ARTIKEL-29-DATENSCHUTZGRUPPE

00461/13/DE
WP 202

Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten

Angenommen am 27. Februar 2013

Zusammenfassung

Für alle gebräuchlichen intelligenten Endgeräte sind Hunderttausende verschiedener Apps von zahlreichen App-Stores erhältlich. Berichten zufolge werden täglich mehr als 1600 neue Apps in App-Stores angeboten. Ein durchschnittlicher Smartphone-Nutzer lädt 37 Apps auf sein Gerät herunter. Apps können dem Endnutzer entweder für geringe Anfangskosten oder auch kostenlos zur Verfügung gestellt werden. Die Nutzerbasis kann sich auf wenige Personen beschränken, aber auch vielen Millionen Nutzer umfassen.

Auf dem jeweiligen Endgerät können Apps Daten (beispielsweise vom Nutzer auf dem jeweiligen Gerät gespeicherte Daten oder Sensordaten wie z. B. Standortdaten) in großem Umfang erfassen und verarbeiten, um dem Endnutzer neue und innovative Dienstleistungen anbieten zu können. Die Daten können jedoch – gewöhnlich zur Erzielung von Einnahmen – in einer Weise weiterverarbeitet werden, die dem Endnutzer nicht bewusst ist und vom Endnutzer auch nicht gewünscht wird.

App-Entwickler, die mit den Datenschutzbestimmungen nicht vertraut sind, können erhebliche Risiken für die Privatsphäre und den Ruf von Nutzern intelligenter Endgeräte verursachen. Die wichtigsten Datenschutzrisiken für Endnutzer sind die mangelnde Transparenz und die mangelnde Kenntnis der von einer App ausgeführten Verarbeitungen sowie das Fehlen einer expliziten Einwilligung des Endnutzers vor der Verarbeitung. Unzureichende Sicherheitsmaßnahmen, ein offenkundiger Trend zur Datenmaximierung und die ungenaue Festlegung der Zwecke, für die personenbezogene Daten erfasst werden, erhöhen die Datenschutzrisiken bei Apps unter den gegenwärtigen Umständen zusätzlich.

Ein hohes Risiko für den Datenschutz besteht auch infolge des Umfangs der Fragmentierung unter den zahlreichen Akteuren im Umfeld der Entwicklung von Apps. Zu diesen Akteuren gehören Entwickler und Eigentümer von Apps, App-Stores, Hersteller von Betriebssystemen und Endgeräten sowie andere Dritte, die an der Erfassung und Verarbeitung personenbezogener Daten von intelligenten Endgeräten beteiligt sein können (z. B. Anbieter von Analyse- und Werbedienstleistungen). Die meisten Schlussfolgerungen und Empfehlungen in dieser Stellungnahme sind an App-Entwickler gerichtet (da diese am stärksten auf die genaue Art und Weise Einfluss nehmen können, in der die Verarbeitung erfolgt oder in der Informationen über die App vermittelt werden). Um die höchsten Standards für den Datenschutz und den Schutz der Privatsphäre zu erreichen, müssen die App-Entwickler jedoch häufig mit anderen Parteien im App-Ökosystem zusammenarbeiten. Dies ist insbesondere in Bezug auf die Sicherheit wichtig, da die aus zahlreichen Akteuren bestehende Kette in diesem Bereich immer nur so stark ist wie das schwächste Glied.

Zahlreiche auf einem intelligenten mobilen Endgerät verfügbare Daten sind personenbezogene Daten. Der geltende Rechtsrahmen in diesem Bereich ergibt sich aus der Datenschutzrichtlinie sowie aus den in der Datenschutzrichtlinie für elektronische Kommunikation enthaltenen Vorschriften zum Schutz mobiler Endgeräte als Teil der Privatsphäre der Nutzer. Diese Vorschriften gelten unabhängig vom Standort des App-Entwicklers oder vom App-Store für jede App, die an App-Nutzer in der EU vertrieben wird.

Die vorliegende Stellungnahme der Datenschutzgruppe verdeutlicht den Rechtsrahmen für die Verarbeitung personenbezogener Daten bei der Entwicklung, Verbreitung und Nutzung von Apps auf intelligenten Endgeräten. Dabei liegt der Schwerpunkt auf der Einwilligungsanforderung, den Grundsätzen der Zweckbindung und der Datenminimierung,

der Notwendigkeit angemessener Sicherheitsmaßnahmen, der Verpflichtung zu einer korrekten Aufklärung der Endnutzer, den Rechten der Endnutzer, angemessenen Speicherfristen und insbesondere der Verarbeitung der von Kindern und über Kinder erfassten Daten nach Treu und Glauben.

