/Stamm/Yereaztian (2012), S. 29 f.

seiten.[61] Web-Apps haben gegenüber nativen Apps den großen Vorteil, dass sie plattformunabhängig sind. Sie funktionieren auf jedem Smartphone oder Tablet-Computer, egal mit welchem Betriebssystem es ausgestattet ist. Voraussetzung ist lediglich ein mobiler Internet-Browser.[62]

Wenn in der vorliegenden Arbeit von Apps die Rede ist, dann sind damit immer native Apps gemeint. Web-Apps werfen keine datenschutzrechtlich relevanten Problemstellungen auf, die sich in spezifischer Weise von denen klassischer Webseiten unterscheiden würden.

2.3 Mobile Apps und M-Government

Vor dem Hintergrund der großen Verbreitung und hohen Beliebtheit mobiler Apps ist es nicht verwunderlich, dass auch zahlreiche öffentliche Institutionen und Körperschaften wie Gemeinden, Städte, Ministerien, Universitäten, Museen, Theater und Bibliotheken bemüht sind, von diesem Trend zu profitieren und sich die Vorteile mobiler Apps im Bereich des E-Government zunutze zu machen. In Analogie zum Begriff der mobilen App spricht man in diesem Zusammenhang auch gerne vom „Mobile Government" bzw. M-Government.[63] Klingt es nicht verlockend, den Bürgerinnen und Bürgern zentrale Verwaltungsdienstleistungen oder Bildungsangebote orts- und zeitunabhängig auf den so beliebten mobilen Endgeräten anbieten zu können? Was läge da näher, als entsprechende mobile Apps zu programmieren und in den jeweiligen App-Stores zum Download anzubieten? Mittlerweile hat sich für diese Apps der öffentlichen Verwaltung eine eigene Bezeichnung eingebürgert: Government-Apps oder kurz GovApps. Ein entsprechendes Projekt des Bundes sollte dazu beitragen, die Entwicklung dieser Apps zu fördern und bestimmte Qualitätsstandards zu etablieren. Das Projekt ist mittlerweile abgelaufen und es ist etwas ruhiger um die GovApps geworden.[64] Der „eGovernment Monitor 2015" zeigt aber eindeutig, dass bei den Bürgerinnen und Bürgern eine deutliche Nachfrage nach Anwendungen besteht, die an die Charakteristika mobiler Endgeräte angepasst sind und mit denen zentrale Dienstleistungen der öffentlichen Verwaltung auf den

---

[61] Goltz (2015), S. 8.

[62] Denker/Hartl/Denker, in: Solmecke/Taeger/Feldmann (2013), Kap. 1, Rn. 29; Marly (2014), Rn. 1159.

[63] Hoffmann (2013), S. 631.

[64] http://www.oeffentliche-it.de/govapps (Letzter Zugriff: 15.02.2017).

drei Interaktionsstufen Information, Kommunikation und Transaktion komfortabel genutzt werden können.[65]

2.4 Bibliotheks-Apps: Begriffsbestimmung und Zweck

Bibliotheks-Apps sind typische Vertreter nativer mobiler Apps. Sie werden auch als bibliothekarische Apps oder mobile Applikationen für Bibliotheken bezeichnet.[66] Bibliotheken stellen mit ihnen ihre wesentlichen Dienstleistungen und digitalen Bestände in moderner und kundenorientierter Weise zur Verfügung. Damit verfolgen sie folgendes Ziel: „Unsere Nutzer wollen Information schnell, unkompliziert und integriert in ihren (mobilen) Alltag. Sie sind mobil unterwegs und erhalten durch (gut gemachte und funktionierende) Applikationen auf ihrem Smartphone oder anderen mobilen Geräten die in der jeweiligen Alltagssituation benötigte Information in kürzester Zeit. Wenn Bibliotheken ihre Nutzer nicht an andere Anbieter verlieren wollen, müssen sie ‚ihren' Content mobil anbieten."[67] Für Bibliotheken stellt sich bei der App-Entwicklung regelmäßig folgendes Problem: Da Bibliotheken als öffentliche Einrichtung ihre Angebote selbstverständlich einem möglichst breiten Kundenkreis zur Verfügung stellen möchten, dürfen keine Benutzer aufgrund des mobilen Betriebssystems ihres mobilen Endgeräts benachteiligt werden. Als native Apps müssen Bibliotheks-Apps allerdings für jedes Betriebssystem getrennt entwickelt werden, in der Realität also zumindest für iOS und Android als den beiden verbreitetsten Betriebssystemen. Dadurch entstehen hohe Kosten, die in der Regel nur von größeren Bibliotheken geschultert werden können.

Mittlerweile gibt es eine beachtliche Anzahl verschiedener Bibliotheks-Apps, die sich nicht nur inhaltlich, sondern auch bezüglich der Qualität der technischen Umsetzung, der Anwenderfreundlichkeit und der Nützlichkeit zum Teil deutlich unterscheiden. Pohla (2011) und Goltz (2015) geben in ihren Arbeiten einen guten Überblick über das momentan verfügbare Angebot.[68] Als bibliothekarische Dienstleistungen, die über mo-

---

65 Initiative D21 (2015), S. 28-31.

66 Pohla (2010) spricht in seiner Darstellung regelmäßig von „bibliothekarischen Apps", während Goltz (2015) den Ausdruck „mobile Applikation für Bibliotheken" verwendet.

67 Goltz (2015), S. 3.

68 Pohla (2011), S. 75-77; Goltz (2015), S. 28-32.

bile Apps angeboten werden, lassen sich im Wesentlichen folgende identifizieren:[69]

- Recherche im Bibliothekskatalog (OPAC) mit Integration von Bibliotheksdatenbanken und externen Quellen
- Benutzerkontoverwaltung, Benachrichtigungsservice
- Zugang zu Unterrichts- und/oder Forschungsmaterialien
- Zugang zu Lernorten, freien Rechnerkapazitäten und Gruppenräumen
- Informationen zur Bibliothek und zu Ansprechpartnern
- Neuerwerbungslisten
- Veranstaltungen mit Kalenderfunktion
- Wissensvermittlung, Lernvideos, Bibliotheksvideos
- Navigation (durch die Räumlichkeiten der Bibliothek)
- Präsentation von digitalem Content (digitalisierte Handschriften und wertvolle Drucke,[70] digitalisierte Erstausgaben,[71] 3D-Virtualisierung hochrangiger Kunst- und Kulturobjekte[72])
- Angebot von Location Based Services[73]

2.5 Beispiele für Bibliotheks-Apps

Exemplarisch sollen zwei Bibliotheks-Apps kurz vorgestellt werden, die sich hinsichtlich des angebotenen Dienstleistungsspektrums deutlich unterscheiden:

a) Bibliotheks-App der Hochschule der Medien, Stuttgart

Die Bibliotheks-App der Hochschule der Medien ist sowohl für den App-Store von Google als auch für den von Apple verfügbar. Sie bün-

---

[69] Pohla (2011), S. 43-64; Goltz (2015), S. 10; Ceynowa/Hermann (2013), S. 360-363.

[70] Z.B. die Apps der Bayerischen Staatsbibliothek: „*Famous Books*“ https://www.bsb-muenchen.de/recherche-und-service/apps/famous-books (Letzter Zugriff: 15.02.2017) und „*Pracht auf Pergament*“: https://www.bsb-muenchen.de/recherche-und-service/apps/pracht-auf-pergament (Letzter Zugriff: 15.02.2017).

[71] Z.B. die App „*Deutsche Klassiker in Erstausgaben*“ der Bayerischen Staatsbibliothek: https://www.bsb-muenchen.de/recherche-und-service/apps/deutsche-klassiker (Letzter Zugriff: 15.02.2017).

[72] Z.B. die App „*bavarikon3D*“ der Bayerischen Staatsbibliothek: https://www.bsb-muenchen.de/recherche-und-service/apps/bavarikon3d (Letzter Zugriff: 15.02.2017).

[73] Z.B. die Apps „*Ludwig II. – Auf den Spuren des Märchenkönigs*“: https://www.bsb-muenchen.de/recherche-und-service/apps/ludwig-ii (Letzter Zugriff: 15.02.2017) und „*BSB-Navigator*“: https://www.bsb-muenchen.de/recherche-und-service/apps/bsb-navigator/ (Letzter Zugriff: 15.02.2017).

delt klassische Bibliotheksdienstleistungen wie Bibliothekskatalog (OPAC),[74] Bestellfunktion und Benutzerkontoverwaltung, ebenso bietet sie Informationen zu Öffnungszeiten, Medienstandorten und Ansprechpartnern, außerdem einen Wegweiser durch die Gebäude der Bibliothek mit Anzeige von Lesesälen, Schulungsräumen und Gruppenarbeitsräumen.[75]

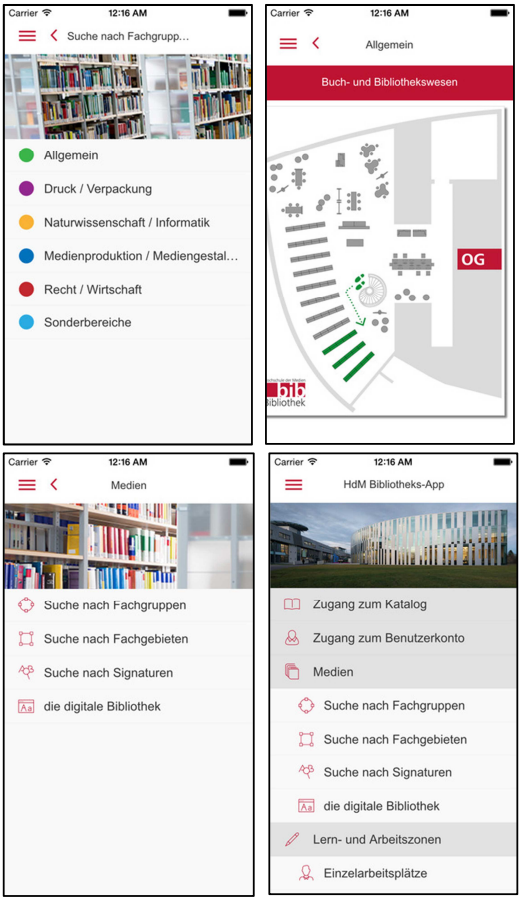

Abbildung 2: Screenshots der Bibliotheks-App der Hochschule der Medien, Stuttgart[76]

[74] OPAC: Online Public Access Catalogue.

[75] https://www.hdm-stuttgart.de/bibliothek/angebot/Apps (Letzter Zugriff: 15.02.2017).

b) App „Ludwig II. – Auf den Spuren des Märchenkönigs“ der Bayerischen Staatsbibliothek

Die Location-Based-Services-App „Ludwig II. – Auf den Spuren des Märchenkönigs“ präsentiert eine Vielfalt multimedialer Informationen zu König Ludwig II. von Bayern. Sie ist ein Angebot der Bayerischen Staatsbibliothek in Kooperation mit der der Bayerischen Verwaltung der staatlichen Schlösser, Gärten und Seen. Nahezu alle Inhalte sind auch offline nutzbar. Die App umfasst folgende Dienste (in Auswahl):[77]

- Informationen zu 140 Locations in Bayern und Europa mit Bezug zu König Ludwig II.; diese können live in das Kamerabild des iPhones eingeblendet bzw. per Karten- oder Listenansicht erschlossen werden
- Ausführliche, multimedial angereicherte Beschreibungen der wichtigsten Orte im Leben des Königs
- Umfangreiche Bildergalerien mit mehr als 400 – oft historischen – Fotos
- Gesprochene Zeitzeugenzitate, z.B. von Richard Wagner und Otto von Bismarck; diese vermitteln einen lebendigen Eindruck, wie Personen aus Ludwigs Umfeld den König erlebten
- Hörbilder zu besonderen Themen und Orten, u.a. zur Baugeschichte von Schloss Neuschwanstein
- Orts- und kontextbezogen verlinkte Experten-Videointerviews zu den Themen Architektur, Politik, Musik, Technik, Leben und Mythos Ludwigs II.
- Augmented-Reality-Simulation des berühmten, heute nicht mehr existenten Wintergartens Ludwigs II. in der Münchner Residenz in Echtzeit im Kamerabild des iPhones
- 360-Grad-Panoramaansicht des Thron- und Sängersaals von Schloss Neuschwanstein, ebenfalls als Augmented-Reality-Feature

---

[76] https://itunes.apple.com/de/app/hdm-bibliotheks-app/id1018167442?mt=8 (Letzter Zugriff: 15.02.2017).

[77] https://www.bsb-muenchen.de/recherche-und-service/apps/ludwig-ii (Letzter Zugriff: 15.02.2017).

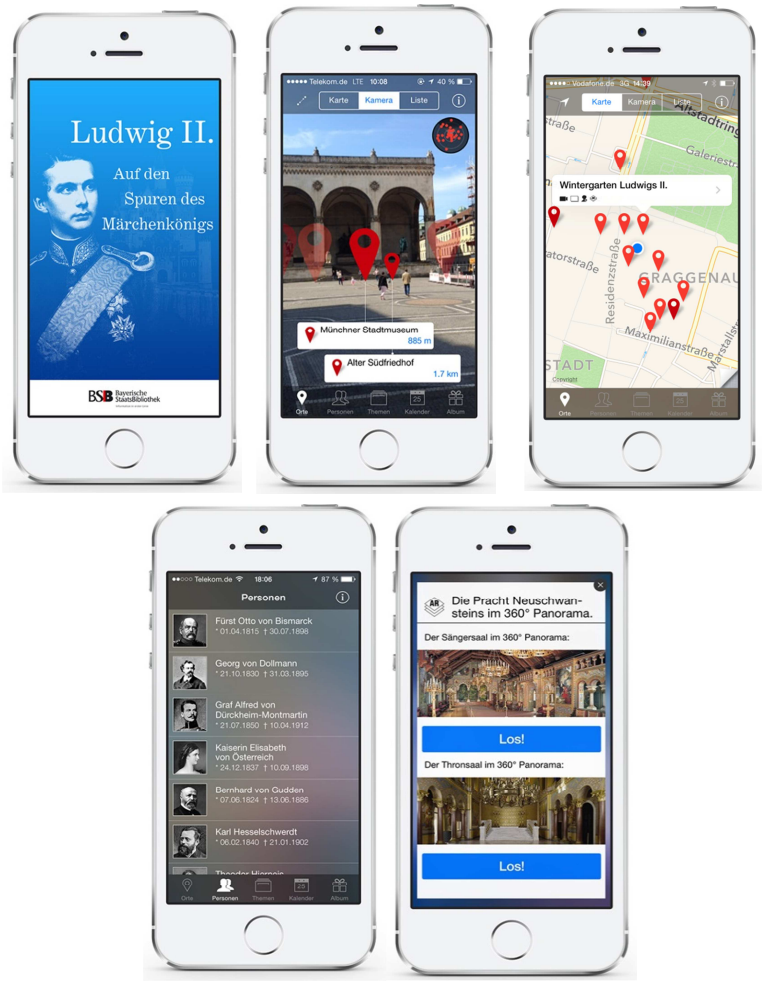

Abbildung 3: Screenshots der App „Ludwig II. – Auf den Spuren des Märchenkönigs“[78]

[78] https://www.flickr.com/photos/marissabergbahn/albums/72157645583614191 (Letzter Zugriff: 15.02.2017).

3 Datenschutzrechtliche Analyse

Bibliotheks-Apps unterscheiden sich nicht in spezifischer Weise von den mobilen Apps anderer Anbieter. Aus diesem Grund wird im Folgenden nicht ausschließlich der Begriff Bibliotheks-Apps verwendet, sondern oft ganz einfach die Begriffe App oder mobile App. Das allermeiste, das in datenschutzrechtlicher Hinsicht für die mobilen Apps kommerzieller Anbieter gilt, kann auch auf Bibliotheks-Apps angewendet werden. Wie bereits erwähnt, besteht dahingehend eine Besonderheit, dass Bibliotheks-Apps von Bibliotheken und damit von öffentlichen Anbietern verantwortet werden. Auf die jeweiligen Konsequenzen wird an den relevanten Stellen eingegangen.

3.1 Datenschutz als Persönlichkeitsrecht und europarechtlicher Bezugsrahmen

Sowohl das internationale als auch das nationale Datenschutzrecht verfolgen das Ziel, den Einzelnen vor der Verletzung seiner Privatsphäre durch den Umgang mit ihn betreffenden Daten zu schützen. Der Begriff des Datenschutzes ist dabei durchaus missverständlich. Er suggeriert, dass es primär um den Schutz von Daten ginge. Allerdings steht beim Datenschutz der Schutz desjenigen im Mittelpunkt, den die Daten betreffen. Datenschutz ist damit vor allem Betroffenenschutz bzw. Schutz des Persönlichkeitsrechts.[79] Eine besondere Ausprägung dieses Persönlichkeitsrechts ist das Grundrecht auf informationelle Selbstbestimmung. Dieses im so genannten „Volkszählungsurteil“ (15.12.1983)[80] vom Bundesverfassungsgericht aus Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG entwickelte Grundrecht, das auch als Datenschutz-Grundrecht bezeichnet wird, besagt, dass jeder Mensch grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen darf.[81]

Die rechtliche Gewährleistung des Datenschutzes ist keine rein nationale Aufgabe.[82] Aufgrund der grenzüberschreitenden Übermittlung personenbezogener Daten im Internet und der zunehmenden Entgrenzung der Welt im Zuge der Globalisierung muss diese Aufgabe immer mehr auf der internationalen Ebene geleistet werden, um wirksam zu sein. Das

---

79 Taeger (2014), Kap. III Rn. 29; Comans (2012), S. 29; Bodenschatz (2010), S. 19.

80 BVerfG, Urteil vom 15.12.1983, Az 1 BvR 209/83, in: BVerfGE 65, 1.

81 Kühling/Seidel/Sivridis (2015), Rn. 151; Tinnefeld/Buchner/ Petri (2012), S. 97-101.

82 Taeger (2014), Kap. I Rn. 1.

deutsche Datenschutzrecht steht dabei im Kontext des Rechts der Europäischen Union (EU) und ist maßgeblich von diesem geprägt.[83]

Die primärrechtlichen Grundlagen des europäischen Datenschutzrechtes finden sich in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union (GRC). Art. 7 GRC normiert das Recht auf Achtung des Privatlebens und der Kommunikation.[84] Art. 8 GRC ist als *lex specialis* zu Art. 7 GRC zu verstehen und normiert explizit ein Grundrecht auf Datenschutz. In den sachlichen Schutzbereich von Art. 8 GRC fallen personenbezogene Daten, d.h. alle Informationen über eine bestimmte oder bestimmbare Person.[85] Die Verarbeitung personenbezogener Daten stellt einen Eingriff in Art. 8 GRC dar. Verarbeitung ist hier als Oberbegriff für sämtliche Datenverarbeitungsschritte von der Erhebung über die Weitergabe bis hin zur Löschung personenbezogener Daten zu verstehen. Jeder Eingriff in das Grundrecht auf Datenschutz ist rechtfertigungsbedürftig.[86] Im Bereich des sekundären EU-Rechts war insbesondere die allgemeine Datenschutzrichtlinie 95/46/EG[87] (DSRL) vom 24.10.1995 für die Thematik der vorliegenden Arbeit von Bedeutung. Sie galt als das zentrale Element der Datenschutzvorschriften auf Unionsebene und bildete das Fundament des Datenschutzrechts in den EU-Mitgliedstaaten.[88] Mit der Transformation in nationales Recht sollte ein einheitlicher Rechtsrahmen für die Verarbeitung personenbezogener Daten im europäischen Binnenmarkt und ein einheitliches Schutzniveau in den Mitgliedstaaten erreicht werden.[89] Dieses Ziel wurde aber nur unzureichend verwirklicht. Die Praxis zeigte vielmehr, „[…] dass innerhalb der EU mitnichten von einer ‚Vollharmonisierung' des Datenschutzrechts infolge der EU-Datenschutzrichtlinie gesprochen werden kann."[90] Große Hoffnungen werden diesbezüglich auf die EU-Datenschutz-Grundverordnung (EU-DSGVO) gesetzt, die künftig den Rahmen für den europäischen Datenschutz bilden wird. Die am europäischen Ge-

---

83 Kühling/Seidel/Sivridis (2015), Rn. 50.

84 Oppermann/Classen/Nettesheim (2014), § 17 Rn. 50 f.

85 Bodenschatz (2010), S. 31; Kühling/Seidel/Sivridis (2015), Rn. 42.

86 Kühling/Seidel/Sivridis (2015), Rnn. 44 f.; Comans (2012), S. 79-82; Bodenschatz (2010), S. 86.

87 RL 95/46/EG, Abl. EG 1995, L 281, 31.

88 Hijmans/Langfeldt (2012), S. 404; Brennscheidt (2013), S. 47.

89 Taeger (2014), Kap. I Rn. 28; Comans (2012), S. 84.

90 Baumgartner, in: Baumgartner/Ewald (2016), Fußnote 194.

setzgebungsprozess beteiligten Institutionen (EU-Kommission, EU-Parlament und EU-Ministerrat) einigten sich am 15.12.2015 im Rahmen des so genannten Trilogs auf eine gemeinsame Textfassung, die – nach Verabschiedung im EU-Ministerrat und Billigung durch das Plenum des EU-Parlaments – am 27.04.2016 verabschiedet und am 04.05.2016 im Amtsblatt der Europäischen Union veröffentlicht wurde.[91] 20 Tage später, also am 25.05.2016, trat sie in Kraft und wird nach einer zweijährigen Übergangszeit am 25.05.2018 sowohl für den öffentlichen als auch für den privaten Bereich mit Anwendungsvorrang vor den nationalen Datenschutzvorschriften anzuwenden sein.[92] Die EU-DSGVO stellt sich „[…] der Herausforderung, ein (zumindest weitgehend) harmonisiertes und effektives europäisches Datenschutzniveau auf den Weg zu bringen, das den digitalen Rahmenbedingungen des 21. Jahrhunderts gewachsen ist."[93] Bisher ist allerdings nur in Ansätzen absehbar, welche unmittelbaren Rechtswirkungen mit ihr tatsächlich verbunden sein werden.[94] Kühling/Martini et al. (2016) führen hierzu aus: „Dem Ende des unionalen Gesetzgebungsprozesses wohnt ein nicht weniger bedeutender Anfang eines Anpassungsprozesses auf nationaler Ebene inne. Die Verordnung setzt das nationale Datenschutzrecht nachhaltigen Umwälzungen aus. […] Mit rund vier Dutzend Öffnungsklauseln belässt sie den Mitgliedstaaten reichlich normativen Gestaltungsspielraum für eigene Regelungen. Das gilt für Regelungen im allgemeinen und bereichsspezifischen Datenschutzrecht […]. Welche Vorschriften des allgemeinen und bereichsspezifischen deutschen Datenschutzrechts bestehen bleiben können, welche zu modifizieren sind und welcher zusätzlichen Vorschriften es bedarf, um den Anforderungen der Datenschutz-Grundverordnung gerecht zu werden, ist gegenwärtig noch offen."[95] Aufgrund dieser Unwägbarkeiten konnten die bevorstehenden rechtlichen Anpassungen in der vorliegenden Arbeit noch nicht berücksichtigt werden.