Inhaltsverzeichnis

1. Einleitung

Apps sind Softwareanwendungen, die häufig für eine bestimmte Aufgabe entwickelt werden und für eine bestimmte Gruppe intelligenter Endgeräte wie Smartphones, Tablet-Computer und Fernsehgeräte mit Internetanschluss bestimmt sind. Sie organisieren Informationen in für die spezifischen Eigenschaften des jeweiligen Endgeräts geeigneter Form und interagieren häufig eng mit der Hardware und den Funktionen des auf den Geräten installierten Betriebssystems.

Für jede verbreitete Art von intelligenten Endgeräten sind in zahlreichen App-Stores Hunderttausende von Apps erhältlich. Apps werden für ein breites Spektrum von Zwecken eingesetzt: Internetzugriff, Kommunikation (E-Mail, Telefonie und webbasierte Nachrichten), Unterhaltung (Spiele, Filme/Videos und Musik), soziale Netzwerke, Online-Banking, standortbezogene Dienste usw. Berichten zufolge werden täglich mehr als 1600 neue Apps in App-Stores angeboten.[1] Der durchschnittliche Smartphone-Nutzer lädt 37 Apps auf sein Gerät herunter.[2] Apps können dem Endnutzer entweder für geringe Anfangskosten oder auch kostenlos zur Verfügung gestellt werden. Die Nutzerbasis kann sich auf wenige Personen beschränken, aber auch vielen Millionen Nutzer umfassen.

Das zugrunde liegende Betriebssystem umfasst auch Software- oder Datenstrukturen, die für die Kerndienste des intelligenten Endgeräts wichtig sind (z. B. das Adressbuch eines Smartphones). Das Betriebssystem ist darauf ausgelegt, diese Komponenten über Programmierschnittstellen (APIs) für Apps nutzbar zu machen. Diese Programmierschnittstellen bieten Zugriff auf die zahlreichen Sensoren, die in intelligenten Endgeräten vorhanden sein können. Solche Sensoren sind beispielsweise ein Gyroskop, ein digitaler Kompass und ein Beschleunigungssensor zur Ermittlung der Geschwindigkeit und der Richtung von Bewegungen, Kameras an Vorder- und Rückseite zur Aufnahme von Videos oder Fotos und ein Mikrofon für Audioaufnahmen. Intelligente Endgeräte können auch mit Näherungssensoren ausgestattet sein[3] und über zahlreiche Netzschnittstellen verfügen (z. B. Wi-Fi, Bluetooth, NFC oder Ethernet). Schließlich kann durch Geolokalisierungsdienste der Standort eines Geräts präzise bestimmt werden (siehe Beschreibung in WP29, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten intelligenter mobiler Endgeräte[4]). Art, Genauigkeit und Messhäufigkeit dieser Sensordaten sind je nach Gerät und Betriebssystem unterschiedlich.

Über die Programmierschnittstellen können App-Entwickler solche Daten fortlaufend erfassen, auf Kontaktdaten zugreifen oder Kontaktdaten erstellen, E-Mails, SMS oder

---

[1] Bericht in ConceivablyTech vom 19. August 2012, abrufbar unter www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of; zitiert von Kamala D. Harris, Attorney General California Department of Justice, *Privacy on the go, Recommendations for the mobile ecosystem*, Januar 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[2] Dies ist ein weltweiter Schätzwert von ABI Research für 2012, http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o.

[3] Ein Sensor, der das Vorhandensein eines physischen Objekts berührungsfrei ermitteln kann; siehe http://www.w3.org/TR/2012/WD-proximity-20121206/.

[4] Siehe Stellungnahme 13/2011 der Artikel-29-Datenschutzgruppe zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten (Mai 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf.

Nachrichten im Rahmen eines sozialen Netzwerks senden, Inhalte von SD-Karten lesen, ändern oder löschen, Audioaufnahmen erstellen, die Kamera nutzen und auf gespeicherte Bilder zugreifen, den Telefonstatus und die Gerätekennungen lesen, die globalen Systemeinstellungen ändern und den Standby-Modus deaktivieren. Außerdem können Programmierschnittstellen Informationen über das Gerät selbst in Form einer oder mehrerer eindeutiger Kennungen sowie Informationen über andere installierte Apps bereitstellen. Die Daten können jedoch – gewöhnlich zur Erzielung von Einnahmen – in einer Weise weiterverarbeitet werden, die dem Endnutzer nicht bewusst ist und vom Endnutzer auch nicht gewünscht wird.

Mit dieser Stellungnahme soll der Rechtsrahmen für die Verarbeitung personenbezogener Daten bei der Verbreitung und Nutzung von Apps auf intelligenten Endgeräten beschrieben werden. Außerdem sollen weitere Verarbeitungen betrachtet werden, die möglicherweise außerhalb der App erfolgen (z. B. die Nutzung der erfassten Daten zur Erstellung von Profilen und Nutzer-Zielgruppen). In der Stellungnahme werden die wichtigsten Datenschutzrisiken analysiert, die unterschiedlichen beteiligten Parteien beschrieben und die jeweiligen gesetzlichen Pflichten dieser Akteure erläutert. Zu diesen Akteuren gehören App-Entwickler, App-Eigentümer, App-Stores, Hersteller von Geräten und Betriebssystemen und sonstige Dritte, die an der Erfassung und Verarbeitung personenbezogener Daten von intelligenten Endgeräten beteiligt sein können (z. B. Anbieter von Analyse- und Werbedienstleistungen).

Schwerpunkte der Stellungnahme sind die Einwilligungsanforderung, die Grundsätze der Zweckbindung und der Datenminimierung, die Notwendigkeit angemessener Sicherheitsmaßnahmen, die Verpflichtung zur korrekten Aufklärung der Endnutzer, die Rechte der Endnutzer und angemessene Speicherfristen sowie insbesondere die Verarbeitung erfasster Daten von Kindern und über Kinder nach Treu und Glauben.

Der Gegenstandsbereich der Stellungnahme umfasst zahlreiche Arten intelligenter Endgeräte, konzentriert sich jedoch besonders auf Apps, die für intelligente mobile Endgeräte verfügbar sind.

2. Datenschutzrisiken

Durch die enge Verzahnung mit dem Betriebssystem können Apps auf wesentlich mehr Daten zugreifen als ein herkömmlicher Internet-Browser.[5] Apps können auf dem jeweiligen Endgerät große Datenmengen (Standortdaten, vom Nutzer auf dem Gerät gespeicherte Daten sowie verschiedene Sensordaten) erfassen und verarbeiten, um dem Endnutzer neue und innovative Dienstleistungen anbieten zu können.

Ein hohes Risiko für den Datenschutz ergibt sich aus der ausgeprägten Fragmentierung unter den zahlreichen Akteuren im Umfeld der App-Entwicklung. Ein einzelnes Datenelement kann in Echtzeit vom Gerät übermittelt werden, um dann in einem anderen Teil der Welt verarbeitet oder zwischen Ketten dritter Akteure kopiert zu werden. Einige der bekanntesten Apps werden von großen Technologieunternehmen entwickelt. Viele Apps werden aber auch von kleinen, neu gegründeten Unternehmen hergestellt. Ein einziger Programmierer, der zwar

[5] Web-Browser für Desktop-Geräte erhalten aufgrund entsprechender Bestrebungen der Entwickler von Internetspielen ebenfalls einen immer umfangreicheren Zugriff auf Sensordaten.

eine Idee hat, aber vielleicht nur geringe oder keinerlei einschlägige Vorkenntnisse besitzt, kann in kurzer Zeit ein weltweites Publikum erreichen. App-Entwickler, die nicht mit den Datenschutzbestimmungen vertraut sind, können erhebliche Risiken für die Privatsphäre und den Ruf von Nutzern intelligenter Endgeräte verursachen. Gleichzeitig entwickeln sich rasch Drittanbieter-Dienste (z. B. Werbung), die erhebliche Mengen personenbezogener Daten weitergeben können, wenn sie von einem App-Entwickler ohne angemessene Vorsichtsmaßnahmen integriert werden.