---

[91] Der offizielle Text der EU-DSGVO findet sich unter folgendem Link: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=de (Letzter Zugriff: 15.02.2017).

[92] Taeger/Rose (2016), 819; Gierschmann (2016), S. 51; Herdegen (2015), § 8 Rn. 40; Oppermann/Classen/Nettesheim (2014), § 9 Rn. 78-80; Kühling/Martini (2016), S. 448.

[93] Kühling/Martini et. al. (2016), S. 1.

[94] Baumgartner, in: Baumgartner/Ewald (2016), Rnn. 363-368; Albrecht (2016), S. 88-98; Gierschmann (2016), S. 51-55; Taeger/Rose (2016), S. 819-831; Roßnagel (2016), S. 553.

[95] Kühling/Martini et al. (2016), S. 1 f.

3.2 Anwendbarkeit des deutschen Datenschutzrechts

Als datenschutzrechtliche Regelungen kommen im Wesentlichen das Bundesdatenschutzgesetz (BDSG), die Landesdatenschutzgesetze sowie die bereichsspezifischen Regelungen des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) in Betracht.

3.2.1 Bundesdatenschutzgesetz und Landesdatenschutzgesetze

Die Frage der Anwendbarkeit der deutschen Datenschutzgesetze ist bezogen auf die Apps nicht-öffentlicher Anbieter mitunter ausgesprochen schwer zu beantworten. Die Literatur hält hierzu eine Fülle von Kriterien und Fallbeispielen bereit.[96] Die Schwierigkeit liegt darin, dass Unternehmen, die Apps anbieten, oft mehrere Niederlassungen haben – in Deutschland, innerhalb der EU, im EWR-Raum oder außerhalb des EWR-Raumes – und dass nicht ohne Weiteres klar ist, welchem nationalen Datenschutzregime eine bereitgestellte App unterworfen ist. Diese keinesfalls als abgeschlossen zu bezeichnende Diskussion kreist um die Anwendung des Territorialprinzips oder des Sitzprinzips, die bei multinationalen Konzernen sehr komplex ist.[97] Im Fall der mobilen Apps deutscher Bibliotheken stellt sich die Lage wesentlich einfacher dar. Der entscheidende Punkt ist die Frage, wo die für die Datenerhebung und -verarbeitung verantwortliche Stelle[98] ihren Sitz hat. Fungiert eine deutsche Bibliothek als App-Anbieter, was bei Bibliotheks-Apps in aller Regel der Fall sein dürfte, dann ist nach dem Territorialprinzip unproblematisch das BDSG anzuwenden,[99] was das BDSG in der Kollisionsnorm § 1 Abs. 5 im Übrigen wegen des fehlenden Auslandsbezugs als Selbstverständlichkeit gar nicht explizit erwähnt.[100]

Für die App-Thematik sind insbesondere die ersten drei Abschnitte des BDSG von Bedeutung. Der erste Abschnitt („Allgemeine und gemeinsame Bestimmungen“) gilt sowohl für öffentliche als auch für nicht-

[96] Lober/Falker (2013), S. 358 f.; Sachs/Meder (2013), S. 303 f.; Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 22-33; Baumgartner, in: Baumgartner/Ewald (2016), Rnn. 193-297; Düsseldorfer Kreis (2014), S. 4.

[97] Gola/Schomerus (2012), § 1 Rnn. 27-31; Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 28 und 31; Baumgartner, in: Baumgartner/Ewald (2016), Rn. 194 und 196; Kühling/Seidel/Sivridis (2015), Rn. 272 f.

[98] Der Begriff der verantwortlichen Stelle wird weiter unten noch ausführlicher behandelt.

[99] Lober/Falker (2013), S. 358.

[100] Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 28.

öffentliche Stellen. Im zweiten („Datenverarbeitung der öffentlichen Stellen“) und dritten Abschnitt („Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen“) findet dann eine Differenzierung statt, auf die § 2 BDSG bereits hinweist.[101] Unter dem Begriff der öffentlichen Stelle wird gemäß § 2 Abs. 1 und 2 BDSG der gesamte Bereich der Betätigung der öffentlichen Hand verstanden, also die Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen ungeachtet ihrer Rechtsform.[102] Bibliotheken fallen eindeutig unter diesen Begriff, es sei denn, es handelt sich um Privat- oder Firmenbibliotheken oder kirchliche Bibliotheken.[103] Öffentliche Stellen der Länder gelten gemäß § 1 Abs. 2 BDSG nur insofern als Normadressaten des BDSG, als der Datenschutz nicht durch Landesrecht geregelt ist. Da aber jedes Bundesland ein eigenes Landesdatenschutzgesetz erlassen hat, verbleibt diesbezüglich kein Anwendungsbereich des BDSG. Für die öffentlich-rechtlich organisierten Einrichtungen der Länder, Gemeinden und Gemeindeverbände greifen vielmehr die jeweiligen Landesdatenschutzgesetze.[104] Auf den Bibliotheksbereich bezogen bedeutet dies, dass z.B. für die Staatsbibliothek zu Berlin – Preußischer Kulturbesitz oder die Deutsche Nationalbibliothek mit den Standorten Frankfurt, Berlin und Leipzig oder auch für die Bibliothek des Bundesfinanzhofes in München gemäß § 1 Abs. 2 Nr. 1 BDSG i.V.m. § 2 Abs. 1 BDSG das BDSG gilt. Dahingegen kommt für die Bayerische Staatsbibliothek gemäß § 1 Abs. 2 Nr. 2 BDSG i.V.m. § 2 Abs. 2 BDSG das Bayerische Datenschutzgesetz (BayDSG) zur Anwendung.

Obwohl viele deutsche Bibliotheken unter die jeweiligen Landesdatenschutzgesetze fallen, wird sich die datenschutzrechtliche Analyse in der vorliegenden Arbeit im Wesentlichen auf die Bestimmungen des BDSG konzentrieren. Der Hauptgrund liegt darin, dass zwischen den Bundes- und den Landesregelungen kaum Unterschiede bestehen.[105] Schließlich

---

[101] Kühling/Seidel/Sivridis (2015), Rn. 206.

[102] Kühling/Seidel/Sivridis (2015), Rn. 260.

[103] Für den kirchlichen Bereich existieren eigene datenschutzrechtliche Regelungen: Für die evangelische Kirche das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD), für die katholische Kirche Kirchliche Anordnung über den Datenschutz (KDO).

[104] Kühling/Seidel/Sivridis (2015), Rn. 266.

[105] Kühling/Seidel/Sivridis (2015), Rn. 459; Taeger (2014), Kap. III Rn. 23.

stehen sowohl das BDSG als auch die Landesdatenschutzgesetze im europarechtlichen Kontext und sind bei Auslegungsschwierigkeiten im Lichte der EU-Datenschutzrichtlinie 95/46/EG zu interpretieren.[106] Dazu tritt ein weiterer Grund, der eher praktischer Natur, aber deswegen keineswegs weniger wichtig ist: Fast die gesamte datenschutzrechtliche Literatur bezieht sich auf das BDSG (oder das TMG bzw. TKG). Darstellungen mit landesrechtlichem Schwerpunkt sind die Ausnahme. Vor diesem Hintergrund wird nur dann auf landesrechtliche Regelungen verweisen, wenn sie eine Regelung enthalten, die sich in spezifischer Weise von der bundesrechtlichen Regelung unterscheidet. In Bezug auf Bibliotheks-Apps ist dies nur sehr selten der Fall, da keine Bereiche betroffen sind, die landesspezifische Besonderheiten enthalten, wie es etwa im Bereich der Eingriffsverwaltung der Fall ist, beispielsweise im Versammlungsrecht oder im Polizeirecht.

3.2.2 Bereichsspezifisches Recht: Telemediengesetz und Telekommunikationsgesetz

Während das BDSG und die Landesdatenschutzgesetze als allgemeines Datenschutzrecht gelten, enthalten die §§ 11 ff. TMG sowie die §§ 91 ff. TKG spezifische Datenschutzregeln für Telemediendienste bzw. Telekommunikationsdienste. Als bereichsspezifische Rechtsvorschriften gehen diese gemäß § 1 Abs. 3 S. 1 BDSG dem allgemeinen Datenschutzrecht vor.[107] Allerdings bleiben das BDSG und die Landesdatenschutzgesetze subsidiär in Geltung, d.h. TMG und TKG sind nur dann vorrangig, wenn deckungsgleiche Erlaubnistatbestände existieren.[108] Bei den bereichsspezifischen Datenschutzgesetzen existiert keine Differenzierung nach öffentlichen und nicht-öffentlichen Stellen. Sie gelten für beide Bereiche vor den jeweiligen allgemeinen Datenschutzgesetzen. Was die Konkurrenz zu internationalen Gesetzen betrifft, kann man im Bereich der öffentlichen App-Anbieter im Übrigen wieder davon ausgehen, dass TMG und TKG unproblematisch angewandt werden dürfen.[109]

---

[106] Herdegen (2015), § 8 Rnn. 46-49; Oppermann/Classen/Nettesheim (2014), § 9 Rn. 99.

[107] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 202.

[108] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 202; Lachenmann, in: Koreng/Lachenmann (2014), S. 233.

[109] Lober/Falker (2013), S. 359; Ewald, in: Baumgartner/Ewald (2016), Rn. 146.

Das TMG gilt gemäß § 1 Abs. 1 für Telemediendienste, also für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind.[110] Unter Rundfunk versteht man alle Dienste, die Bild oder Ton linear verbreiten, beispielsweise Radio-Streams.[111] Vom TMG erfasst sind damit nach herrschender Meinung alle Apps mit:

1. Online-Anbindung,
2. die nicht nur Daten transportieren, sondern auch aufbereiten und
3. nicht nur lineare Streams anbieten.[112]

Das TMG findet immer dann Anwendung, wenn der Datenumgang auf der Diensteebene betroffen ist. Gemeint ist der Umgang mit Daten, die zur Bereitstellung des Dienstes erhoben und verwendet werden. Von Bedeutung sind einerseits die Bestandsdaten (§ 14 TMG) und andererseits die Nutzungsdaten (§ 15 TMG).[113] Einen Telemediendienst stellen nach herrschender Meinung in jedem Fall die App-Stores der Plattformbetreiber dar. Allerdings stellt sich hier die Frage, ob der App-Store-Betreiber oder der App-Anbieter für die datenschutzkonforme Gestaltung der jeweiligen Produktseiten der Apps verantwortlich ist.[114] Nicht als Telemedien zu qualifizieren sind Apps, die ausschließlich zum Zweck der Verwendung auf dem mobilen Endgerät des Nutzers installiert werden, deren Nutzung keine Internetverbindung erfordert und die auch nicht unbemerkt über das Internet kommunizieren.[115] Diese reinen Offline-Apps bzw. kommunikationslosen Apps sind in datenschutzrechtlicher Hinsicht weniger problematisch als Apps mit Online-Anbindung.[116]

Normadressaten des TKG sind Diensteanbieter im Sinne des § 3 Nr. 6 TKG, d.h. jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Die Legaldefinition für Telekommunikationsdienste findet sich in § 3 Nr. 24 TKG. Demnach sind Telekommunikationsdienste in der Regel gegen Entgelt

---

110 Ewald, in: Baumgartner/Ewald (2016), Rn. 148.

111 Ewald, in: Baumgartner/Ewald (2016), Rn. 148.

112 Ewald, in: Baumgartner/Ewald (2016), Rn. 149.

113 Düsseldorfer Kreis (2014), S. 9.

114 Ewald, in: Baumgartner/Ewald (2016), Rn. 154; Lober/Falker (2013), S. 359 f.

115 Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 38.

116 Die reinen Offline-Apps werden im weiteren Verlauf der vorliegenden Arbeit, im Kapitel 3.7, noch ausführlicher behandelt.

erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetze. Zur Abgrenzung vom Gegenstandsbereich des TMG wird das so genannte Schichtmodell herangezogen, demzufolge das TKG den technischen Vorgang des Übertragens von Inhalten (Transportebene) und das TMG das Angebot der Inhalte (Interaktions- oder Anwendungsebene) umfasst.[117] Es gibt durchaus mobile Apps, die der Definition des TKG entsprechend als Telekommunikationsdienste beschrieben werden können, beispielsweise Radio-Apps von Rundfunkanstalten oder Apps mit Voice-over-IP-Funktionen (Skype-App). Allerdings gibt es bisher keine Bibliotheks-Apps, die als Telekommunikationsdienst anzusehen sind. Vor diesem Hintergrund hat das TKG, obwohl es grundsätzlich auf mobile Apps anwendbar wäre, für Bibliotheks-Apps keine praktische Relevanz.[118]

3.3 Im App-Kontext relevante datenschutzrechtliche Grundbegriffe und -prinzipien

Das Datenschutzrecht ist ein komplexes Rechtsgebiet. Bereits die Beschreibung der Grundbegriffe und -prinzipien füllt in den einschlägigen Abhandlungen umfangreiche Kapitel. Die folgende Darstellung kann daher nur einen sehr begrenzten Überblick geben und konzentriert sich auf das für den App-Kontext Wesentliche.

3.3.1 Personenbezogene Daten

Schutzgegenstand des Datenschutzrechts sind nicht irgendwelche beliebigen Daten, sondern personenbezogene Daten. Gemäß der Legaldefinition des § 3 Abs. 1 BDSG versteht man darunter Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), d.h. Informationen, die direkt oder auch mit Hilfe von Zusatzwissen auf eine namentlich benennbare Person zurückgeführt werden können.[119] Deutsche Gerichte und Datenschutzaufsichtsbehörden legen die Frage, ob ein ausreichender Perso-

[117] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 205.

[118] Die Orientierungshilfe des Düsseldorfer Kreises enthält im Übrigen keinerlei Ausführungen zum TKG, vermutlich aufgrund der mangelnden Relevanz des TKG für mobile Apps.

[119] Düsseldorfer Kreis (2014), S. 5; Taeger (2014), Kap. III Rn. 35; Kühling/Seidel/Sivridis (2015), Rn. 214-220.

nenbezug vorliegt, traditionell sehr weit aus. Es kommt weniger darauf an, ob eine Zuordnung zu einer bestimmten Person tatsächlich erfolgt, als dass hierzu faktisch die Möglichkeit besteht.[120]

3.3.2 Erheben, Verarbeiten, Übermitteln, Nutzen

Die drei Begriffe „Erheben", „Verarbeiten" und „Nutzen" umfassen fast jeden denkbaren Umgang mit personenbezogenen Daten.[121] Das „Erheben" wird dabei gemäß § 3 Abs. 3 BDSG als das zielgerichtete Beschaffen von Daten über den Betroffenen definiert und stellt eine Vorphase für die sich anschließende Verarbeitung dar.[122] Das „Verarbeiten" bildet einen Oberbegriff für die Phasen Speichern, Verändern, Übermitteln, Sperren und Löschen (§ 3 Abs. 4 BDSG), wobei „Speichern" das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger (§ 3 Abs. 4 S. 2 Nr. 1 BDSG) und „Verändern" deren inhaltliches Umgestalten (§ 3 Abs. 4 S. 2 Nr. 2 BDSG) bedeuten. Beim „Sperren" geht es darum, dass durch Anbringen eines Kennzeichens oder einer technischen Zugangsbarriere das weitere Verarbeiten oder Nutzen personenbezogener Daten verhindert wird (§ 3 Abs. 4 S. 2 Nr. 4 BDSG), wohingegen „Löschen" die vollständige und dauerhafte Unkenntlichmachung personenbezogener Daten bezeichnet (§ 3 Abs. 4 S. 2 Nr. 5 BDSG).[123] Im App-Kontext hat vor allem das „Übermitteln" praktische Relevanz, da mobile Apps – wie oben beschrieben – durch die enge technische Verknüpfung mit dem mobilen Betriebssystem Zugriff auf zahlreiche Geräteinformationen haben. Das BDSG versteht unter Übermitteln die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten (§ 3 Abs. 4 S. 2 Nr. 3 BDSG), entweder durch Weitergabe der Daten oder dadurch, dass dem Dritten Zugang zu den Daten ermöglicht wird.[124] Unter „Nutzen" versteht das BDSG jede zielgerichtete Verwendung personenbezogener Daten, sofern es sich nicht um eine Erhebung oder Verarbeitung handelt (§ 3 Abs. 5 BDSG). Die Aufnahme der Definition des Nutzens ist hier als Auffangtatbestand zu interpretieren, der immer dann

---

[120] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 213.

[121] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 223.

[122] Taeger (2014), Kap. III Rn. 44.

[123] Taeger (2014), Kap. III Rnn. 45-53.

[124] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 223; Kühling/Seidel/Sivridis (2015), Rn. 240-242.

greift, wenn die Verwendung der Daten keiner der Phasen des „Verarbeitens“ von Daten zugewiesen werden kann.[125]

3.3.3 Automatisiert erhobene und vom Nutzer übermittelte Daten

Im Kontext von mobilen Endgeräten und mobilen Apps ist eine ganze Reihe von Informationen als personenbezogene Daten im Sinne des BDSG anzusehen. Man unterscheidet grundsätzlich zwei Arten von Daten: Automatisiert erhobenen Daten und Daten, die von den Nutzern selbst übermittelt werden. Während die erste Art eher technischer Natur ist und der Nutzer auf ihre Erhebung und Verarbeitung in der Regel kaum Einfluss hat, muss der Nutzer bei der zweiten Art selbst tägig werden, beispielsweise indem er Formulare ausfüllt: Um eine App herunterladen und installieren zu können, muss ein Nutzer sich zunächst bei einem App-Store-Betreiber registrieren und hierfür bestimmte personenbezogenen Daten hinterlegen. Bei vielen Apps, die Online-Dienste bereitstellen oder nutzen, ist zusätzlich eine Registrierung und Anmeldung des Nutzers beim App-Anbieter oder dem Anbieter des Online-Dienstes notwendig.[126] Zur besseren Übersichtlichkeit sollen die Arten der von den App-Nutzern erhobenen und verarbeiteten Daten in Form einer Tabelle dargestellt werden:[127]

[125] Gola/Schomerus (2012), § 3 Rn. 42.

[126] Lober/Falker (2013), S. 358.

[127] Für die Erstellung der Tabelle wurde auf folgende Quellen zurückgegriffen: Baumgartner, in: Baumgartner/Ewald (2016), Rnn. 212-221; Lober/Falker (2013), S. 357 f.; Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rnn. 16-21; Düsseldorfer Kreis (2014), S. 4-6.

	Benennung	Beschreibung
Automatisiert erhobene Daten	UDID	Unique Device Identifier: eindeutige Gerätenummer eines iOS-Geräts; sie wird sowohl von Apple selbst zur Zuordnung des Geräts zu einer Apple-ID als auch von App-Anbietern zu Identifizierung eines App-Nutzers verwendet; wichtigstes Merkmal der UDID ist, dass sie übergreifend von allen Apps verwendet werden kann und das Tracking des Nutzers ermöglicht.
	Android Device-ID	Eindeutige Gerätenummer eines Android-Geräts, vergleichbar mit der UDID bei iOS
	IMEI	International Mobile Equipment Identity; eindeutige Gerätenummer, anhand derer jedes Mobilfunk-Endgerät weltweit eindeutig identifiziert werden kann
	IMSI	International Mobile Subscriber Identity; eindeutige Kartenkennung im Bereich des mobilen Internets
	IDFA	Identifier for Advertising; eindeutiger Werbeidentifikator bei iOS-Geräten
	Android WerbeID	Eindeutiger Werbeidentifikator bei Android-Geräten
	MAC-Adresse	Media AccessControl-Adresse; eindeutige Hardware-Adresse eines Netzwerkadapters; z.B. notwendig für das Einloggen in einem WLAN-Zugangspunkt
	IP-Adresse	Bei allen Apps notwendig, die Online-Dienste bzw. Internetkommunikation anbieten
	Standortdaten	Standortdaten werden von vielen Apps erhoben, insbesondere wenn sie standortbasierte Dienste (Location Based Services) bieten; die Geolokalisierung kann mit Hilfe von GPS-, Bluetooth- (z.B. Indoornavigation mit iBeacons) oder WLAN-Signalen durchgeführt werden; die Artikel-29-Datenschutzgruppe hat im Jahr 2011 eindeutig festgelegt, dass Sandortdaten als personenbezogene Daten zu qualifizieren sind.
Vom Nutzer übermittelte Daten (in Auswahl)	**Benennung**	**Beschreibung**
	Name	Vor- und Nachname des App-Nutzers; für die Registrierung bei einem App-Store-Betreiber bzw. Betriebssystemanbieter notwendig (z.B. für Apple-ID oder Android-ID)
	E-Mail-Adresse	E-Mail-Adresse des App-Nutzers; für die Registrierung bei einem App-Store-Betreiber bzw. Betriebssystemanbieter notwendig (z.B. für Apple-ID oder Android-ID)
	Zahlungsinformationen	Z.B. Bankdaten oder Kreditkarteninformationen; für bestimmte Registrierungsvorgänge notwendig ebenso bei der Benutzern einiger Apps sowie bei Bezahlvorgängen
	Apple-ID	Muss beim Herunterladen und Installieren von Apps aus Apples App-Store angegeben werden; eindeutige Identifikation des Kunden
	Google-ID	Muss beim Herunterladen und Installieren von Apps aus Google-Play angegeben werden; eindeutige Identifikation des Kunden
	Bibliotheksbenutzer-Nummern	Bei Bibliotheks-Apps: Eingabe der Benutzernummer, um Zugriff zum OPAC-Benutzerkonto zu erhalten; ist in Verbindung mit den bei der Bibliothek hinterlegten Daten ein personenbezogenes Datum
	PIN-Codes	Sicherheits-Codes, um Zugriff auf bestimmte Online-Dienste zu erhalten; in der Regel in Verbindung mit Zugangsnamen oder -nummern
	Fotos, Videos	Werden mit dem Smartphone aufgenommen oder dort gespeichert; vielfach enthalten sie zusätzliche Informationen wie Datum, Uhrzeit, Standort, etc.

3.3.4 Bestandsdaten, Nutzungsdaten, Inhaltsdaten

Im Bereich der mobilen Apps, die als Telemedien zu qualifizieren sind, ist eine weitere begriffliche Differenzierung wichtig, nämlich zwischen „Bestandsdaten" und „Nutzungsdaten". Davon abzugrenzen sind die „Inhaltsdaten", auf die nicht das TMG, sondern die Bestimmungen des BDSG und der Landesdatenschutzgesetze anzuwenden sind. Was darunter im Einzelnen zu verstehen ist, soll in der folgenden Tabelle erläutert und mit Beispielen versehen werden:[128]

Benennung	Erläuterung	Beispiele
Bestandsdaten (§ 14 TMG)	Personenbezogene Daten, die für die Begründung, Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind	Merkmale zur Identifikation des Nutzers wie - Name - Adresse - E-Mail-Adresse - Apple-ID oder Android Device-ID - Passwort - Gerätenummern
Nutzungsdaten (§ 15 TMG)	Personenbezogene Daten, die für die Ermöglichung der Inanspruchnahme von Telemedien und für die Abrechnung erforderlich sind	Wiederum Merkmale zur Identifikation des Nutzers (s.o.) sowie - Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung der App - IP-Adressen beim Zugriff auf Webcontent - Standortdaten beim Angebot von Location Based Services
Inhaltsdaten (nach BDSG bzw. den Landesdatenschutzgesetzen)	Personenbezogene Daten, die mit Hilfe eines Telemediendienstes übermittelt werden, um eine Vertrags- oder Leistungsverhältnis zu begründen, das selbst kein Telemediendienst ist („Offline-Vertrag")	- Bestellung von Waren bei Amazon über die Amazon-App - Bestellung einer Pizza über die App eines Pizzadienstes - Bestellung von Büchern einer Bibliothek über eine Bibliotheks-App - Auskunftsanfragen an eine Bibliothek über eine Bibliotheks-App

[128] Zur Erstellung der Tabelle wurde auf Sachs/Meder (2013), S. 304; Lober/Falker (2013), S. 360; Baumgartner, in: Baumgartner/Ewald (2016), Rn. 249; Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5, Rn. 47, Düsseldorfer Kreis (2014), S. 10-14 sowie Lachenmann, in: Koreng/Lachenmann (2014), S. 233 f. zurückgegriffen.

3.3.5 Verantwortliche Stelle

Der Legaldefinition des § 3 Abs. 7 BDSG zufolge ist die verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Verantwortliche Stelle ist damit derjenige, der über die Datenerhebung und Datenverarbeitung eigenverantwortlich entscheidet.[129] Nicht relevant für die Bestimmung der Verantwortlichkeit ist dahingegen, dass die betroffene Stelle die Daten selbst erhebt und verarbeitet.[130] Als verantwortliche Stelle und damit als Adressat der datenschutzrechtlichen Vorgaben für den Datenumgang kommen zunächst die App-Anbieter in den Blick ist,[131] wobei die Frage, wer die App technisch entwickelt hat, nur von untergeordneter Bedeutung ist. Häufig sind App-Anbieter und App-Entwickler nicht identisch. Vielfach produzieren Softwareunternehmen oder Internetagenturen die App im Rahmen eines Softwareentwicklungsvertrags.[132] Die Orientierungshilfe des Düsseldorfer Kreises macht vor diesem Hintergrund deutlich: „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-Angebots 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 […].“[133]

In Bezug auf Bibliotheks-Apps bedeutet das, dass in aller Regel die Bibliothek als App-Anbieter die verantwortliche Stelle im Sinne des BDSG ist und für die Rechtmäßigkeit der Datenerhebung und -verarbeitung durch die eigene App geradezustehen hat.[134] Sicherlich gibt es auch Konstellationen, in denen andere Akteure aus dem App-Bereich als verantwortliche Stelle in Frage kommen, beispielsweise die App-Entwickler, wenn sie entgegen den Weisungen des Auftraggebers oder ohne sein

[129] Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 24.

[130] Kühling/Seidel/Sivridis (2015), Rn. 254.

[131] Düsseldorfer Kreis (2014), S. 6.

[132] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 191.

[133] Düsseldorfer Kreis (2014), S. 6

[134] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 191.

Wissen personenbezogene Daten erheben oder verwenden,[135] die App-Store-Betreiber, die beim Herunterladen von Apps personenbezogene Daten erheben,[136] oder Dritte, die weder App-Anbieter noch App-Entwickler sind und sich durch die App personenbezogene Daten übertragen lassen.[137] Ulrich Dammann weist in diesem Zusammenhang darauf hin, dass zunehmend bezweifelt werden könne, ob der Ansatz des BDSG, der für jede Verarbeitung eine – und nur eine – verantwortliche Stelle vorsieht, der heutigen IT-Wirklichkeit noch gerecht werde.[138] Für den App-Bereich trifft diese Einschätzung mit Sicherheit zu.

3.3.6 Dritte und Auftragsdatenverarbeitung

Neben dem von der Datenverarbeitung Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle trifft man immer wieder auf den Begriff des „Dritten". Was genau ist damit im datenschutzrechtlichen Kontext eigentlich gemeint? Gemäß § 3 Abs. 8 S. 1 BDSG ist jede Person oder Stelle, die Daten erhält, als „Empfänger" anzusehen.[139] Dahingegen bezieht sich der Begriff „Dritter" auf jede natürliche oder juristische Person außerhalb der verantwortlichen Stelle mit Ausnahme des Betroffenen und eines Auftragnehmers in Deutschland oder im EU-Ausland.[140] Der Frage, wer jeweils als „Dritter" im Sinne des BDSG zu verstehen ist, kommt im Hinblick auf die datenschutzrechtlichen Anforderungen an mobile Apps große Bedeutung zu, da die Weitergabe von personenbezogenen Daten nur dann den qualifizierten gesetzlichen Anforderungen genügen muss, wenn sie tatsächlich an Dritte erfolgt. Nur in diesem Fall handelt es sich nämlich um eine Übermittlung im Sinne des

---

[135] Düsseldorfer Kreis (2014), S. 8.

[136] Die Frage, inwiefern App-Store-Betreiber als verantwortliche Stelle im Sinne des BDSG angesehen werden können, ist in der Literatur stark umstritten und nicht abschließend geklärt (Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 25; Baumgartner, in: Baumgartner/Ewald (2016), Rn. 192).

[137] Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 26. Genannt werden können hier z.B. Zulieferer von SDKs (Software Development Kits), also Programmbestandteilen der App, oder Marktforschungsunternehmen, die mit Hilfe von Standortdaten Bewegungsprofile erstellen.

[138] Dammann, in: Simitis (2011), § 3 Rn. 224.

[139] Taeger (2014), Kap. III Rn. 56.

[140] Gola/Schomerus (2012), § 3 Rn. 52.

§ 3 Abs. 4 S. 2 Nr. 3 BDSG und damit um einen Datenumgang, mit dem bestimmte gesetzliche Restriktionen verbunden sind.[141]

Eine besondere gesetzliche Privilegierung liegt bei der Auftragsdatenverarbeitung vor.[142] Die einschlägigen rechtlichen Bestimmungen dazu finden sich in § 11 BDSG. Sie gelten gleichermaßen für den öffentlichen wie den nicht-öffentlichen Bereich. Auftragsdatenverarbeitung spielt im Zusammenhang mit mobilen Apps eine ausgesprochen wichtige Rolle und kommt in vielerlei Gestalten vor, beispielsweise wenn Apps auf Websites oder Webcontent außerhalb der Server des App-Anbieters zugreifen, wenn zum Betrieb von Apps Speicherkapazitäten bei Cloud-Computing-Anbietern genutzt oder wenn Bezahlvorgänge mit Unterstützung von Finanzdienstleistern abgewickelt werden. Eine Auftragsdatenverarbeitung liegt dann vor, wenn eine verantwortliche Stelle personenbezogene Daten durch eine andere Stelle im Auftrag erheben, verarbeiten oder nutzen lässt. Durch diese Vergabe wird er zum Auftraggeber, der Dienstleister zum Auftragnehmer.[143] Dieser nimmt seine Aufgabe in völliger Abhängigkeit von den Weisungen des Auftraggebers, quasi als „verlängerter Arm", als „Werkzeug" bzw. „ausgelagerte Abteilung" des Auftraggebers wahr.[144] Der Auftraggeber als die verantwortliche Stelle bleibt jederzeit „Herr der Daten".[145] Aus einer wirksamen Auftragsdatenverarbeitung resultiert, dass der Auftragnehmer nicht mehr als „Dritter" gilt: „Er wird vielmehr dem Auftraggeber zugerechnet und bildet – durch die datenschutzrechtliche Brille betrachtet – eine organisatorische Einheit mit dem Auftraggeber."[146] Dies hat nach herrschender Meinung zur Folge, dass eine Datenübermittlung an den Auftragsdatenverarbeiter keine Übermittlung im Sinne des § 3 Abs. 4 S. 2 Nr. 3 BDSG darstellt und dementsprechend auch keine gesetzliche Erlaubnisnorm oder Einwilligung des Betroffenen notwendig ist.[147] Gleichzeitig bleibt – gemäß § 11 Abs. 1 BDSG – der Auftraggeber für die Einhaltung der daten-

---

[141] Kühling/Seidel/Sivridis (2015), Rn. 255.

[142] Kühling/Seidel/Sivridis (2015), Rn. 256.

[143] Düsseldorfer Kreis (2014), S. 6.

[144] Kühling/Seidel/Sivridis (2015), Rn. 504; Baumgartner, in: Baumgartner/Ewald (2016), Rn. 286.

[145] Taeger (2014), Kap. III Rn. 61.

[146] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 288.

[147] Taeger (2014), Kap. III Rn. 61; Baumgartner, in: Baumgartner/Ewald (2016), Rn. 288; Kühling/Seidel/Sivridis (2015), Rn. 505.

schutzrechtlichen Vorschriften vollumfänglich verantwortlich und es ergeben sich für ihn zahlreiche Sorgfalts- und Kontrollverpflichtungen.[148]

Um eine wirksame Auftragsdatenverarbeitung durchführen zu können, muss ein Vertrag zwischen Auftraggeber und Auftragnehmer geschlossen werden. Für diesen Vertrag ist die Schriftform erforderlich und er muss eine ganze Reihe von Sachverhalten regeln, die in § 11 Abs. 2 S. 2 BDSG detailliert genannt sind.[149] Anbieter von mobilen Apps haben die Möglichkeit, für diese Auftragsdatenverarbeitungsvereinbarung auf Musterverträge verschiedener Datenschutzorganisationen zurückzugreifen.[150] Während Vertragsabschlüsse zur Auftragsdatenverarbeitung innerhalb der EU oder des Europäischen Wirtschaftsraums (EWR) relativ unproblematisch sind, beinhalten solche Verträge mit Firmen, die ihren Sitz in Staaten außerhalb der EU oder des EWR haben, beispielsweise in den USA, einige rechtliche Hürden. Auftragnehmer aus solchen Drittländern gelten aufgrund von § 3 Abs. 8 S. 3 BDSG als Dritte im datenschutzrechtlichen Sinne. Mit ihnen ist die Auftragsdatenvereinbarung nur zulässig, wenn dort ein so genanntes angemessenes Datenschutzniveau, herrscht, also ein Schutzniveau, das mit dem innerhalb von EU bzw. EWR vergleichbar ist. In diesem Zusammenhang spielen die EU-Standardvertragsklauseln, d.h. von der EU-Kommission veröffentlichte Musterverträge, eine wichtige Rolle. Sie müssen zwischen Auftraggeber im EWR-Staat und Auftragnehmer im Drittland geschlossen werden.[151] Zur Datenübertragung in die USA hatte man sich lange Zeit mit der so genannten Safe-Harbour-Zertifizierung von Datenimporteuren beholfen. Das Safe-Harbor-Abkommen stand allerdings seit seinem Abschluss zwischen der EU-Kommission und der US-Regierung im Jahr 2000 in der Kritik. Mittlerweile hat der Europäische Gerichtshof mit Urteil vom 6.10.2015 entschieden, dass die Datenübertragung in die USA

---

[148] Düsseldorfer Kreis (2014), S. 6.

[149] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 289.

[150] Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) bietet unter folgender URL ein deutschsprachiges Muster zur Auftragsdatenverarbeitung an: https://www.gdd.de/links/downloads/deutschsprachiges-muster-zur-auftragsdatenverarbeitung (Letzter Zugriff: 15.02.2017).

[151] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 298; Taeger (2014), Kap. III Rn. 66. Die aktuelle Version der EU-Standardvertragsklauseln sind online beispielsweise unter folgender URL verfügbar: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF (Letzter Zugriff: 15.02.2017).

auf Grundlage des Safe-Harbor-Abkommens nicht mehr zulässig ist, da in den USA kein ausreichendes Datenschutzniveau gegeben sei.[152]

Zu den Konsequenzen aus diesem Urteil hat die Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder am 26.10.2015 ein gemeinsames Positionspapier veröffentlicht. Darin wird festgestellt, dass eine Übermittlung von Daten, die allein auf das Safe-Harbor-Abkommen gestützt ist, durch das Urteil des Europäischen Gerichtshofs künftig ausgeschlossen ist. Wenn die Behörden davon Kenntnis erlangten, würden solche Übermittlungen untersagt.[153]

3.3.7 Zweckbindung, Datenvermeidung und Datensparsamkeit

Im Hinblick auf die datenschutzfreundliche Gestaltung mobiler Apps sind drei datenschutzrechtliche Prinzipien besonders wichtig: Zweckbindung, Datenvermeidung und Datensparsamkeit.

Der Grundsatz der Zweckbindung beinhaltet, dass die verantwortliche Stelle personenbezogene Daten nur zu dem Zweck verarbeiten und nutzen darf, zu dem diese erhoben wurden. Ändert sich der Verarbeitungszweck, ist dafür eine erneute Legitimation durch Gesetz oder Einwilligung notwendig.[154] Obwohl der Zweckbindungsgrundsatz ein für das gesamte deutsche Datenschutzrecht prägendes Regelungselement darstellt, [155] wird er weder in allgemeinen noch in bereichsspezifischen Datenschutzgesetzen legaldefiniert. Er bildet vielmehr ein Leitprinzip, das bei zahlreichen datenschutzrechtlichen Vorschriften berücksichtigt werden muss. Ein gutes Beispiel findet sich in § 12 Abs. 2 TMG, demzufolge sich der Diensteanbieter auf einen gesetzlichen Erlaubnistatbestand stützen können oder die Einwilligung des Nutzers einholen muss, wenn er ursprünglich für die Bereitstellung von Telemedien erhobene und verwendete personenbezogenen Daten für andere Zwecke nutzen möchte.[156] Bei mobilen Apps kommt der Zweckbindungsgrundsatz insbeson-

---

[152] EuGH, Urteil vom 06.10.2015, Az. C-362/14. Online verfügbar unter http://curia.europa.eu (Letzter Zugriff: 15.02.2017).

[153] Das Positionspapier ist online verfügbar unter der URL https://www.datenschutz-bayern.de/faq/FAQ-SafeHarbor-Positionspapier.pdf (Letzter Zugriff: 15.02.2017).

[154] Taeger (2014), Kap. III Rn. 114.

[155] Kühling/Seidel/Sivridis (2015), Rn. 286.

[156] Kühling/Seidel/Sivridis (2015), Rn. 663; Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5, Rn. 58.

dere bei der Einholung von Berechtigungen und der damit verbundenen Möglichkeit, Zugriff auf Daten auf dem mobilen Endgerät nehmen zu können, zum Tragen. Die Orientierungshilfe des Düsseldorfer Kreises fordert in diesem Zusammenhang, dass nur die für die App erforderlichen Berechtigungen vom Nutzer angefordert werden. Lasse sich eine unnötige Berechtigungsgewährung nicht vermeiden, sollte der App-Anbieter in der Datenschutzerklärung 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 habe, dürfe die verantwortliche Stelle lediglich auf diejenigen Daten zugreifen, die für den verfolgten legitimen Zweck benötigt würden.[157]

Sowohl der Datenumgang als auch die Gestaltung und Auswahl von Datenverarbeitungssystemen sollen sich § 3a BDSG zufolge an den Grundsätzen der Datenvermeidung und Datensparsamkeit orientieren, d.h. es sollen keine oder nur so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden.[158] Im Hintergrund steht die Erkenntnis, dass ein allein rechtlich ausgerichteter Datenschutz niemals mit dem rasanten Tempo der technischen Entwicklungen im Bereich der Vernetzung und Datenauswertung mithalten kann und damit sein Ziel verfehlen wird. Als wesentlich moderner und effektiver gilt ein Konzept des technischen Datenschutzes bzw. Systemdatenschutzes, dessen Kern in der datenschutzfreundlichen Gestaltung der Systemstruktur von Datenverarbeitungssystemen und Telemediendiensten besteht:[159] „Technischer Datenschutz ist wesentlich effektiver als nur rechtlicher Datenschutz, da Verarbeitungsvorgänge, die technisch verhindert werden können, nicht mehr verboten werden müssen und im Unterschied zu Rechtsregeln gegen technische Begrenzungen nicht verstoßen werden kann. […] International ist dieser Weg mit dem Begriff der Privacy Enhancing Technologies verbunden – also einer Strategie, datensparsame Produkte zu entwickeln und auf den Markt zu bringen."[160] Bei der Entwicklung einer App sollte demnach von Anfang an auf die Implementierung des Systemdatenschutzes geachtet sowie sichergestellt werden, dass

[157] Düsseldorfer Kreis (2014), S. 17.

[158] Taeger (2014), Kap. III Rnn. 120 f.

[159] Kühling/Seidel/Sivridis (2015), Rn. 293.

[160] Scholz, in: Simitis (2011), § 3a Rn. 15.

die App später nur diejenigen personenbezogenen Daten erhebt und verwendet, die erforderlich sind.[161]

3.3.8 Verbot mit Erlaubnisvorbehalt

Das deutsche Datenschutzrecht ist vom Grundprinzip des „Verbots mit Erlaubnisvorbehalt" geprägt. Dieses findet sich in § 4 Abs. 1 BDSG und besagt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten ist, außer es liegt eine gesetzliche Erlaubnisvorschrift vor oder der Betroffene hat wirksam eingewilligt.[162] Für mobile Apps, die als Telemediendienst zu qualifizieren sind und damit dem TMG unterfallen, findet sich der Grundsatz des Verbots mit Erlaubnisvorbehalt in § 12 Abs. 1 und Abs. 2 TMG.

3.3.8.1 Gesetzliche Erlaubnistatbestände

Bezüglich der gesetzlichen Erlaubnistatbestände kommt im Bereich des allgemeinen Datenschutzrechts (BDSG, Landesdatenschutzgesetze) die Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen zum Tragen. Die wesentlichen Rechtsvorschriften für den öffentlichen Bereich finden sich in den §§ 13-16 BDSG sowie den entsprechenden Bestimmungen in den Landesdatenschutzgesetzen, die für den nicht-öffentlichen Bereich in den §§ 28-32 BDSG. Jürgen Taeger gibt zu bedenken, dass sich die Situation für öffentliche Stellen aufgrund des Eingriffscharakters der Datenerhebung und -verarbeitung insofern als strenger darstelle, als die gesetzliche Erlaubnis einen den verfassungsrechtlichen Anforderungen genügenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung zulassen müsse.[163] Grundsätzlich gilt für öffentliche Stellen, dass die Datenerhebung und -verarbeitung nur dann erlaubt ist, wenn sie für die rechtmäßige Aufgabenerfüllung der Behörde erforderlich ist.[164]

Da Bibliotheken dem öffentlichen Bereich zuzurechnen sind, muss zunächst geprüft werden, welche gesetzlichen Erlaubnistatbestände für sie in Frage kommen. Hier stellt sich das Problem, dass der Bibliotheksbe-

---

[161] Düsseldorfer Kreis (2014), S. 16; Scholz, in: Simitis (2011), § 3a Rnn. 40 f.

[162] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 225; Taeger (2014), Kap. III Rn. 133; Sachs/Meder (2013), S. 304; Düsseldorfer Kreis (2014), S. 9.

[163] Taeger (2014), Kap. III Rn. 134.

[164] Taeger (2014), Kap. III Rn. 136 und 138.

reich in Deutschland kaum gesetzlich normiert ist. Nur wenige Bundesländer haben ein Bibliotheksgesetz erlassen. Die vorhandenen Bibliotheksgesetze, beispielsweise das Hessische Bibliotheksgesetz oder das Thüringische Bibliotheksgesetz, sind ausgesprochen kurz und enthalten keinerlei Bestimmungen zum Datenschutz. In Bayern gibt es kein Bibliotheksgesetz, dafür aber mit der „Allgemeinen Benützungsordnung der Bayerischen Staatlichen Bibliotheken" (ABOB) eine Rechtsverordnung, die für alle Bibliotheken in Landesträgerschaft gilt. In Bezug auf den Datenschutz heißt es in § 3 ABOB: „Die Bayerischen Staatlichen Bibliotheken sind berechtigt, personenbezogene Daten zu erheben und zu verarbeiten, soweit dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist." Allerdings kann nicht ohne weiteres davon ausgegangen werden, dass das Angebot mobiler Apps zum Aufgabenspektrum staatlicher Bibliotheken im Sinne des § 2 ABOB gezählt werden kann. Das gleiche gilt in Bezug auf Bibliotheken anderer Bundesländer oder des Bundes. Bibliotheken haben demnach keine speziell für ihren Bereich zutreffende rechtliche Regelung, die ihnen die Datenerhebung und -verarbeitung im Zusammenhang mit mobilen Apps erlauben würde. Bibliotheks-Apps stellen vielmehr eine freiwillige Zusatzleistung dar, die das Dienstleistungsspektrum einer Bibliothek erweitern und die Kundenorientierung fördern kann.

Dennoch finden sich gesetzliche Erlaubnisse für die Erhebung und Verwendung personenbezogener Daten, die auf Bibliotheks-Apps anzuwenden sind, nämlich im TMG. Als bereichsspezifisches Datenschutzgesetz geht das TMG dem BDSG und den Landesdatenschutzgesetzen vor und gilt gleichermaßen für den öffentlichen wie für den nicht-öffentlichen Bereich. Die Vorschriften des TMG finden immer dann Anwendung, wenn es um die Datenerhebung auf der Dienstebene geht, also bei einem Datenumgang, der die Bereitstellung des Dienstes überhaupt erst ermöglicht. [165] Das TMG erlaubt die Erhebung und Verarbeitung personenbezogener Daten, insoweit es sich dabei um Bestandsdaten (§ 14 TMG) oder Nutzungsdaten (§ 15 TMG) handelt.

Auch das TKG enthält eine Reihe von Erlaubnistatbeständen zur Erhebung und Verarbeitung personenbezogener Daten. Da Bibliotheks-Apps

[165] Düsseldorfer Kreis (2014), S. 9.

jedoch nicht als Telekommunikationsdienst einzustufen sind, wird auf eine gesonderte Darstellung verzichtet.

3.3.8.2 Einwilligungen

Für den Fall, dass keine gesetzliche Erlaubnisnorm greift, bedarf es zur Zulässigkeit der Erhebung und Verarbeitung personenbezogener Daten einer wirksamen Einwilligung der betroffenen Person, im App-Kontext also des App-Nutzers.[166] Die Voraussetzungen für die Wirksamkeit der Einwilligung finden sich in § 4a BDSG und § 13 Abs. 2 und 3 TMG. Demnach muss die Einwilligung informiert erfolgen. Der Betroffene muss vor der Erhebung, Verarbeitung und Nutzung seiner Daten über Zweck und genaue Umstände der Datenverwendung unterrichtet werden.[167] Am besten geschieht das im Rahmen einer App-spezifischen Datenschutzerklärung.[168] Des Weiteren muss die Einwilligung freiwillig erfolgen und es darf kein Druck auf den Betroffenen ausgeübt werden, die Einwilligung zu erteilen.[169] § 4a BDSG fordert grundsätzlich die Schriftlichkeit der Einwilligung. § 13 Abs. 2 und 3 TMG erlauben dahingegen die Einholung einer elektronischen Einwilligung. Da die meisten mobilen Apps als Telemedien zu qualifizieren sind, geht hier die bereichsspezifische Regelung vor.[170] Für die elektronische Einwilligung schreibt der Gesetzgeber folgendes vor:[171]

(1) Der Nutzer muss seine Einwilligung bewusst und eindeutig erteilen (z.B. durch das Ankreuzen einer vorformulierten Antwort).
(2) Die Einwilligung muss protokolliert werden.
(3) Der Nutzer muss den Inhalt der Einwilligung jederzeit abrufen können.
(4) Der Nutzer muss die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können.

Die Orientierungshilfe des Düsseldorfer Kreises weist in diesem Zusammenhang darauf hin, dass es sich nicht um eine wirksame Einwilli-

---

166 Sachs/Meder (2013), S. 305.

167 Baumgartner, in: Baumgartner/Ewald (2016), Rn. 227.

168 Die Datenschutzerklärung wird weiter unten, in Kapitel 3.5.2, ausführlich thematisiert.

169 Baumgartner, in: Baumgartner/Ewald (2016), Rn. 235.

170 Lober/Falker (2013), S. 363 f.; Bodden/Rasthofer/Richter/Roßnagel (2013), S. 723.

171 Baumgartner, in: Baumgartner/Ewald (2016), Rn. 236; Düsseldorfer Kreis (2014), S. 15.

gung handelt, wenn der App-Nutzer den Dienst „so nehmen muss, wie er ist“ oder den Dienst ansonsten nicht in Anspruch nehmen kann und ein Widerruf der „Einwilligung“ nur durch Beendigung des Nutzungsvertrages möglich ist.[172] Die Datenschutzaufsichtsbehörden sprechen hiermit das Problem an, dass Nutzer eine App oft überhaupt nicht herunterladen können, wenn sie ihre Einwilligung in die teils sehr weitreichende Erlaubnis zur Datenverwendung verweigern.[173] Außerdem muss die Einwilligung ausdrücklich und aktiv erfolgen, idealerweise durch ein Opt-In-Verfahren, bei dem vor Beginn der Datenerhebung und -verwendung – d.h. schon im App-Store des Plattformanbieters oder vor der ersten Inbetriebnahme der App unmittelbar nach dem Download[174] – eine entsprechende Check-Box angekreuzt werden muss. Weniger optimal ist eine Opt-Out-Lösung, bei der der Nutzer erst die entsprechenden Voreinstellungen abwählen muss, indem er beispielsweise ein bereits aktiviertes Kreuzchen deaktiviert.[175] Dies bedeutet, dass die Annahme einer konkludenten Einwilligung im Zusammenhang mit der Erhebung und Verarbeitung personenbezogener Daten durch mobile Apps nicht akzeptabel ist.[176]

3.4 Apps mit Standortdatenerhebung (Location-Based-Services)

Eine Besonderheit des mobilen Internets sind die so genannten Standortdaten.[177] Sie sind sowohl in technischer und wirtschaftlicher als auch in datenschutzrechtlicher Hinsicht sehr interessant und sollen daher gesondert betrachtet werden.

3.4.1 Besonderheiten bei Apps mit Standortdatenerhebung

Aufgrund der raschen Verbreitung des mobilen Internets und tragbarer mobiler Endgeräte ist es für App-Anbieter und Hersteller mobiler Betriebssysteme mittlerweile sehr leicht möglich, einzelne App-Nutzer mit hoher Genauigkeit zu lokalisieren.[178] Die dabei generierten Standortdaten werden für die Erbringung von standortbezogenen Diensten (Location-

[172] Düsseldorfer Kreis (2014), S. 15 Fußnote 26.

[173] Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5, Rn. 84.

[174] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 237 f.

[175] Düsseldorfer Kreis (2914), S. 15 Fußnote 25.

[176] Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5, Rn. 82.

[177] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 311.

[178] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 312.

Based-Services) genutzt. Zur Inanspruchnahme solcher Dienste muss die Position des App-Nutzers bekannt sein.[179] Zahlreiche Apps beinhalten Location-Based-Services, beispielsweise im Rahmen von Routenplanung und Navigation, regionaler Wettervorhersage, Reiseführern sowie um Geschäfte, Restaurants, Bankautomaten oder interessante Sehenswürdigkeiten auffinden zu können.

Der Standort eines App-Nutzers kann in technischer Hinsicht auf verschiedene Arten ermittelt werden. Die beiden wichtigsten davon sind einerseits die Lokalisierung mittels GPS-Signalen und den GPS-Sensoren der mobilen Endgeräte, andererseits die Standortbestimmung mit Hilfe der eindeutigen Identifikationsnummer der geräteeigenen Netzwerkekarte (MAC-Adresse) und der Netzwerkidentifikationsnummern der WLAN-Zugangspunkte.[180] Aus datenschutzrechtlicher Perspektive besonders kritisch sind die Standortdaten, da mit ihnen genaue Bewegungsprofile des App-Nutzers erstellt werden können. Aufgrund der Tatsache, dass mobile Endgeräte sehr eng mit ihrem Inhaber verbunden und über eindeutige Gerätekennungen bzw. Mobilfunkkartennummern leicht zu identifizieren sind, erlauben Bewegungsprofile Rückschlüsse auf das Leben und die Gewohnheiten der Nutzer. Diese werden wiederum zu Werbezwecken herangezogen, meist ohne dass die App-Nutzer davon überhaupt Kenntnis erlangen.[181]

3.4.2 Die Empfehlungen der Artikel-29-Datenschutzgruppe

Aufgrund der erwähnten Gefahren für den Datenschutz hat sich die Artikel-29-Datenschutzgruppe der EU intensiv mit der Geolokalisierung befasst und in einem Working Paper aus dem Jahr 2011 bestimmte Mindeststandards für den Umgang mit Standortdaten aufgestellt. Die im Düsseldorfer Kreis versammelten deutschen Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich orientieren sich in ihren Handlungsempfehlungen für App-Entwickler und App-Anbieter aus dem Jahr 2014 an diesen Standards. Die wichtigsten Forderungen der

---

[179] Lober/Falker (2013), S. 360; Lachenmann, in: Koreng/Lachenmann (2014), S. 275.

[180] Lober/Falker (2013), S. 358. Ausführliche Darstellungen des technischen Hintergrundes finden sich bei Baumgartner, in: Baumgartner/Ewald (2016), Rnn. 314-318 und Artikel-29-Datenschutzgruppe (2011), S. 5-7.

[181] Baumgartner, in: Baumgartner/Ewald (2016), Rnn. 319; Artikel-29-Datenschutzgruppe (2011), S. 7 f.

Artikel-29-Datenschutzgruppe lassen sich folgendermaßen zusammenfassen:[182]

Bereich	Empfehlungen
Genauigkeit der Standortdaten	- Standortdaten sollten nur mit der Genauigkeit erhoben werden, die für die jeweilige App zwingend erforderlich ist (Beispiel: eine App, die eine Wanderstrecke aufzeichnen soll, braucht möglichst exakte Standortdaten, ansonsten ist die App wenig nützlich; dahingegen genügen beim Einblenden standortbezogener Hinweise auf Restaurants auch weniger präzise Standortangaben) - Standortdaten sollten „verwaschen" werden, so dass der exakte Standort der Nutzer nicht bekannt wird
Standardeinstellung bei Lokalisierungsdiensten	- Die Standardeinstellung („by default") sollte „aus" sein - Der Nutzer sollte dann die Möglichkeit haben, bei bestimmten Anwendungen stufenweise auf „an" zu schalten - Der Nutzer sollte jedes Mal beim Start der Apps erneut gefragt werden
Informationen über die Standortdatenübertragung	- Wenn das mobile Endgerät Standortdaten an den App-Anbieter oder Dritte überträgt, sollte ein ständiger Warnhinweis, z.B. in Form eines Icons, erscheinen
Erteilung der Einwilligung	- Eine Standortdatenverarbeitung setzt grundsätzlich die aktive Einwilligung des Nutzers voraus - Andere Berechtigungen können höchstens ausnahmsweise vorliegen, wenn die Erhebung der Standortdaten für den Betrieb der App zwingend erforderlich ist - Notwendig ist ein informiertes Opt-In-Verfahren; eine Opt-Out-Möglichkeit genügt nicht - Die Einwilligung muss gesondert eingeholt werden und darf beispielsweise nicht mit Allgemeinen Geschäftsbedingungen kombiniert sein - Die Einwilligung muss regelmäßig (alle 12 Monate) erneut eingeholt werden und muss jederzeit sehr einfach zu widerrufen sein

3.4.3 Apps zur Indoor-Navigation mit Bluetooth Low Energie Beacons

Wie im Vorangegangenen erwähnt, funktioniert die traditionelle Standortdatenerhebung mit Hilfe von GPS-Signalen und WLAN-Zugangspunkten. Im Rahmen der zunehmenden Vernetzung von All-

[182] Zur Erstellung der Tabelle wurde im Wesentlichen auf Lober/Falker (2013), S. 361; Sachs/Meder (2013), S. 307; Baumgartner, in: Baumgartner/Ewald (2016), Rnn. 321-324 und Artikel-29-Datenschutzgruppe (2011), S. 21-23 zurückgegriffen.

tagsgegenständen, dem so genannten „Internet der Dinge", kommt aktuell eine neue Art der Lokalisierung hinzu, die Beacon-Technologie.[183] Sie ist insbesondere für die Nahbereichsortung, die Kundenlokalisation in größeren Geschäften und die Indoor-Navigation attraktiv.[184] Beacons (dt. „Leuchtfeuer") ermöglichen eine genaue Standortbestimmung von Personen in Bereichen, in denen keine exakte Lokalisierung oder Navigation mit anderen Geolokalisierungsmethoden möglich ist. Sie arbeiten mit einem Empfangsgerät (in der Regel einem Smartphone) und einer darauf installierten mobilen App zusammen.[185]

Beacons benutzen den neuen Bluetooth Standard „Bluetooth Low Energy" (BLE), der für die Vernetzung mobiler Kleingeräte über kurze Distanzen entwickelt wurde und nur sehr wenig Energie verbraucht. Im Gegensatz zum herkömmlichen Bluetooth ist die Beacon-Technologie beim Datenaustausch stark vereinfacht, beispielsweise wird auf eine „Kopplung" der Geräte verzichtet. Dies hat zur Folge, dass nur ein einseitiger Datentransfer vom Beacon zum Empfangsgerät möglich ist. Beacons sind reine Sender. Sie senden lediglich ihre eigene Beacon-ID sowie ihre Ausgangssendeleistung und können nicht nachvollziehen, welches Gerät ihre ID empfangen hat. Die Datenverarbeitung zur Positionsbestimmung und Indoor-Navigation findet ausschließlich in der Empfängersoftware, also der mobilen App, statt. Datenschutzrechtlich muss daher zwischen dem Beacon als Sender und dem Empfängerprogramm (Smartphone-App) unterschieden werden.[186]

Nach herrschender Meinung gelten Beacons als datenschutzrechtlich unbedenklich.[187] Sie selbst verarbeiten keinerlei personenbezogene Daten. Datenschutzrechtlich relevant ist dahingegen die Verarbeitung der Beacon-Signale innerhalb der Empfänger-App. Durch sie ergeben sich bisher kaum vorstellbare Trackingmöglichkeiten innerhalb von Gebäuden, also beispielsweise der Kundenbewegungen in Geschäften, und damit vielfältige Gefahren für das informationelle Selbstbestimmungsrecht

[183] Oberbeck (2015). S. 30; Venzke-Caprarese (2014), S. 839; Kramer (2016), S. 36.

[184] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 330.

[185] Venzke-Caprarese (2014), S. 839 f.; Ceynowa (2016), S. 13 f.

[186] Oberbeck (2015), S. 30.

[187] Oberbeck (2015), S. 31; Venzke-Caprarese (2014), 842; Baumgartner, in: Baumgartner/Ewald (2016), Rn. 330.

der Betroffenen.[188] Außer wenn es sich um reine Offline-Apps handelt, unterfallen Apps mit Beacon-Technologie daher eindeutig den datenschutzrechtlichen Bestimmungen des BDSG und des TMG.

3.5 Informationspflichten gegenüber den App-Nutzern und Nutzerrechte

Datenschützer sehen eines der Hauptrisiken für den Datenschutz mobiler Apps in der mangelnden Informiertheit der Nutzer. Daher fordern sie Transparenz hinsichtlich der Erhebung und Verarbeitung personenbezogener Daten.[189] Dazu muss der App-Anbieter ein Impressum und eine App-spezifische Datenschutzerklärung vorhalten. Außerdem stehen dem App-Nutzer einige Nutzerrechten zu, deren Erfüllung er teilweise aktiv einfordern muss.[190]

3.5.1 Impressumspflicht

Mobile Apps, die als Telemediendienst einzustufen sind, fallen in den Anwendungsbereich des TMG. Die Bestimmungen über die Impressumspflicht finden sich in § 5 TMG. Danach haben Diensteanbieter für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien einige Pflichtangaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten.[191] Das Merkmal der Geschäftsmäßigkeit darf dabei nach herrschender Meinung nicht zu eng ausgelegt werden.[192] Kein Kriterium für die Geschäftsmäßigkeit ist eine Gewinnerzielungsabsicht, allerdings werden eine gewisse Nachhaltigkeit und ein Angebot verlangt, das auf einen längeren Zeitraum ausgelegt ist. Dies bedeutet, dass lediglich Telemedien, die zu rein privaten Zwecken angeboten werden, nicht der Impressumspflicht unterfallen. Die Orientierungshilfe des Düsseldorfer Kreises sieht bereits dann kein solches rein privates Angebot mehr vorliegen, wenn eine App über einen App-Store angeboten wird.[193] Bibliotheks-Apps werden in aller Regel kostenlos angeboten. Ihre Anbieter haben keine Gewinnerzielungsabsicht. Dennoch ist nach der üblichen weiten Auslegung des Kriteriums „geschäftsmäßig" eindeutig davon aus-

[188] Venzke-Caprarese (2014), 844.

[189] Sachs/Meder (2013), S. 305.

[190] Düsseldorfer Kreis (2014), S. 18.

[191] Selent (2013), S. 40.

[192] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 162.

[193] Düsseldorfer Kreis (2014), S. 18.

zugehen, dass für sämtliche Bibliotheks-Apps, die als Telemedium einzustufen sind, die Impressumspflicht besteht.[194]

Wenn die App journalistisch-redaktionelle Teile enthält, müssen auch die Bestimmungen des § 55 des Rundfunkstaatsvertrags (RStV) beachtet werden. Wann das genau der Fall ist, wird nach wie vor diskutiert. Meist wird vorausgesetzt, dass der App-Anbieter selbst Inhalte erstellt oder zumindest durch Auswahl, Kommentierung oder Bearbeitung so aufbereitet, dass seine eigene Wertung in die Inhalte einfließt.[195] Für viele Bibliotheks-Apps dürfte das zutreffen, d.h. das Impressum müsste zusätzlich eine inhaltlich verantwortliche Person benennen, wobei es sich explizit um eine natürlich, geschäftsfähige Person handeln muss.[196]

Mobile Apps weisen gegenüber Websites einige Unterschiede auf. Diesen muss bei der Gestaltung des App-Impressums Rechnung getragen werden. Wegen der geringen Displaygröße der mobilen Endgeräte ist es beispielsweise nicht einfach, den Hinweis auf das Impressum leicht auffindbar anzubringen. Ein Blick auf die Rechtsprechung zu § 5 TMG macht jedoch deutlich, dass ein verstecktes oder unzureichend benanntes Impressum zu wettbewerbsrechtlichen Abmahnungen oder Bußgeldern führen kann. So hat der Bundesgerichtshof im Jahr 2006 entschieden, dass die Anbieterkennzeichnung innerhalb von zwei Klicks von jeder Seite des Webangebots erreichbar sein muss. Dies sollte auch für mobile Apps berücksichtigt werden. In Bezug auf die Informationspflichten gegenüber den App-Nutzern ist demnach zu beachten, dass das Impressum vom durchschnittlichen Nutzer leicht und ohne langes Suchen gefunden werden kann.[197]

3.5.2 App-spezifische Datenschutzerklärung

Bei der ein oder anderen mobilen App mag die Geschäftsmäßigkeit des angebotenen Dienstes und damit die Impressumspflicht diskutabel sein. Die Frage der Notwendigkeit einer Datenschutzerklärung ist dahingegen einfacher zu beantworten. Eine solche Erklärung ist unabhängig von der

---

[194] Die genauen Pflichtangaben, die gemäß § 5 TMG im Impressum enthalten sein müssen, werden weiter unten im Rahmen der Checkliste (Kapitel 4.2) aufgezählt.

[195] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 151.

[196] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 165; Wiedemann, in: Solmecke/Taeger/Feldmann (2013), Kap. 4, Rn. 154.

[197] Selent (2013), S. 41; Kramer (2014), S. 156.

Geschäftsmäßigkeit erforderlich, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Bei allen mobilen Apps – mit Ausnahme der reinen Offline-Apps – ist das regelmäßig der Fall.[198] Praktische Erfahrungen aber zeigen immer wieder, dass gar keine oder mangelhafte Datenschutzerklärungen vorhanden sind. Insbesondere finden sich kaum App-spezifischen Datenschutzerklärungen, d.h. solche, die die besonderen Charakteristika mobiler Apps berücksichtigen. Dies ist deswegen besonders bedauerlich, weil mobile Apps über die enge Verknüpfung mit dem mobilen Betriebssystem und den direkten Zugriff auf die Hardware-Schnittstellen des mobilen Endgeräts eine wesentlich größere Gefahrenquelle für die persönlichen Daten des Gerätebesitzers darstellen als klassische Websites.[199] Die im Düsseldorfer Kreis versammelten Datenschützer erläutern hierzu: „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."[200] Zu nennen sind in diesem Zusammenhang die Zugriffsberechtigungen auf die Kamera, das Mikrophon, den GPS-Sensor und die Bluetooth-Funktion, die in der Datenschutzerklärung offengelegt werden müssen. Das gleiche gilt für Zugriffe auf Daten, die auf dem mobilen Endgerät gespeichert sind, wie z.B. Adressverzeichnisse, Telefonnummern, Memos, SMS oder WhatsApp-Nachrichten.[201] Nicht ausreichend für eine hinreichende Information sind die standardmäßigen Berechtigungsbeschreibungen, die den App-Nutzern durch den jeweiligen App-Store zur Verfügung gestellt werden, da mit ihnen nicht vermittelt wird, auf welche Daten zu welchen Zwecken konkret zugegriffen wird.[202]

Die wesentlichen Bestimmungen bezüglich der Datenschutzerklärung finden sich in § 13 TMG. Laut Abs. 1 S. 1 dieses Paragraphen muss der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezoge-

198 Selent (2013), S. 41.

199 Sachs/Meder (2013), S. 305.

200 Düsseldorfer Kreis (2014), S. 19.

201 Baumgartner, in: Baumgartner/Ewald (2016), Rn. 232.

202 Sachs/Meder (2013), S. 305.

ner Daten sowie über die Verarbeitung seiner Daten außerhalb der EU in allgemein verständlicher Form zu unterrichten. Der Inhalt dieser Unterrichtung muss jederzeit für den App-Nutzer abrufbar bleiben. Gemäß § 13 Abs. 1 S. 2 TMG ist der Nutzer außerdem über eingesetzte automatisierte Verfahren zu informieren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung und Verwendung personenbezogener Daten vorbereiten[203]. Beispiele für solche Verfahren sind der Einsatz von Cookies oder Analysetools zur Reichweitenmessung.

Die in der Datenschutzerklärung enthaltenen Informationen[204] müssen zu Beginn des Nutzungsvorgangs erteilt werden, am besten bereits im App-Store auf der Produktseite der jeweiligen App, also noch vor dem Download der App. Alternativ, jedoch weniger optimal, kann die Datenschutzerklärung innerhalb der App, nach Download und Installation, aber noch vor der ersten Nutzung der App, angeboten werden.[205] Bezüglich der Erreichbarkeit der Datenschutzerklärung und der Lesbarkeit auf dem Display des mobilen Endgeräts gelten die gleichen Anforderungen wie beim Impressum. Abschließend muss noch einmal betont werden, dass eine Datenschutzerklärung den Zweck hat, den App-Nutzer über datenschutzrechtlich relevante Gesichtspunkte im Zusammenhang mit der App zu informieren und eine vom Gesetz geforderte informierte Einwilligung vorzubereiten. Dabei setzt eine vollständige Datenschutzerklärung die Rechtmäßigkeit der Datenerhebung, -speicherung und -übermittlung voraus. Markus Selent zufolge nützt es daher wenig, „[…] in einer Datenschutzerklärung einer App über ein amerikanisches Trackingtool wie Flurry Analytics zu unterrichten, wenn dessen Einsatz aufgrund fehlender Einwilligung des Nutzers oder vertraglicher Regelungen rechtswidrig ist.“[206]

---

[203] Sachs/Meder (2013), S. 305; Lober/Falker (2013), S. 362; Lachenmann, in: Koreng/Lachenmann (2014), S. 229.

[204] Die Informationen, die in der Datenschutzerklärung enthalten sein müssen, werden weiter unten im Rahmen der Checkliste (Kapitel 4.2) aufgezählt.

[205] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 232 und 237 f.; Sachs/Meder (2013), S. 305; Düsseldorfer Kreis (2014), S. 18 f.; Lober/Falker (2013), S. 362; Lachenmann, in: Koreng/Lachenmann (2014), S. 268 f.

[206] Selent (2013), S. 41.

3.5.3 Recht des Nutzers auf Auskunft und Löschung seiner Daten

App-Anbieter sind gemäß § 13 Abs. 8 TMG auf formloses Verlangen des App-Nutzers zur Auskunft über die zu seiner Person gespeicherten Daten verpflichtet. Diese Vorschrift des TMG gilt gleichermaßen für den öffentlichen wie für den nicht-öffentlichen Bereich. Die konkrete Ausgestaltung dieses Auskunftsanspruchs unterscheidet sich jedoch. Für öffentliche Stellen ist sie in den §§ 19 f. BDSG bzw. den entsprechenden landesrechtlichen Bestimmungen geregelt, für nicht-öffentliche Stellen in den §§ 34 f. BDSG. Auf die in diesen Paragraphen enthaltenen zahlreichen Detailregelungen kann hier nicht eingegangen werden. Für den App-Kontext sind sie außerdem kaum relevant. Festzuhalten bleibt allerdings, dass App-Nutzer jederzeit die Berichtigung, Löschung und Sperrung ihrer Daten verlangen können. App-Anbieter sollten darauf vorbereitet sein, um bei Bedarf zeitnah reagieren zu können.[207]

3.6 Technischer Datenschutz

Beim technischen Datenschutz bzw. Systemdatenschutz, der oben bereits kurz erwähnt wurde, spielt die Sicherheit der App eine tragende Rolle. Diese sollte bereits ganz am Beginn der App-Entwicklung mit eingeplant werden, um später erhöhte Entwicklungs- und Nachbesserungskosten zu vermeiden.[208] Angaben zu den notwendigen technischen Schutzanforderungen, die der Diensteanbieter bzw. die verantwortliche Stelle gewährleisten müssen, finden sich in den „technischen und organisatorischen Vorkehrungen" des § 13 Abs. 4 TMG und der „technischen und organisatorischen Maßnahmen des § 9 BDSG sowie den dazugehörigen Anlagen. Der Grad an Sicherheit gilt dabei als variabel, daher ist nur diejenige Sicherheit zu gewährleisten, die erforderlich ist und in einem angemessenen Verhältnis von Aufwand und Schutzzweck steht.[209] Die vielfältigen Vorgaben lassen sich folgendermaßen zusammenfassen.[210]

---

[207] Düsseldorfer Kreis (2014), S. 21; Lober/Falker (2014), S. 363; Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5, Rn. 91-93.

[208] Düsseldorfer Kreis (2014), S. 21.

[209] Taeger (2014), Kap. III Rn. 129.

[210] Zur Erstellung der Tabelle wurde insbesondere auf folgende Literatur zurückgegriffen: Düsseldorfer Kreis (2014), S. 21-27; Baumgartner, in: Baumgartner/Ewald (2016), Rn. 340-362; Brennscheid (2013), S. 87-97.

Technisch-organisatorische Maßnahme	Beschreibung
Verschlüsselung	- Der Datentransfer muss durch eine Transportverschlüsselung abgesichert sein - Sowohl die mobile App als auch der Server des App-Anbieters (bzw. eines Auftragsdatenverarbeiters) müssen mithilfe verschlüsselter Protokollvarianten kommunizieren
Lokale Speicherung	- Auf dem mobilen Endgerät sollen nur diejenigen personenbezogenen Daten lokal gespeichert werden, die für den App-Betrieb unbedingt erforderlich sind
Löschung der Daten	- Die lokal gespeicherten personenbezogenen Daten sollen automatisch gelöscht werden, wenn die App deinstalliert wird. - Die auf dem Server des App-Anbieters anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung sollen dahingegen unmittelbar nach deren Beendigung gelöscht werden, außer sie sind zum weiteren ordnungsgemäßen Betrieb der App oder zu vertraglichen Zwecken (z.B. Bezahlung) zwingend erforderlich
Passwörter	- Wenn eine Authentifizierung innerhalb der App vorgesehen ist, z.B. um auf bestimmte Webinhalte oder Datenbanken zugreifen zu können, sollen die App-Nutzer durch technische Vorkehrungen dazu gezwungen werden, in ausreichendem Maße komplexe und damit sichere Passwörter zu wählen - Die Rechtevergabe im Rahmen einer Authentifizierung sollte immer über den Server des App-Anbieters verlaufen, nicht über in die App integrierte Sicherheitsmechanismen, da diese in der Regel leichter zu umgehen sind
Logging	- Protokollierungen von Fehlermeldungen und Systemereignissen (Logging) sollten möglichst ganz unterbleiben - Es ist nicht auszuschließen, dass andere Apps Zugriff auf diese Logfiles erhalten und mit diesen verbundene personenbezogene Daten ausspähen
Einbindung von Websites	- Wenn Webseiten in die App-Nutzung eingebunden werden (so genanntes In-App-Browsing), ist das für den Nutzer oft nicht ersichtlich - Mitunter kann es dadurch zu Datenschutzverstößen kommen, wenn die Webseiten Dritter Aktionen ausführen, für die keine Einwilligungen eingeholt wurden (z.B. Reichweitenmessungen mittels Analysetools oder das Setzen von Cookies) - Es muss technisch sichergestellt werden, dass datenschutzrechtlich nicht zulässiger Webseiten-Code Dritter von den In-App-Browsern nicht ausgeführt wird oder die Nutzer einen entsprechenden Warnhinweis erhalten
Server-absicherung	- Nicht nur die App muss technisch abgesichert sein, sondern auch die beteiligten Server - Die erforderlichen Schutzmaßnahmen sind mit denen bei Webapplikationen vergleichbar (z.B. geeignete Firewall-Architektur)

3.7 Sonderfall: Reine Offline-Apps

Apps, die gänzlich ohne Onlineanbindung auskommen, bezeichnet man als Offline-Apps. Nach dem Download aus dem App-Store und der Installation auf dem mobilen Endgerät arbeiten sie vollständig ohne Zugriff auf das Internet. Beispiele für solche reinen Offline-Apps sind Adressbücher, Fotoalben, Taschenrechner, einige Fitness-Apps etc. Auch die App „BSB-Navigator" der Bayerischen Staatsbibliothek, die eine Indoor-Navigation innerhalb des Gebäudes der Bayerischen Staatsbibliothek mit Hilfe von Bluetooth Low Energie Beacons ermöglicht, kann als Offline-App eingestuft werden. Nach Download und Installation funktioniert sie ohne Zugriff auf das Internet.[211] Wegen der fehlenden Onlineanbindung gelten Offline-Apps nicht als Telemedien und dementsprechend ist das TMG auf sie nicht anwendbar.[212] Möglich erscheint zwar die Anwendung des BDSG, jedoch finden sich dort für Apps ohne Onlineanbindung kaum klare datenschutzrechtliche Vorgaben. Sven Venzke-Caprarese zufolge spricht daher vieles dafür, dass auch der Anwendungsbereich des BDSG nicht eröffnet ist, wenn eine App zwar vom App-Anbieter angeboten und vom Nutzer heruntergeladen, dann aber keine Onlineverbindung mehr aufbaut und weder dem App-Anbieter, noch einem Dritten Daten übermittelt werden: „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."[213] Sind weder BDSG noch TMG anwendbar, dann gelten auch die im vorangegangenen Kapitel gezeigten datenschutzrechtlichen Grundprinzipien bzw. Pflichten nicht, beispielsweise das Verbot mit Erlaubnisvorbehalt oder die Informationspflichten gegenüber den App-Nutzern.

[211] Kramer (2016), S. 36.

[212] Lober/Falker (2013), S. 360.

[213] Venzke-Caprarese (2014), S. 842.

3.8 Innerbehördliche Datenschutzkontrolle bei mobilen Apps am Beispiel der Situation in Bayern (Art. 26 BayDSG)

In Deutschland beruht das Datenschutzkontrollprinzip auf drei Säulen: Selbstkontrolle des Betroffenen, Eigenkontrolle innerhalb der verantwortlichen Stelle und Fremdkontrolle im Rahmen hoheitlicher Überwachung.[214] Während der Betroffene durch die verschiedenen datenschutzrechtlichen Informationspflichten der verantwortlichen Stelle und sein Recht auf Auskunft und Löschung in die Lage versetzt werden soll, eine wirksame Selbstkontrolle durchführen zu können, wird der hoheitliche Datenschutz von den staatlichen Aufsichtsbehörden wahrgenommen, jeweils getrennt für den öffentlichen und den nichtöffentlichen Bereich. Wie aber wird die Eigenkontrolle ausgeübt? Zuständig dafür ist der behördliche bzw. der betriebliche Datenschutzbeauftragte. Er hat gemäß § 4g Abs. 1 S. 1 BDSG die Aufgabe, auf die Einhaltung der datenschutzrechtlichen Vorschriften hinzuwirken. Insbesondere ist er dafür verantwortlich, ein Verfahrensverzeichnis sämtlicher im Betrieb oder der Behörde vorhandener automatisierter Datenverarbeitungsprozesse zu führen.[215]

Interessanter Weise finden sich in keiner der für die Erstellung dieser Arbeit verwendeten Abhandlungen zum Thema App-Datenschutz irgendwelche Hinweise, welche Rechte und Pflichten dem behördlichen Datenschutzbeauftragten bezüglich der Rechtmäßigkeit einer eingesetzten mobilen App zukommen oder wie die Aufnahme in das Verfahrensverzeichnis konkret auszusehen hat. Dies ist angesichts der Tatsache durchaus verwunderlich, dass in der Praxis gerade die korrekte Beschreibung des der App zugrundeliegenden Datenverarbeitungsverfahrens besondere Probleme bereitet. Möglicherweise ist der Grund darin zu suchen, dass es diesbezüglich zwischen den bundes- und den landesrechtlichen Regelungen große Unterschiede gibt. Meines Erachtens sind diese Unterschiede weitreichender als in allen anderen Bereichen des Datenschutzrechts.

Während bundesrechtlich immer nur davon die Rede ist, dass der behördliche Datenschutzbeauftragte eine Verfahrensbeschreibung in das behördliche Verfahrensverzeichnis aufnehmen soll – wobei ihm gemäß

[214] Taeger (2014), Kap. III Rn. 76.

[215] Taeger (2014), Kap. III Rn. 273.

§ 4g Abs. 1 Nr. 2 BDSG selbstverständlich ein angemessener Zeitraum zur Überprüfung des Verfahrens und zur Stellungnahme eingeräumt wird[216] – gibt es beispielsweise im Bayerischen Datenschutzgesetz mit Art. 26 BayDSG sehr detaillierte Bestimmungen über das datenschutzrechtliche Freigabeverfahren für automatisierte Verfahren. Demnach bedarf jeder erstmalige Einsatz eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, der vorherigen schriftlichen Freigabe durch die einsetzende öffentliche Stelle.[217] Diese Freigabe muss eine Reihe von Angaben enthalten, z.B. die Bezeichnung des Verfahrens, Zweck und Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung, Art der gespeicherten Daten, Kreis der Betroffenen, etc.[218] Die Behörden haben ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens eine Verfahrensbeschreibung mit den in Abs. 2 aufgeführten Angaben zur Verfügung zu stellen. Außerdem ist eine allgemeine Beschreibung der Art der für das Verfahren eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen beizugeben.[219] Die behördlichen Datenschutzbeauftragten haben sodann den Auftrag, die datenschutzrechtliche Freigabe zu erteilen.[220] Verweigern sie die Freigabe aufgrund von Bedenken, kann ersatzweise der Behördenleiter das geplante automatisierte Verfahren freigeben.[221] Insgesamt handelt es sich bei dem nach BayDSG vorgesehenen Freigabeverfahren um einen eng normierten Prozess, der in der Praxis vieler Behörden immer wieder zu Problemen führt, v.a. dann, wenn er zu kurzfristig vor der Einführung eines automatisierten Verfahrens begonnen wurde.

---

[216] Teager (2014), Kap. III Rn. 280.

[217] Art. 26 Abs. 1 S. 1 BayDSG.

[218] Art. 26 Abs. 2 BayDSG

[219] Art. 26 Abs. 3 S. 1 BayDSG. Der Bayerische Landesbeauftragte für den Datenschutz hat hierzu ein Formular erstellt, das Behörden beim Erstellen der Verfahrensbeschreibung unterstützten soll. Das Formular findet sich unter folgender URL: https://www.datenschutz-bayern.de/download/verfbes.pdf (Letzter Zugriff: 15.02.2017).

[220] Art. 26 Abs. 3 S. 2 BayDSG.

[221] Art. 26 Abs. 3 S. 3 BayDSG.

4 Leitfaden für die Praxis

Bibliotheken, die eine mobile App anbieten, sind als verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG anzusehen. Dies ist völlig unabhängig davon, wer die App technisch entwickelt hat. In den seltensten Fällen wird die Bibliothek selbst der Entwickler sein. Meist werden Softwareunternehmen oder Internetagenturen im Rahmen eines Softwareentwicklungsvertrags damit beauftragt. Als verantwortliche Stelle ist jedoch die Bibliothek – nicht der App-Entwickler – für die Einhaltung sämtlicher datenschutzrechtlich relevanter Vorschriften zuständig. Mit den daraus resultierenden datenschutzrechtlichen Anforderungen und Pflichten sind viele Bibliotheken erfahrungsgemäß überfordert. Der vorliegende Leitfaden für die Praxis soll sie dabei unterstützen, ihrer datenschutzrechtlichen Verantwortung gerecht werden zu können, indem er ihnen Hilfestellung und Orientierung in den wichtigsten Phasen des App-Entwicklungsprozesses anbietet.

Der Leitfaden gliedert sich in zwei Teile. Der erste Teil (Kapitel 4.1) enthält Empfehlungen für die Konzeption und Entwicklung datenschutzfreundlicher Bibliotheks-Apps. Die Empfehlungen bauen auf den Ergebnissen der datenschutzrechtlichen Analyse im 3. Kapitel dieser Arbeit auf. Die Empfehlungen orientieren sich an den einzelnen Phasen der App-Entwicklung. Die Hauptphasen sind jeweils mit römischen Zahlen von I. bis VIII. nummeriert. Wenn nötig, wurden die Hauptphasen untergliedert. Die Unterphasen sind mit Kleinbuchstaben nummeriert.

Den zweiten Teil des Praxisleitfadens (Kapitel 4.2) bildet eine Checkliste, die die wichtigsten Aussagen der Empfehlungen noch einmal in übersichtlicher Form und zum Abhaken auf den Punkt bringt. Die Gliederung der Checkliste entspricht exakt der Gliederung der Empfehlungen (Hauptphasen mit römischen Buchstaben von I. bis VIII., Unterphasen mit Kleinbuchstaben). Bei der Konzeption wurde großes Gewicht auf diese parallele Struktur der Empfehlungen und der Checkliste gelegt. Im späteren Praxiseinsatz in Bibliotheken sollten die Empfehlungen und die Checkliste nebeneinander verwendet werden: Die Empfehlungen bieten praxisgerechte Erläuterungen der datenschutzrechtlichen Anforderungen an mobile Bibliotheks-Apps, die Checkliste führt die Projektleiter innerhalb der Bibliotheken Schritt für Schritt durch den App-Entwicklungsprozess.

4.1 Empfehlungen für die Konzeption und Entwicklung datenschutzfreundlicher Bibliotheks-Apps

I. Beginn / Konzeptphase

I. a) Datenschutzfreundliche Gestaltung von Anfang an

Von Projektbeginn an sollte die datenschutzfreundliche Gestaltung der App im Auge behalten oder zumindest nicht aufgeschoben oder ausgeklammert werden. Dies verhindert, dass es in späteren Projektphasen zu Problemen bezüglich des Datenschutzes kommt, die das gesamte Projekt gefährden oder es zumindest verzögern können. Meist ist es wesentlich einfacher und kostengünstiger, die Anforderungen des Datenschutzes zu Projektbeginn mit zu berücksichtigen, als zu versuchen, sie in einem späteren Projektstadium oder sogar erst nachträglich bei einem bereits fertigen Endprodukt umzusetzen. Besonders empfehlenswert ist es, den behördlichen Datenschutzbeauftragten direkt bei Projektbeginn in die Planungen miteinzubeziehen. Bei sehr umfangreichen App-Entwicklungsprojekten, die im Bibliotheksbereich aber wohl nicht die Regel sind, kann es sinnvoll sein, auch die entsprechenden Datenschutzaufsichtsbehörden vorab zu informieren und um Beratung zu bitten. In den meisten Fällen werden sie dieser Bitte gerne nachkommen. Dadurch wird die Gefahr minimiert, dass mobile Apps später von den Aufsichtsbehörden beanstandet werden.

I. b) Berücksichtigung des Datenschutzes im Zeitplan

Die Erfüllung der datenschutzrechtlichen Anforderungen kostet Zeit. Diese sollte im Zeitplan berücksichtigt werden. Zeit ist beispielsweise für folgende Aktionen einzuplanen:

- Abschluss von Vereinbarungen zur Auftragsdatenverarbeitung mit Dritten
- Freigabeverfahren für den erstmaligen Einsatz automatisierter Verfahren, wenn dies landesrechtlich vorgeschrieben ist
- Datenschutzkonforme Gestaltung von Einwilligungserklärungen
- Abfassen einer App-spezifischen Datenschutzerklärung
- Umsetzung von Sicherungsmaßnahmen zur Gewährleistung eines effektiven technischen Datenschutzes

I. c) Welche Daten werden erhoben?

Anhand des geplanten Einsatzzwecks der Bibliotheks-App sollte überlegt werden, welche Arten von personenbezogenen Daten erhoben werden müssen, damit die App bestimmungsgemäß funktioniert (automatisiert erhobene Daten, vom Nutzer eingegebene Daten, Bestandsdaten, Nutzungsdaten, Inhaltsdaten). Bereits hier sollte immer auf die Prinzipien der Datenvermeidung bzw. der Datensparsamkeit geachtet werden, d.h. nur die Daten dürfen erhoben werden, die auch tatsächlich erforderlich sind (technisch wie organisatorisch) um die mit der App angestrebten Dienstleistungen verwirklichen zu können.

I. d) Klären der Rechtsgrundlage der Datenerhebung und -verarbeitung

Wichtig ist auch, sich bereits in der Konzeptphase mit der Frage zu befassen, ob für die geplante Datenerhebung und -verarbeitung eine Rechtsgrundlage existiert oder ob Einwilligungen von den App-Nutzern eingeholt werden müssen. Wenn letzteres der Fall ist, muss als nächstes geklärt werden, in welcher Form die Einholung der Einwilligung erfolgen soll.

I. e) Prüfen der Realisierungsmöglichkeit als reine Offline-App

Ebenfalls in der Konzeptphase sollte geprüft werden, ob die geplante Bibliotheks-App als Offline-App realisiert werden kann. Nach herrschender Meinung gelten reine Offline-Apps in datenschutzrechtlicher Perspektive als unbedenklich, da für sie weder aus dem BDSG oder den Landesdatenschutzgesetzen noch aus dem TMG spezifische datenschutzrechtliche Anforderungen hergeleitet werden können. Für sie gelten daher auch viele der im 3. Kapitel dieser Arbeit skizzierten datenschutzrechtlichen Grundprinzipien und Pflichten nicht, beispielsweise das Verbot mit Erlaubnisvorbehalt oder die Informationspflichten gegenüber den App-Nutzern. Ebenso wenig müsste vor der Inbetriebnahme offline arbeitender Bibliotheks-Apps das von manchen Landesdatenschutzgesetzen vorgeschriebene Freigabeverfahren durchgeführt werden. Vermutlich werden aber die meisten Bibliotheks-Apps nur als App mit Onlineanbindung zu realisieren sein, da immer mehr Bibliotheksservices über das Internet erbracht werden (z.B. E-Books, E-Journals, elektronische Datenbanken, Benutzung des OPAC, etc.).

I. f) Bei Apps mit Onlineanbindung

Apps, die zur Erbringung ihres Dienstleistungsspektrums über das Internet kommunizieren, sind als Telemedien im Sinne des § 1 Abs. 1 TMG anzusehen. Neben den einschlägigen Bestimmungen des BDSG bzw. der Landesdatenschutzgesetze müssen daher auch die entsprechenden Vorgaben des TMG berücksichtigt werden. Dies sollte man sich so früh wie möglich bewusst machen, um bereits in der Konzeptionsphase die entsprechenden Schritte einleiten zu können. Die praktische Erfahrung zeigt dahingegen, dass das TKG nicht auf Bibliotheks-Apps anzuwenden ist, da diese nicht als Telekommunikationsdienste zu qualifizieren sind. Bibliotheken müssen sich im Hinblick auf von ihnen angebotene mobile Apps nicht weiter mit dem TKG beschäftigen. Von großer Bedeutung ist dahingegen die Frage, mit welchen Servern die Bibliotheks-App über das Internet kommuniziert, mit den eigenen Servern der Bibliothek oder auch mit den Servern Dritter.

I. g) Gestaltung der datenschutzrechtlich relevanten Beziehungen zu Dritten

Vielfach kommunizieren Bibliotheks-Apps nur mit den bibliothekseigenen Servern. Aus der Perspektive des Datenschutzes ist dies relativ unproblematisch. Um einen echten Mehrwert für die App-Nutzer zu generieren und das Nutzungserlebnis zu steigern, ist es aber häufig erforderlich, dass auch auf Webcontent Dritter zugegriffen wird, beispielsweise könnten Karten der Vermessungsämter, Dokumente und Bilder aus Archiven, Aufnahmen von Kunstobjekten aus Museen sowie weitere audiovisuelle Beiträge von beliebigen Partnern in die App integriert werden. Hierdurch kommt es zu einer ganzen Reihe von Datenaustauschprozessen mit den genannten Dritten, die datenschutzrechtlich korrekt gestaltet sein müssen. Dies geht nur über den Abschluss vertraglicher Regelungen, den so genannten Vereinbarungen zur Auftragsdatenverarbeitung. Befinden sich die Auftragnehmer der Datenverarbeitung innerhalb der EU oder des EWR, sind die notwendigen Vereinbarungen relativ einfach. Komplizierter wird es, wenn sich die Auftragnehmer außerhalb dieses Bereichs befinden. Dann muss beispielsweise auf die EU-Standardvertragsklauseln zurückgegriffen werden.

I. h) Einbindung von Webseiten der Bibliothek oder Dritter

Häufig werden ganze Webseiten der Bibliothek oder Dritter innerhalb einer App angezeigt, beispielsweise der Bibliothek-OPAC, elektronische Datenbanken oder weiterführende Informationen von der Homepage. Dem App-Nutzer ist dabei oft nicht ersichtlich, dass der Content, den er gerade zu sehen bekommt, nicht aus der App stammt, sondern über das Internet übertragen wurde. Man spricht in diesem Zusammenhang vom so genannten In-App-Browsing. Links innerhalb der App, die zu Webseiten führen – seien es eigene oder fremde – müssen eindeutig gekennzeichnet werden. Beim Betätigen eines solchen Links sollte idealerweise ein entsprechendes Pop-Up-Fenster mit einem Warnhinweis erscheinen. Mit dem Öffnen eigener oder fremder Webseiten werden nämlich vielfach Datenübertragungsprozesse angestoßen, für die möglicherweise weder gesetzliche Erlaubnistatbestände noch eine Einwilligung des App-Nutzers vorliegen. Zu denken ist hier beispielsweise daran, dass mit der Website auch Cookies oder Analysetools zur Reichweitenmessung ohne Wissen des App-Nutzers auf dessen mobiles Endgerät übertragen werden. Hierdurch würde sich die Bibliothek als verantwortliche Stelle an den auftretenden Datenschutzverstößen zumindest mitschuldig machen.

I. i) Überlegungen zur möglichen Standortdatenerhebung

Immer häufiger bieten Bibliotheken mobile Apps mit Location-Based-Services an, also Dienstleistungen, die auf den jeweiligen Standort des App-Nutzers zugeschnitten sind. Dazu muss mithilfe der geräteeigenen Sensoren (v.a. GPS-Sensor oder Bluetooth-Empfänger) die genaue Position des App-Nutzers festgestellt werden. Arbeitet die App offline, dann werden diese Standortdaten nicht über das Internet übertragen, sondern es werden direkt aus der App Informationen geladen, die sich auf den Standort beziehen, beispielsweise Beschreibungen, Texte, Fotos oder auch multi-mediale Elemente. Datenschutzrechtlich ist dies unbedenklich. Meistens aber werden die Standortdaten über das Internet auf den Server der Bibliothek – oder im Rahmen einer Auftragsdatenverarbeitungsvereinbarung an den Server Dritter – übertragen und von dort der entsprechende Content zurück an die App geschickt. Für diese Datenübertragungsprozesse gibt es keine gesetzlichen Erlaubnistatbestände. Erforderlich ist dafür die Einwilligung des App-Nutzers. Für die Form, wie diese Einwilligungserklärung gestaltet sein muss, gibt es sowohl von gesetzlicher Seite als auch von den Datenschutzaufsichtsbehörden klare Vorgaben, die von den App-Anbietern eingehalten werden müssen. Es

empfiehlt sich, bereits in der Konzeptionsphase zu planen, wie diese Einwilligungserklärung technisch umgesetzt werden soll.

I. j) Vorarbeiten für eine mögliche Verfahrensbeschreibung beim ersten Einsatz automatisierter Verfahren

Ein letzter Punkt, der durchaus schon in der Konzeptphase bedacht werden sollte, ist die Vorarbeit für eine mögliche Verfahrensbeschreibung, wenn diese – wie es beispielsweise im Anwendungsbereich des BayDSG[222] der Fall ist – beim erstmaligen Einsatz eines automatisierten Verfahrens vorgeschrieben ist. Die praktische Erfahrung zeigt, dass eine solche Verfahrensbeschreibung nachträglich nur mit sehr großer Mühe anzufertigen ist. Viele Details sind dann bereits in Vergessenheit geraten oder man hat kurz vor dem Launch einer Bibliotheks-App mit anderen Dingen zu kämpfen und keine Zeit mehr für eine Verfahrensbeschreibung. Dies führt mitunter dazu, dass mobile Apps vor der Aufnahme in das Verfahrensverzeichnis oder ohne die Freigabeerteilung durch den behördlichen Datenschutzbeauftragten an den Start gehen müssen. Dies ist zwar rechtlich möglich, aber kein befriedigender Zustand. Außerdem kann es später zu Beanstandungen durch die Datenschutzaufsichtsbehörden kommen.

II. Ausschreibungsphase/Suche eines geeigneten App-Entwicklers

Bei der Suche und Auswahl eines geeigneten App-Entwicklers empfiehlt es sich, auf eine Softwareagentur zu setzen, die nicht nur in technischer, sondern auch in datenschutzrechtlicher Hinsicht über das notwendige Fachwissen verfügt. Im Falle einer Ausschreibung sollte die datenschutzfreundliche Gestaltung der App daher mit in das Lastenheft aufgenommen werden. Außerdem ist es ratsam, sich Referenzen des potentiellen App-Entwicklers anzuschauen oder andere Apps, die er bereits erstellt hat. Im Falle einer Ausschreibung wäre es sogar denkbar, die Erarbeitung des gesamten Datenschutzkonzepts mit in die Ausschreibung hineinzunehmen. Die im Vorangegangenen in den Punkten I a) – j) genannten Empfehlungen müssten dann – nach Möglichkeit vollständig – von den App-Entwicklern berücksichtigt und in die Angebotserstellung integriert werden. Es ist klar, dass in diesem Fall höhere Kosten anfallen würden, da die Softwareagentur die bei ihnen anfallenden Kosten für da-

[222] Art. 26 BayDSG.

tenschutzrechtliche Beratung in das Angebot einpreisen müsste. Wenn der datenschutzfreundlichen App-Gestaltung ein hoher Stellenwert beigemessen wird, wozu ich dringend raten würde, sollte sich dies in einer entsprechend hohen Bepunktung dieses Aspekts im Rahmen der Angebotsbewertung niederschlagen.

III. Nach Festlegen des App-Entwicklers

Im Falle einer Ausschreibung sollte die Berücksichtigung datenschutzrechtlicher Aspekte gebührend im Pflichtenheft zum Ausdruck kommen. Dies muss überprüft werden, möglichst mit Hilfe kompetenter Unterstützung, beispielsweise in Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten. Ist der App-Entwickler auf andere Art und Weise festgelegt worden, ist es sinnvoll, das Thema Datenschutz an dieser Stelle noch einmal gemeinsam mit dem Entwickler durchzuplanen, möglicherweise ebenfalls in Kooperation mit dem behördlichen Datenschutzbeauftragten. Falls vorher noch nicht geschehen, könnten die einzelnen Schritte bzw. Empfehlungen aus Punkt I noch einmal gemeinsam durchgegangen werden.

IV. Entwicklungsphase/Umsetzungsphase

Die nächste Phase bildet die technische Erstellung der App. Die datenschutzrechtlichen Belange werden entsprechend dem in den vorhergehenden Schritten erstellen Konzept umgesetzt. An dieser Stelle ist nochmals besonderes Augenmerk darauf zu richten, welche Daten für welchen Zweck erhoben und welche Verarbeitungsprozesse durchgeführt werden.

IV. a) Dokumentation

An dieser Stelle empfiehlt es sich, eine Dokumentation anzulegen, und zwar nicht nur eine technische, sondern auch eine datenschutzrechtliche. Diese bildet später die Grundlage für die Verfahrensbeschreibung und mögliche Freigabeprozeduren.

IV. b) Umsetzung von Einwilligungen:

Spätestens in der Umsetzungs- bzw. der Entwicklungsphase muss geklärt werden, auf welche Gerätesensoren und -daten (Gerätenummern, Standortdaten, interne Speicher, ggf. die Kamera oder das Mikrophon) zugegriffen werden muss. Danach sollte festgelegt werden, welche Ein-

willigungen von den App-Nutzern eingeholt werden müssen und wie diese Einwilligungserklärungen technisch umgesetzt werden können. Idealerweise sollten die Einwilligungserklärungen bereits vor dem Download der App aus dem jeweiligen App-Store eingeholt werden. Wenn dies aus technischen Gründen nicht möglich ist, dann spätestens vor dem ersten Betrieb der App. Zu beachten ist hier, dass es bei der Gestaltung von Einwilligungen in technischer Hinsicht erhebliche Unterschiede zwischen den einzelnen Betreiberplattformen gibt. Dies ist insbesondere dann von Bedeutung, wenn eine App für mehrere Plattformen gleichzeitig entwickelt wird, z.B. für Apples iOS und Googles Android. Außerdem muss den App-Nutzern genau erläutert werden, wie sie die erteilten Einwilligungen in den Geräteeinstellungen jederzeit wieder rückgängig machen können. Auch hier sind betreiber- bzw. plattformabhängige Unterschiede zu beachten.

IV. c) Vereinbarungen zur Auftragsdatenverarbeitung

Ein letzter Punkt, dessen Beachtung sich in dieser Phase der App-Entwicklung unbedingt empfiehlt, ist der Abschluss von Vereinbarungen zur Auftragsdatenverarbeitung mit denjenigen Dritten, mit denen Daten zum ordnungsgemäßen Funktionieren der App ausgetauscht werden müssen (z.B. Serverbetreibern oder Lieferanten von Webcontent). Nach dem Abschluss solcher Vereinbarungen gelten sie in datenschutzrechtlicher Hinsicht nicht mehr als Dritte und der Datenaustausch mit ihnen ist rechtlich zulässig. Zum korrekten Abschluss solcher Vereinbarungen zur Auftragsdatenvereinbarung sind vertiefte rechtliche Kenntnisse erforderlich. Hier sollte die Bibliothek auf die Hilfe ihrer Rechtsabteilung oder derjenigen ihrer Trägerinstitution zurückgreifen (wie z.B. Universität, Gemeinde, etc.). Außerdem empfiehlt es sich, die entsprechenden Vertragsvorlagen anerkannter Datenschutzinstitutionen zu verwenden oder zumindest zu Rate zu ziehen.

IV. d) Impressum

Gemäß § 5 TMG müssen Bibliotheks-Apps, die als Telemediendienst einzustufen sind, über ein Impressum verfügen. Dieses sollte nach herrschender Meinung von jeder beliebigen Stelle innerhalb der App aus mit maximal zwei Schritten zu erreichen sein. Für Bibliotheks-Apps, die rein offline funktionieren und damit nicht dem TMG unterliegen, besteht prinzipiell keine Impressumspflicht. Dennoch empfiehlt es sich, dass

Bibliotheken als App-Anbieter auch in diesem Fall ein Impressum einbauen. Dies dient der Transparenz und Bibliotheken könnten auf diese Weise eine Vorbildrolle einnehmen.

IV. e) Datenschutzerklärung

§ 13 TMG zufolge müssen Bibliotheks-Apps, die einen Telemediendienst darstellen, eine Datenschutzerklärung aufweisen. Diese muss den Empfehlungen der deutschen Datenschutzaufsichtsbehörden zufolge App-spezifisch sein, d.h. es darf nicht einfach die Datenschutzerklärung von der Webseite verwendet oder gar einfach nur auf diese verlinkt werden. Für den verpflichtenden Inhalt einer App-spezifischen Datenschutzerklärung gibt es genaue Vorgaben.[223]

V. Usability-Tests der Beta-Version der App

Nach der technischen Fertigstellung der App sollte eine Beta-Version für Usability-Tests[224] mit nicht vorbelasteten Testpersonen genutzt werden. Gemeint ist in diesem Kontext ein Usability-Test, der sich nicht auf den gesamten Funktionsumfangs bezieht, sondern auf einen Teilaspekt, nämlich den Datenschutz: Sind Impressum und Datenschutzerklärung leicht auffindbar und gut verständlich? Wie kommen die Nutzer mit den notwendigen Einwilligungserklärungen zurecht? Ist auch hier alles verständlich formuliert? Es sollte darauf geachtet werden, dass die Grundfunktionen der App auch bei Nicht-Zustimmung nutzbar bleiben. Wer beispielsweise seine Einwilligung zur Verwendung seiner Standortdaten verweigert, sollte dennoch die Möglichkeit haben, Informationen wie Texte, Bilder, Audio- oder Videodateien zu bestimmten Points-of-Interest abzurufen, den Bibliotheks-OPAC über die App zu benutzen oder eine Auskunftsanfrage an die Bibliothek stellen zu können.

VI. Sicherstellen des technischen Datenschutzes

Nach der technischen Fertigstellung der App, aber noch mit einigem zeitlichen Abstand zum Produktiveinsatz ist es ratsam, sich noch einmal intensiver mit dem technischen Datenschutz auseinanderzusetzen, also mit Fragen der Serverabsicherung, der Sicherheit der Übertragungswege, der Verschlüsselung, des Loggings und der Datenlöschung. Werden hier

[223] Baumgartner, in: Baumgartner/Ewald (2016), Rn. 232.

[224] Hilpert/Gillitzer/Kuttner/Schwarz (2014), S. 28-30.

Defizite festgestellt, bleibt noch genügend Zeit für Nacharbeiten, denn keine Bibliotheks-App sollte mit mangelhaftem technischen Datenschutz an den Start gehen.

VII. Verfahrensbeschreibung erstellen

In vielen Fällen ist vor dem erstmaligen Einsatz eines automatisierten Verfahrens eine behördeninterne Freigabeerteilung vorgeschrieben. Nähere Einzelheiten dazu finden sich meist in den Landesdatenschutzgesetzen. Für das Land Bayern wird beispielsweise in Art. 26 Abs. 3 BayDSG bestimmt, dass dem behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz oder wesentlichen Änderungen eines automatisierten Verfahrens eine Verfahrensbeschreibung zur Verfügung gestellt wird, die bestimmte Angaben enthalten muss. Wenn – wie in diesem Praxisleitfaden vorgeschlagen – bereits in der Konzeptphase[225] und der Entwicklungs-/Umsetzungsphase[226] die entsprechenden Vorarbeiten geleistet wurden, dann sollte die vollständige Abfassung einer solchen Verfahrensbeschreibung eigentlich kein Problem darstellen. Falls das unterblieben ist, muss die Verfahrensbeschreibung dennoch angefertigt werden, aber vermutlich mit mehr Aufwand und möglicherweise auch mit einigen Verzögerungen im Projektzeitplan.

VIII. Gestaltung des zugehörigen Bereichs im App-Store

Unmittelbar vor dem Release der App muss im jeweiligen App-Store der entsprechende Bereich gestaltet werden. Neben einer Schilderung des Funktionsumfangs und der Auswahl einiger Screenshots der App-Oberfläche, die beide eher werbenden Charakter haben, müssen im App-Store auch einige Informationen untergebracht werden, die datenschutzrechtlich vorgeschrieben sind: Impressum, Datenschutzerklärung und ggf. Einwilligungserklärungen. Die unterschiedlichen Plattformanbieter bieten hier ganz verschiedene Möglichkeiten. Standard ist meist eine Verlinkung auf das Impressum und die Datenschutzerklärung im Webauftritt der Bibliothek. Dies ist allerdings nicht unbedingt die ideale Lösung, da der App-Nutzer dazu gezwungen wird, bereits vor dem Download und der erstmaligen Nutzung der App Datenübertragungsprozesse anzustoßen. Besser wäre es, das Impressum und die Datenschutzerklärung

[225] Oben Punkt I. j).

[226] Oben Punkt IV. a).

vollständig im App-Store zu hinterlegen. Dies sollte an sich problemlos möglich sein, da es sich jeweils um sehr kurze Texte bzw. geringe Datenvolumen handelt. Auch die Erklärung von Einwilligungen, z.B. zur Nutzung von Standortdaten oder zum Zugriff auf bestimmte Gerätesensoren bzw. -speicher, sollten nach Möglichkeit bereits im App-Store eingeholt werden. Bisher bieten allerdings nur wenige App-Store-Betreiber diese Möglichkeit.

4.2 Checkliste

Die Checkliste ist so konzipiert, dass sie von oben nach unten durchgearbeitet werden kann, immer entsprechend dem jeweiligen Fortschritt des App-Entwicklungsprozesses. Sie enthält genau 100 Schritte. Dieser engmaschige Aufbau wurde bewusst gewählt, um die in datenschutzrechtlicher Hinsicht vielfach unerfahrenen Projektverantwortlichen in den Bibliotheken möglichst intensiv zu begleiten und dadurch in die Lage zu versetzen, alle wesentlichen Herausforderungen auf dem Weg zur datenschutzfreundlichen Bibliotheks-App souverän zu meistern. Selbstverständlich ist es ohne weiteres möglich, einzelne Schritte der Checkliste zu überspringen, beispielsweise wenn keine Ausschreibung (Phase II.) vorgenommen oder kein Usability-Test (Phase V.) durchgeführt wird. Genauso ist es möglich, einzelne Schritte erneut abzuarbeiten, wenn dies vom Verlauf der App-Entwicklung her angezeigt erscheint.

Die Checkliste gliedert sich in vier Spalten. Die erste Spalte dient der Nummerierung der einzelnen Schritte von 01 bis 100, die zweite verweist auf die Kapitel innerhalb der vorliegenden Arbeit, in denen der jeweilige Schritt rechtlich erläutert wurde. Dadurch soll ein enger Bezug zur rechtlichen Analyse im 3. Kapitel hergestellt und den Anwendern der Checkliste gezeigt werden, wo sie sich bei Bedarf zu einem bestimmten Sachverhalt ausführlicher informieren können. Die dritte Spalte nennt die Frage- bzw. Aufgabenstellungen, die in den jeweiligen Schritten abgearbeitet werden sollen. In der vierten Spalte können diese als erledigt bzw. berücksichtigt abgehakt werden. Dies dient dazu, den Überblick zu behalten, welche Schritte bereits durchlaufen wurden und welche noch zu erledigen oder gegebenenfalls erneut zu durchlaufen sind.

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berücksichtigt
I. Beginn / Konzeptphase			
		I. a) Datenschutzfreundliche Gestaltung von Anfang an	
01		Ist die datenschutzfreundliche Gestaltung der App im Blick?	□
02	3.8	Soll der behördliche Datenschutzbeauftragte in die Planungen einbezogen werden?	□
03		Sollen die Datenschutzaufsichtsbehörden informiert oder um Beratung gebeten werden?(in der Regel nur bei Großprojekten oder in besonders sensiblen Fällen; im Bibliotheksbereich eher selten)	□
		I. b) Berücksichtigung des Datenschutzes im Zeitplan	□
04	3.3.6	Wurde Zeit eingeplant für den Abschluss von Vereinbarungen zur Auftragsdatenverarbeitung?	□
05	3.8.	Wurde Zeit eingeplant für das Freigabeverfahren für den erstmaligen Einsatz automatisierter Verfahren (falls vorgeschrieben)?	□
06	3.3.8.2	Wurde Zeit eingeplant für die datenschutzkonforme Gestaltung von Einwilligungserklärungen?	□
07	3.5.1 3.5.2	Wurde Zeit eingeplant für das Abfassen des Impressums und einer App-spezifischen Datenschutzerklärung?	□
08	3.6	Wurde Zeit eingeplant für die Umsetzung von Sicherungsmaßnahmen zur Gewährleistung eines effektiven technischen Datenschutzes?	□
		I. c) Arten der erhobenen Daten und Zweck der Datenerhebung	
09	3.3.3 3.3.4	Welche Arten von personenbezogenen Daten müssen erhoben werden, damit die App bestimmungsgemäß funktioniert?	□
10	3.3.7	Zu welchem Zweck werden die Daten erhoben?	□
11	3.3.7	Wurden die Prinzipien der Datenvermeidung bzw. der Datensparsamkeit beachtet?	□
		I. d) Klären der Rechtsgrundlage der Datenerhebung und -verarbeitung	
12	3.2	Welche datenschutzrechtlichen Bestimmungen sind anwendbar? (EU-Vorschriften, BDSG, Landesdatenschutzgesetze, TMG, ggf. TKG)	□
13	3.2 3.3.8.1	Gibt es für die geplante Datenerhebung und -verarbeitung eine Rechtsgrundlage?	□
14	3.3.8.2	Welche Einwilligungen müssen von den App-Nutzern eingeholt werden?	□

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berücksichtigt
		I. e) Prüfen der Realisierungsmöglichkeiten als reine Offline-App	
15	3.3.2 3.7	Muss die App zur Gewährleistung des Funktionsumfangs in irgendeiner Weise über das Internet kommunizieren?	□
16	3.2.2; 3.7	Ist eine Realisierung als reine Offline-App möglich?	□
17	3.5.2 3.7	Konsequenzen hieraus prüfen; ggf. weitere Bearbeitung dieser Checkliste ab Schritt 41.	□
		I. f) Apps mit Onlineanbindung	
18	3.2.2	Überprüfen, ob die App als Telemedium im Sinne des § 1 Abs. 1 TMG anzusehen ist.	□
19	3.3.6	Planen, mit welchen Servern die App über das Internet kommunizieren muss.	□
20	3.3.6	Kommuniziert die App lediglich mit den eigenen Servern, also den Servern der Bibliothek?	□
21	3.3.6	Kommuniziert die App mit den Servern Dritter?	□
	3.3.6	**I. g) Gestaltung der datenschutzrechtlich relevanten Beziehungen zu Dritten**	
22	3.3.2 3.3.6	Welche Datenaustauschprozesse mit Dritten finden statt?	□
23	3.3.6	Auf welchen rechtlichen Grundlagen finden die Datenaustauschprozesse statt?	□
24	3.3.6	Vorarbeiten zur Gestaltung der entsprechenden vertraglichen Regelungen (Auftragsdatenverarbeitungsvereinbarungen) durchführen.	□
25	3.3.6	Befinden sich die Auftragnehmer der Datenverarbeitung innerhalb der EU oder des EWR? (Vertragsvorlagen berücksichtigen)	□
26	3.3.6	Befinden sich die Auftragnehmer außerhalb der EU oder des EWR? (ggf. EU-Standardvertragsklauseln sowie aktuelle Empfehlungen der Datenschutzaufsichtsbehörden berücksichtigen)	□
		I. h) Einbindung von Webseiten der Bibliothek oder Dritter	
27	3.6	Werden Webseiten innerhalb der App angezeigt (In-App-Browsing)?	□
28	3.6	Sind Links, die zu Webseiten Dritter führen, eindeutig gekennzeichnet?	□
29	3.6	Planung eines Pop-Up-Fensters mit einem entsprechenden Warnhinweis, dass nun Webseiten einbezogen werden und dadurch ein erhöhtes Datenschutzrisiko besteht.	□

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berücksichtigt
		I. i) Überlegungen zur möglichen Standortdatenerhebung	
30	3.4	Soll die App Location-Based-Services bieten?	□
31	3.4	Auf welche Sensoren des mobilen Endgeräts (z.B. GPS-Sensor, Bluetooth-Empfänger, Gyrosensor, Kompass) soll zugegriffen werden?	□
32	3.4 3.7	Planen, ob die Location-Based-Services offline oder online erbracht werden.	□
33	3.4	Werden Standortdaten über das Internet übertragen?	□
34	3.4	Klären, an wen die Standortdaten übertragen werde sollen/müssen.	□
35	3.4.2	Klären, mit welcher Genauigkeit (Granularität) die Standortdaten übertragen werden müssen, damit die App ihren vollen Funktionsumfang entfalten kann.	□
36	3.4.2	Wurden die Empfehlungen der Artikel-29-Datenschutzgruppe zum Umgang mit Standortdaten berücksichtigt?	□
37	3.4 3.3.8.2	Planen, wie die Einholung der erforderlichen Einwilligungen des App-Nutzers technisch realisiert werden kann.	□
		I. j) Vorarbeiten für eine mögliche Verfahrensbeschreibung beim ersten Einsatz automatisierter Verfahren	
38	3.8	Ist vor dem Produktiveinsatz der App eine datenschutzrechtliche Freigabeerteilung vorgesehen? (v.a. Landesdatenschutzrecht beachten)	□
39	3.8	Z.B. gem. BayDSG: Berücksichtigen der Freigabeerteilung durch den behördlichen Datenschutzbeauftragten vor dem Einsatz der App.	□
40	3.8	Z.B. gem. BayDSG: Konzept für eine Verfahrensbeschreibung, anhand derer der behördliche Datenschutzbeauftragte die Freigabe erteilen kann (möglichst verständlich formuliert)	□
II. Ausschreibungsphase/Suche eines geeigneten App-Entwicklers			
41		Verfügt der App-Entwickler in datenschutzrechtlicher Hinsicht über die notwendige Expertise?	□
42		Referenzen des App-Entwicklers beachten / andere Apps des Entwicklers näher anschauen.	□
43		Bei Ausschreibung: Explizite Aufnahme der datenschutzfreundlichen App-Gestaltung in das Lastenheft.	□

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berücksichtigt
44		Bei Ausschreibung: Möglicherweise die Erarbeitung des gesamten Datenschutzkonzepts mit in die Ausschreibung integrieren.	□
45		Bei Ausschreibung: Hohe Bepunktung des Datenschutzaspekts im Rahmen der Angebotsbewertung.	□
46		Bei Ausschreibung: Möglicherweise Beteiligung von Experten an der Angebotsbewertung, z.B. dem behördlichen Datenschutzbeauftragten.	□
		III. Nach Festlegen des App-Entwicklers	
47		Nach der Ausschreibung: Werden datenschutzrechtliche Aspekte im Pflichtenheft gebührend berücksichtigt?	□
48		Sollten Datenschutzexperten, z.B. der behördliche Datenschutzbeauftragte, an dieser Beurteilung beteiligt werden?	□
49		In jedem Fall: Thema Datenschutz sollte mit dem App-Entwickler noch einmal ausführlich erörtert werden.	□
50		Einzelne Schritte (z.B. 04-40) dieser Checkliste sollten noch einmal gemeinsam mit dem App-Entwickler durchgegangen werden.	□
		IV. Entwicklungsphase/Umsetzungsphase	
		IV. a) Dokumentation	
51		Anlegen einer Dokumentation, in der alle datenschutzrechtlich relevanten Aspekte erfasst werden	□
52	3.8	Es sollte beachtet werden, dass die dokumentierten Aspekte im Hinblick auf eine mögliche Verfahrensbeschreibung bzw. Freigabeerteilung verwendet werden können.	□
		IV. b) Umsetzung von Einwilligungen	
53	3.4	Auf welche Gerätesensoren und -daten wird zugegriffen? (z.B. Gerätenummern, Standortdaten, Gyrosensor, interne Speicher, Kamera, Mikrophon o.ä.)	□
54	3.3.7 3.3.8.2 3.4.2	Welche Einwilligungen müssen dafür von den App-Nutzern eingeholt werden?	□
55	3.3.7 3.3.8.2	Wie sollen diese Einwilligungserklärungen technisch umgesetzt werden?	□
56	3.5.2	Idealerweise sollten die Einwilligungserklärungen bereits vor dem Download der App aus dem App-	□

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berücksichtigt
		Store eingeholt werden.	
57	3.5.2	Zumindest sollten die Einwilligungserklärungen vor dem ersten Betrieb der App eingeholt werden.	□
58	3.3.8.2	Berücksichtigen, dass es bei der Gestaltung der Einwilligungserklärungen zwischen den unterschiedlichen Plattformanbietern in technischer Hinsicht erhebliche Unterschiede gibt.	□
59	3.3.8.2	Der Nutzer muss seine Einwilligung bewusst und eindeutig erteilen (z.B. durch das Ankreuzen einer vorformulierten Antwort).	□
60	3.3.8.2	Die Einwilligung muss protokolliert werden.	□
61	3.3.8.2	Die App-Nutzer müssen den Inhalt der Einwilligung jederzeit abrufen können.	□
62	3.3.8.2	Den App-Nutzern muss genau erklärt werden, wie sie die Einwilligungserklärungen in den Einstellungen des jeweiligen mobilen Endgeräts wieder zurücknehmen können.	□
		IV. c) Vereinbarungen zur Auftragsdatenverarbeitung	
63	3.3.6	Abschluss von Auftragsdatenverarbeitungsvereinbarungen mit Serverbetreibern oder Contentanbietern.	□
64	3.3.6	Überprüfen, wer hierbei Unterstützung anbieten kann (Rechtsabteilung, behördlicher Datenschutzbeauftragter, etc.)	□
65	3.3.6	Es empfiehlt sich, Vertragsvorlagen anerkannter Datenschutzorganisationen zu verwenden.	□
		IV. d) Impressum	
66	3.5.1	Ist die Bibliotheks-App als Telemediendienst zu qualifizieren? Dann ist ein Impressum Pflicht.	□
67	3.5.1 3.7	Handelt es sich um eine reine Offline-App? Dann ist die Impressumsangabe rechtlich zwar nicht verpflichtend, aber aufgrund der Vorbildfunktion von Bibliotheken dennoch empfehlenswert.	□
68	3.5.1	Das Impressum sollte von jeder Stelle innerhalb der App in maximal zwei Schritten zu erreichen sein.	□
	3.5.1	Folgende Angaben sollten im Impressum vorhanden sein:	
69		- Name, Anschrift und E-Mail-Adresse des App-Anbieters	□
70		- Angaben zur schnellen Kontaktaufnahme, z.B. ein Kontaktformular oder eine Telefonnummer	□

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berücksichtigt
		Bei juristischen Personen, zu denen Bibliotheken zählen können, kommen noch folgende Angaben hinzu:	
71		- Rechtsform	□
72		- Name der Vertretungsberechtigten	□
73		- Registrierungsnummern wie z.B. Umsatzsteueridentifikationsnummer	□
74		- zuständige Aufsichtsbehörden	□
		IV. e) App-spezifische Datenschutzerklärung	
75	3.2.2 3.5.2	Ist die Bibliotheks-App als Telemediendienst zu qualifizieren? Dann ist eine App-spezifische Datenschutzerklärung Pflicht.	□
76	3.5.2 3.7	Handelt es sich um eine reine Offline-App? Dann ist die Angabe einer Datenschutzerklärung rechtlich zwar nicht verpflichtend, aber aufgrund der Vorbildfunktion von Bibliotheken dennoch empfehlenswert.	□
	3.5.2	Folgende Informationen gehören in der Regel zum verpflichtenden Inhalt einer App-spezifischen Datenschutzerklärung:	
77	3.3.5 3.5.2	Namentliche Bezeichnung der verantwortlichen Stelle, mit Adresse und Kontaktinformationen, ggf. Verweis auf Impressum	□
78	3.3.2 3.3.3 3.4	- Genaue Angabe und Erläuterung der Daten, die die App erhebt, einschließlich der Standortdaten und deren Genauigkeit (Granularität)	□
79	3.4	- Beschreibung der Gerätefunktionen und Sensoren, auf die die App zugreift	□
80	3.3.7	- Aufklärung über die Zwecke, zu denen die Daten erhoben werden	□
81	3.3.6	- Bezeichnung der Dritten, an die Nutzerdaten übermittelt werden sowie Erläuterung des Zwecks der Übermittlung	□
82	3.3.2 3.4.2	- Beschreibung der Einflussmöglichkeiten des Nutzes bezüglich der Erhebung, Nutzung und Verarbeitung seiner Daten	□
83		- Idealerweise sollte dem Nutzer genau erklärt werden, wie er einzelne Datenverwendungen in den App-Einstellungen oder den Einstellungen des mobilen Betriebssystems unterbindet	□

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berücksichtigt
84	3.3.8.2	- Kurze Erläuterung, welche Auswirkungen eine Verweigerung der Einwilligung für die App-Nutzung nach sich zieht	□
85	3.3.6	- Ggf. Informationen über die Datenverarbeitung außerhalb der EU bzw. des EWR sowie über die Rechtsgrundlage, auf denen die Übermittlung erfolgt (z.B. Standardvertragsklauseln)	□
V. Usability-Test der Beta-Version der App			
86		Usability-Test, der die Aspekte des Datenschutzes untersucht.	□
87	3.5.1 3.5.2	Sind Impressum und Datenschutzerklärung leicht auffindbar und verständlich formuliert?	□
88	3.3.8.2 3.4.2	Wie kommen die Nutzer (hier: Testnutzer im Rahmen des Usability-Tests) mit den notwendigen Einwilligungen zurecht?	□
89	3.4.2	Sind die Grundfunktionen der App auch bei Nicht-Zustimmung, beispielsweise zur Standortdatenerhebung, weiterhin nutzbar?	□
VI. Sicherstellen des technischen Datenschutzes			
90	3.3.7 3.6	Wurden die notwendigen technischen und organisatorischen Maßnahmen ergriffen?	□
91	3.6	Ist die Serverabsicherung gewährleistet?	□
92	3.6	Sind die Übertragungswege gesichert (Verschlüsselung)?	□
93	3.6	Funktioniert das Logging rechtskonform?	□
94	3.6	Ist die rechtskonforme Datenlöschung in den vorgeschriebenen Zeitabständen gewährleistet?	□
VII. Verfahrensbeschreibung erstellen			
95	3.8	Muss vor dem Produktiveinsatz der Bibliotheks-App ein datenschutzrechtliches Freigabeverfahren durchgeführt werden?	□
96	3.8	Wenn ja, dann Anfertigen einer Verfahrensbeschreibung anhand der Vorüberlegungen in der Konzeptphase (Schritte 38-40) und der Dokumentation (Schritte 51 f.), ggf. mit Hilfe eines entsprechenden Formulars.	□

Schritt	Bezug zu Kapitel	Fragestellungen / Aufgabenstellungen	Erledigt / Berück-sichtigt
VIII. Gestaltung des zugehörigen Bereichs im App-Store			
97	3.3.8.3 3.5.1 3.5.2	Es empfiehlt sich, im jeweiligen App-Store auch die den Datenschutz betreffenden Informationen zu platzieren (v.a. Impressum, Datenschutzerklärung, ggf. Einwilligungserklärungen).	□
98	2.1 2.2 3.3.8.2	Dabei müssen die Unterschiede bei den verschiedenen Plattformanbietern beachtet werden.	□
99	3.5.1 3.5.2	Idealerweise sollten Impressum und Datenschutzerklärung bereits vollständig im App-Store hinterlegt werden, nicht nur Links auf die jeweiligen Stellen im Webauftritt der Bibliothek.	□
100	3.3.8.2 3.4.2	Prüfen, ob der App-Store auch die Möglichkeit bietet, Einwilligungen der App-Nutzer einzuholen (wiederum plattformabhängig).	□

5 Zusammenfassung und Ausblick

Mit mobilen Apps stellen Bibliotheken ihre digitalen Bestände und zentralen Dienstleistungen in moderner und kundenorientierter Weise zur Verfügung. Sie kommen damit den Erwartungen und Gewohnheiten ihrer Nutzerinnen und Nutzer entgegen, von überall und zu jeder Zeit schnell und unkompliziert auf wesentliche Informationen zugreifen zu können. Außerdem leisten sie einen wichtigen Beitrag zur innovativen Präsentation und Vermittlung digitalisierter Kultur- und Bildungsgüter.

Bei der Entwicklung und beim Anbieten von Bibliotheks-Apps sind neben technischen und vertraglichen Gesichtspunkten auch zahlreiche datenschutzrechtliche Fragestellungen zu beachten. Diese sind mitunter ausgesprochen komplex und bedürfen vertiefter rechtlicher Kenntnisse. Bibliotheken müssen sich darüber im Klaren sein, dass sie in datenschutzrechtlicher Hinsicht eine hohe Verantwortung tragen. Wenn sie eine mobile App anbieten, sind nach geltender Rechtslage eindeutig sie selbst – und nicht etwa der App-Entwickler oder sonst irgendjemand – für die Einhaltung sämtlicher datenschutzrechtlich relevanter Rechtsvorschriften zuständig. Vielfach fehlt es in den Bibliotheken jedoch an der datenschutzrechtlichen Expertise, aber auch an der Einsicht, dass dieser Bereich überhaupt von Bedeutung ist. Die Folge ist, dass viele Bibliotheks-Apps über ein niedriges oder gar mangelhaftes Datenschutzniveau verfügen. Bei Überprüfungen durch die Datenschutzaufsichtsbehörden kann dies zu Beanstandungen und im schlimmsten Fall sogar dazu führen, dass bestimmte Apps nicht mehr angeboten werden dürfen. Soweit muss es allerdings nicht kommen, wenn einigen datenschutzrechtlichen Grundanliegen von Beginn der App-Entwicklung an Rechnung getragen wird.

Dass dies in Bibliotheken gelingen kann, ist das zentrale Anliegen der vorliegenden Masterarbeit. Dazu wurden alle wesentlichen datenschutzrechtlichen Themen rund um mobile Bibliotheks-Apps – angefangen von der Frage, welche Rechtsvorschriften denn eigentlich anwendbar sind, über die im App-Kontext wichtigen datenschutzrechtlichen Grundbegriffe und Grundprinzipien, die besondere Problematik der Apps mit Standortdatenerhebung, die Informationspflichten gegenüber den App-Nutzern in Form von Impressum und Datenschutzerklärungen bis hin zum technischen Datenschutz und der Ausgestaltung der innerbehördlichen Datenschutzkontrolle – analysiert und so zusammenge-

fasst, dass sie auch für interessierte Bibliotheksmitarbeiterinnen und -mitarbeiter ohne vertiefte rechtliche Kenntnisse nachvollziehbar sind. Im Praxisleitfaden wurden diese Ergebnisse der rechtlichen Analyse zu Empfehlungen und einer Checkliste aggregiert, die die Projektverantwortlichen in den Bibliotheken Schritt für Schritt durch den App-Entwicklungsprozess begleiten sollen. Werden die darin enthaltenen Punkte berücksichtigt, ist es – entgegen der landläufigen Meinung[227] – durchaus möglich, innovative, ansprechend gestaltete, intuitiv zu bedienende und nutzbringende Bibliotheks-Apps zu entwickeln, die zugleich datenschutzfreundlich sind. Dies kann allerdings nur gelingen, wenn Datenschutz und technische Innovation bzw. Datenschutz und Anwenderfreundlichkeit nicht als Widersprüche, sondern als verschiedene, sich komplementär ergänzende Aspekte der Kundenorientierung begriffen werden.

[227] Taeger, in: Solmecke/Taeger/Feldmann (2013), Kap. 5 Rn. 2-13.

6 Literaturverzeichnis

ALBRECHT, Jan Philipp (2016): Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog. In: Computer und Recht, 32. Jahrgang, Heft 2/2016, S. 88-98.

APPBRAIN/TECHCRUNCH (2016). Anzahl der angebotenen Apps in den Top App-Stores im August 2016. In: Statista – Das Statistik-Portal. Online verfügbar unter folgender URL: https://de.statista.com/statistik/daten/studie/208599/umfrage/anzahl-der-apps-in-den-top-app-stores/ (Letzter Zugriff: 15.02.2017).

APPLE/TECHCRUNCH (2016). Kumulierte Anzahl der weltweit heruntergeladenen Apps aus dem Apple App Store von Juli 2008 bis September 2016 (in Milliarden). In: Statista – Das Statistik-Portal. Online verfügbar unter folgender URL: https://de.statista.com/statistik/daten/studie/20149/umfrage/anzahl-der-getaetigten-downloads-aus-dem-apple-app-store/ (Letzter Zugriff: 15.02.2017).

ARTIKEL-29-DATENSCHUTZGRUPPE (2011): Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten. WP 185. Brüssel. Online verfügbar unter folgender URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf (Letzter Zugriff: 15.02.2017).

ARTIKEL-29-DATENSCHUTZGRUPPE (2013): Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten. WP 202. Brüssel. Online verfügbar unter folgender URL: http://www.lda.bayern.de/MobileApplikationen/wp202_de.pdf (Letzter Zugriff: 15.02.2017).

BAUMGARTNER, Ulrich / EWALD, Konstantin (2016): Apps und Recht, 2. Auflage, München (Zitierform: Bearbeiter, in: Baumgartner/Ewald (2016)).

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT (2013): App-Prüfung zeigt erhebliche Mängel beim Datenschutz". Pressemitteilung des Bayerischen Landesamtes für Datenschutzaufsicht vom 14.05.2013). Online verfügbar unter folgender URL: https://www.lda.bayern.de/media/pm2013_03.pdf (Letzter Zugriff: 15.02.2017).

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT (2014): Erneute App-Prüfung zeigt weiterhin erhebliche Mängel beim Datenschutz. Pressemitteilung des Bayerischen Landesamtes für Datenschutzaufsicht vom 26.05.2014). Online verfügbar unter folgender URL: https://www.lda.bayern.de/media/pm2014_08.pdf (Letzter Zugriff: 15.02.2017).

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT (2015): 6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2013/2014. Ansbach.

BEIERSMANN, Stefan (2015): Apple entfernt mehr als 250 „Schnüffel"-Apps aus dem App Store. In: ZDNet, Online-Artikel vom 20.10.2015. Online verfügbar unter folgender URL: http://www.zdnet.de/88249592/apple-entfernt-mehr-als-250-schnueffel-apps-aus-dem-app-store/ (Letzter Zugriff: 15.02.2017).

BITKOM (2016): Zukunft der Consumer Technology – 2016. Marktentwicklung, Schlüsseltrends, Mediennutzung, Konsumentenverhalten, Neue Technologien, Berlin 2016. Online verfügbar unter folgender URL: http://www.bitkom-research.de/WebRoot/Store19/Shops/63742557/MediaGallery/Press/2016/September/160831-CT-Studie-2016-online.pdf (Letzter Zugriff: 15.02.2017).

BODDEN, Eric / RASTHOFER, Siegfried / RICHTER, Philipp / ROßNAGEL, Alexander (2013): Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps. Technische Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps. In: Datenschutz und Datensicherheit, Heft 11/2013, S. 720-725.

BODENSCHATZ, Nadine (2010): Der europäische Datenschutzstandard, Frankfurt a. M. (Europäische Hochschulschriften, Bd. 5083).

BÖTTGER, Klaus-Peter (2009): Basiskenntnis Bibliothek. Eine Fachkunde für Fachangestellte für Medien- und Informationsdienste – Fachrichtung Bibliothek, 4. Auflage, Bad Honnef.

BRENNSCHEIDT, Kirstin (2013): Cloud Computing und Datenschutz, Baden-Baden (Internet und Recht, Bd. 13).

CEYNOWA, Klaus (2016): „Leuchtfeuer" in der Bayerischen Staatsbibliothek. Beacons-Technologie zur digitalen Indoor-Navigation für Bibliotheksbesucher. In: Bibliotheksforum Bayern, 10. Jahrgang, 2016, Heft 1/2016, S. 13-16.

CEYNOWA, Klaus / HERMANN, Martin (2013): Nach der Tour mit Ludwig II noch ein Blick ins Gebetbuch der Haremsdame Düsdidil. Die mobilen digitalen Angebote der Bayerischen Staatsbibliothek. In: Forum Bibliothek und Information, 65. Jahrgang, Heft 5/2013, S. 360-363.

COMANS, Clemens David (2012): Ein „modernes europäisches Datenschutzrecht. Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung, Frankfurt a. M. (Kölner Schriften zu Recht und Staats, Bd. 48).

DER BAYERISCHE LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ (2015): 26. Tätigkeitsbericht. Berichtszeitraum 2013/2014. München. Online verfügbar unter folgender URL: https://www.datenschutz-bayern.de/tbs/tb26/tb26.pdf (Letzter Zugriff: 15.02.2017).

DEUTSCHER BIBLIOTHEKSVERBAND (2013): Bibliotheken im Spannungsfeld zwischen Datenschutz und digitalen Services. Presserklärung vom 13.11.2013. Online verfügbar unter folgender URL: http://www.bibliotheksverband.de/fileadmin/user_upload/DBV/positionen/2013_11_13_Bibliotheken_im_Spannungsfeld.pdf (Letzter Zugriff: 15.02.2017).

DÜSSELDORFER KREIS (2014): Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter. Ansbach. Online verfügbar unter folgender URL: http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_App.pdf;jsessionid=0B1658FEB8A4381873B8C3BB4CCD02D2.1_cid354?__blob=publicationFile&v=3 (Letzter Zugriff: 15.02.2017).

FORWARDADGROUP (2016): Wie viele Apps haben Sie auf Ihrem Smartphone installiert? Statista – Das Statistik-Portal. Online verfügbar unter folgender URL:

https://de.statista.com/statistik/daten/studie/162374/umfrage/durchschnittliche-anzahl-von-apps-auf-dem-handy-in-deutschland/ (Letzter Zugriff: 15.02.2017).

GANTERT, KLAUS (2015): Wandel, Vielfalt und Kooperation – Aufgaben, Typen und Träger von Bibliotheken. In: GRIEBEL, Rolf / SCHÄFFLER, Hildegard / SÖLLNER, Konstanze (Hrsg.), Praxishandbuch Bibliotheksmanagement, Band 1, Berlin/Boston (De Gruyter Reference), S. 5-16.

GIERSCHMANN, Sibylle (2016): Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt. In: Zeitschrift für Datenschutz, 6. Jahrgang, Heft 1/2016, S. 51-55.

GOLA, Peter / SCHOMERUS, Rudolf (2015): BDSG. Bundesdatenschutzgesetz. Kommentar, 12. Auflage, München.

GOLTZ, Julia (2014): Mobile Applikationen für Bibliotheken im deutschsprachigen Raum. In: ZIB-Report 15-49. Online-verfügbar unter folgender URL: https://opus4.kobv.de/opus4-zib/frontdoor/index/index/docId/4693 (Letzter Zugriff: 10.04.2017).

GOLTZ, Julia (2015): Mobile Applikationen für Bibliotheken im deutschsprachigen Raum. Aktualisierte und erweiterte zweite Version. In: ZIB-Report 15-49. Online-verfügbar unter folgender URL: https://opus4.kobv.de/opus4-zib/frontdoor/index/index/docId/5624 (Letzter Zugriff: 15.02.2017).

HAAR, Tobias (2013): Älter geworden. Juristische Vorgaben für mobile Apps nehmen zu. In: heise online, Online-Artikel vom 04.03.2013. Online verfügbar unter folgender URL: http://heise.de/-1814007 (Letzter Zugriff: 15.02.2017).

HENNIG, Nicole (2014): Apps for Librarians. Using the Best Mobile Technology to Educate, Create, and Engage, Santa Barbara u.a.

HERDEGEN, Matthias (2015): Europarecht, 17. Auflage, München (Grundrisse des Rechts).

HIJMANS, Hielke / LANGFELDT, Owe (2012): Datenschutz in der Europäischen Union. In: SCHMIDT, Jan-HINRIK / WEICHERT, Thilo (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen, Bonn (Schriftenreihe der Bundeszentrale für politische Bildung, Bd. 1190), S. 403-411.

HILDEBRANDT, Andreas / LUTHIGER, Jörg / STAMM, Christoph / YEREAZTIAN, Chris (2012): Eine Kategorisierung mobiler Applikationen. In: IMVS Fokus Report 2012, S. 27-32.

HILPERT, Wilhelm / GILLITZER, Berthold / KUTTNER, Sven / SCHWARZ, Stephan (2014): Benutzungsdienste in Bibliotheken. Bestands- und Informationsvermittlung, Berlin/Boston (Bibliotheks- und Informationspraxis, Bd. 52).

HLADJIK, Jörg (2013): Datenschutzrechtliche Anforderungen für mobile Apps. In: Datenschutz-Berater, 37. Jahrgang, Heft 4/2013, S. 92-93.

HOFFMANN, Christian (2013): Apps der öffentlichen Verwaltung. Rechtsfragen des Mobile Government. In: MultiMedia und Recht, 13. Jahrgang, Heft 10/2013, S. 631-636.

IFD ALLENSBACH (2016): Anzahl der Internetnutzer in Deutschland, die das Internet über das Handy oder Smartphone nutzen, von 2013 bis 2016 (in Millionen). In: Statista – Das Statistik-Portal. Online verfügbar unter folgender URL: https://de.statista.com/statistik/daten/studie/170557/umfrage/internutzung-ueber-das-handy-oder-smartphone/ (Letzter Zugriff: 15.02.2017).

INITIATIVE D21 (2015): eGovernment Monitor 2015. Nutzung und Akzeptanz von elektronischen Bürgerdiensten im internationalen Vergleich. Berlin.

INITIATIVE D21 (2016): D21-Digital-Index. Jährliches Lagebild zur digitalen Gesellschaft, Berlin 2016.

INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS (2015): Stellungnahme der International Federation of Library Associations and Institutions (IFLA) vom 14.08.2015 zum Datenschutz in Bibliotheken. Online verfügbar unter folgender URL: http://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment-de.pdf (Letzter Zugriff: 15.02.2017).

JOHNSON, Larry / ADAMS-BECKER, Samantha / ESTRADA, Victoria / FREEMAN, Alex (2014). NMC Horizon Report 2014 – Edition Bibliotheken. Austin.

KATZENBERGER, Ruth / TALKE, Armin (2015): Die Privatsphäre der Nutzer fördern. Das müssen Bibliotheken beim Datenschutz beachten. Zusätzliche Vorschriften für Cloud-Lösungen. In: Forum Bibliothek und Information, 67. Jahrgang, Heft 11/2015, S. 684-687.

KRAMER, André (2016): Berührt, geführt. Indoor-Navigation für die Bayerische Staatsbibliothek. In: c't – Magazin für Computer-Technik, 2016, Heft 7/2016, S. 36.

KRAMER, Philipp (2014): Welche Datenschutzanforderungen hat eine App? Neue Checkliste der Aufsichtsbehörden. In: Datenschutz-Berater, 38. Jahrgang, Heft 7-8/2014, S. 155-156.

KORENG, ANSGAR / LACHENMANN, MATTHIAS (Hrsg.) (2014): Formularhandbuch Datenschutzrecht, München (Zitierform: Bearbeiter, in: Koreng/Lachenmann (2014)).

KÜHLING, Jürgen / MARTINI, Mario (2016): Die Datenschutz-Grundverordnung. Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? In: Europäische Zeitschrift für Wirtschaftsrecht, 27. Jahrgang, Heft 12/2016, S. 448-454.

KÜHLING, Jürgen / MARTINI, Mario et al. (2016): Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf. Münster.

KÜHLING, Jürgen / SEIDEL, Christian / SIVRIDIS, Anastasios (2015): Datenschutzrecht, 3. Auflage, München.

LEHNARD-BUCH, Susanne (2012): Mobile Nutzung bibliothekarischer Services. Anforderungen an Bibliotheken mit heterogenen Zielgruppen – Explorative Untersuchung am Beispiel der Regionalbibliotheken des Landesbibliothekszentrums

Rheinland-Pfalz. Köln (Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft, Bd. 65).

LOBER, Andreas / FALKER, Frank (2013): Datenschutz bei mobilen Endgeräten – Roadmap für App-Anbieter. In: Kommunikation und Recht, 16. Jahrgang, Heft 6/2013, S. 357-364.

MARLY, Jochen (2014): Praxishandbuch Softwarerecht. Rechtsschutz und Vertragsgestaltung. Urheberrecht, Patentrecht, Pflichtverletzungen, Vertragsgestaltung, Allgemeine Geschäftsbedingungen, 6. Auflage, München.

MASKE, Philipp (2012): Mobile Applikationen. Interdisziplinäre Entwicklung am Beispiel des Mobile Learning, Band 1, Wiesbaden.

NENTWICH, Boris (2015): Datenschutz ist eine Herkulesaufgabe. Was der Bibliotheksdienstleister OCLC für die Datensicherheit tut – auch in der Cloud. In: Forum Bibliothek und Information, 67. Jahrgang, Heft 11/2015, S. 691-693.

NIETZER, Petra (2015): Praktisch – aber auch sicher? Bibliothekssoftware aus der Cloud. Das Beispiel des Bibliotheksdienstleisters datronic. In: Forum Bibliothek und Information, 67. Jahrgang, Heft 11/2015, S. 694 f.

OBERBECK, DAVID (2015): Die Beacon-Technologie und der Datenschutz. In: Datenschutz-Berater, 39. Jahrgang, Heft 2/2015, S. 30-31.

ODRICH, Peter / MÖRER-FUNK, Axel (2013): Taschenlampen-APP entpuppt sich als kleines Spionageprogramm. In: INGENIEUR.de. Online-Artikel vom 9.12.2013. Online verfügbar unter folgender URL: http://www.ingenieur.de/Themen/Smartphones-Tablets-Co/Taschenlampen-APP-entpuppt-kleines-Spionageprogramm (Letzter Zugriff: 15.02.2017).

OPPERMANN, Thomas / CLASSEN, Claus / NETTESHEIM, Martin (2014): Europarecht. Ein Studienbuch, 6. Auflage, München (Juristische Kurz-Lehrbücher).

PFEIFENBERGER, Regina (2010): Pocket Library. Bibliothekarische Dienstleistungen für Smartphones, Berlin (Berliner Handreichungen zur Bibliotheks- und Informationswissenschaft, Bd. 266).

POHLA, Hans-Bodo (2011): Bibliothekarische Apps. Untersuchung hinsichtlich der technischen Realisierung und des Nutzens, Wiesbaden 2011 (B.I.T.online – Innovativ, Bd. 34).

REIMER, Helmut (2013): Apps mit Datenschutzmängeln. In: Datenschutz und Datensicherheit, 37. Jahrgang, Heft 8/2013, S. 549.

ROßNAGEL, Alexander (2016): Zukunftsfähigkeit der Datenschutz-Grundverordnung. In: Datenschutz und Datensicherheit, 40. Jahrgang, Heft 9/2016, S. 553f.

SACHS, Andreas / MEDER, Miriam (2013): Datenschutzrechtliche Anforderungen an App-Anbieter. Prüfungen am Beispiel von Android-Apps. In: Zeitschrift für Datenschutz, 3. Jahrgang, Heft 7/2013, S. 303-308.

SCHERSCHEL, Fabian (2013): Millionenfach installierte Android-App schnüffelte Nutzerdaten aus. In: heise online, Online-Artikel vom 06.12.2013. Online verfügbar unter folgender URL: http://heise.de/-2062105 (Letzter Zugriff: 15.02.2017).

SCHMITZ, Roland (2015): Datensparsamkeit steht an oberster Stelle. Technische Maßnahmen zum Datenschutz an Hochschulen und wissenschaftlichen Bibliotheken in Baden-Württemberg. In: Forum Bibliothek und Information, 67. Jahrgang, Heft 11/2015, S. 696-698.

SCHNEIDER, Uwe (Hrsg.) (2012): Taschenbuch der Informatik, 7. Auflage, München.

SELENT, Markus (2013): Apps und das Telemediengesetz. In: Datenschutz-Berater, 37. Jahrgang, Heft 2/2013, S. 40 f.

SIMITIS, Spiros (2011): Bundesdatenschutzgesetz. 7. Auflage. München (Nomos-Kommentar) (Zitierform: Bearbeiter in: Simitis (2011)).

SOLMECKE, Christian / TAEGER, Jürgen / FELDMANN, Thorsten (Hrsg.) (2013): Mobile Apps. Rechtsfragten und rechtliche Rahmenbedingungen, Berlin/Boston (De Gruyter Praxishandbuch) (Zitierform: Bearbeiter, in: Solmecke/Taeger/Feldmann (2013)).

STATISTA (2017): Umsatz im Apple App Store und Google Play Store weltweit in den Jahren 2014 bis 2016 (in Milliarden US-Dollar). Statista – Das Statistik-Portal. Online verfügbar https://de.statista.com/statistik/daten/studie/180896/umfrage/apple-app-store-vs-google-playstore-umsatz (Letzter Zugriff: 15.02.2017).

TAEGER, Jürgen (2014): Datenschutzrecht. Einführung, Frankfurt a. M. (Schriftenreihe Kommunikation & Recht).

TAEGER, Jürgen / ROSE, Edgar (2016): Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes. In: Betriebs-Berater, 71. Jahrgang, Heft 2016, S. 819-831.

TINNEFELD, Marie-Theres / BUCHNER, Benedikt / PETRI, Thomas (2012): Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Auflage, München.

VENZKE-CAPRARESE, Sven (2014): Standortlokalisierung und personalisierte Nutzeransprache mittels Bluetooth Low Energie Beacons. Datenschutzrechtliche Rahmenbedingungen einer möglicherweise bald alltäglichen Datenverarbeitung. In: Datenschutz und Datensicherheit, 38. Jahrgang, Heft 12/2014, S. 839-844.

VENZKE-CAPRARESE, Sven (2015): Google Universal Analytics und iBeacons. Neue Möglichkeiten zur Verknüpfung von On- und Offlineaktivitäten. In: IT-Rechtsberater, 15. Jahrgang, Heft 4/2015, S. 97-99.

Mobile Apps für Smartphones und Tablet-Computer erfreuen sich immer größerer Beliebtheit. Auch zahlreiche öffentliche Institutionen und Körperschaften wie Gemeinden, Städte, Ministerien, Universitäten, Museen, Theater und Bibliotheken versuchen, die Vorteile mobiler Apps im Bereich des E-Government und zur Verwaltungsvereinfachung zu nutzen.

Neben technischen und vertraglichen Gesichtspunkten sind es vor allem datenschutzrechtliche Fragestellungen, die in der Praxis immer wieder Probleme bereiten. Ziel dieser Arbeit ist, die entsprechenden rechtlichen Vorgaben gut verständlich zusammenzufassen. Besonderes Gewicht liegt auf der Entwicklung eines Praxisleitfadens mit Empfehlungen und einer Checkliste, der praxisgerecht erläutert, was bei der Konzeption, der technischen Realisierung und dem Produktiveinsatz mobiler Apps aus datenschutzrechtlicher Sicht zu beachten ist.

Die Darstellung ist primär auf den Bibliotheksbereich ausgerichtet. Wesentliche Teile des Praxisleitfadens eignen sich aber auch zur Nutzung durch andere Einrichtungen der öffentlichen Verwaltung.

ISBN 978-3-7376-0294-5