Die größten Datenschutzrisiken für den Endnutzer sind die mangelnde Transparenz und die mangelnde Kenntnis der von einer App ausgeführten Verarbeitungen sowie das Fehlen einer expliziten Einwilligung des Endnutzers vor der Verarbeitung. Unzureichende Sicherheitsmaßnahmen, ein offenkundiger Trend zur Datenmaximierung und die ungenaue Festlegung der Zwecke, für die personenbezogene Daten erfasst werden, tragen zu einer weiteren Erhöhung der Datenschutzrisiken des derzeitigen App-Umfelds bei. Viele dieser Risiken wurden von anderen internationalen Regulierungsbehörden untersucht und in Angriff genommen, beispielsweise von der amerikanischen Wettbewerbsbehörde Federal Trade Commission (FTC), dem kanadischen Office of the Privacy Commissioner und dem Attorney General des kalifornischen Justizministeriums.[6]

- Ein wichtiges Datenschutzrisiko ist mangelnde Transparenz. Aufgrund der von den Herstellern der Betriebssysteme und von den App-Stores bereitgestellten Funktionen müssen App-Entwickler dafür sorgen, dass den Endnutzern zum angemessenen Zeitpunkt umfassende Informationen bereitgestellt werden. Diese Funktionen werden jedoch nicht von allen App-Entwicklern genutzt, da viele Apps keine Datenschutzerklärung enthalten oder die Nutzer nicht klar über die Art der personenbezogenen Daten, die die App möglicherweise verarbeitet, und über die Zwecke dieser Verarbeitung informieren. Die mangelnde Transparenz beschränkt sich nicht auf kostenlose Apps oder auf Apps von unerfahrenen Entwicklern. In einer kürzlich veröffentlichten Studie wurde berichtet, dass nur 61,3 % der 150 beliebtesten Apps eine Datenschutzerklärung enthielten.[7]
- Die mangelnde Transparenz geht häufig mit dem Fehlen einer Einwilligung ohne Zwang und in Kenntnis der Sachlage einher. Sobald eine App heruntergeladen wurde, beschränkt sich die Einwilligung häufig auf ein Kontrollkästchen zur Erklärung, dass der Endnutzer die vorgegebenen Bedingungen akzeptiert, ohne dass auch nur die Auswahlmöglichkeit „Nein, danke“ angeboten wird. Nach einer Studie der GSMA

---

[6] Siehe unter anderem FTC-Bericht: *Mobile Privacy Disclosures, Building Trust Through Transparency*, Februar 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf, FTC-Bericht: *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, Februar 2012, http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf, und Folgebericht: *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, Dezember 2012, http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf, sowie *Canadian Offices of the Privacy Commissioners, Seizing Opportunity: Good Privacy. Practices for Developing Mobile Apps*, Oktober 2012, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf, Kamala D. Harris, Attorney General California Department of Justice, *Privacy on the go, Recommendations for the mobile ecosystem*, Januar 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[7] *FPF Mobile Apps study*, Juni 2012, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf.

vom September 2011 wünschen sich 92 % der App-Nutzer eine differenziertere Auswahl.[8]

- Unzureichende Sicherheitsmaßnahmen können zur unberechtigten Verarbeitung (sensibler) personenbezogener Daten führen, beispielsweise wenn ein App-Entwickler Opfer eines Diebstahls personenbezogener Daten wird oder wenn die App personenbezogene Daten aktiv überträgt.
- Ein weiteres Datenschutzrisiko ergibt sich aus der (absichtlichen oder durch Unwissenheit bedingten) Missachtung des Grundsatzes der Zweckbindung, nach dem personenbezogene Daten nur für genau festgelegte und rechtmäßige Zwecke erfasst und verarbeitet werden dürfen. Von Apps erfasste personenbezogene Daten können für nicht oder ungenau festgelegte Zwecke wie „Marktforschung" an zahlreiche Dritte weitergegeben werden. Die gleiche besorgniserregende Missachtung besteht in Bezug auf den Grundsatz der Datenminimierung. Kürzlich durchgeführte Forschungsarbeiten haben ergeben, dass viele Apps große Datenmengen von Smartphones erfassen, ohne dass ein sinnvoller Bezug zur offensichtlichen Funktion der App besteht.[9]

3. Datenschutzgrundsätze

3.1 Anwendbares Recht

Der maßgebliche EU-Rechtsrahmen besteht in der Datenschutzrichtlinie (Richtlinie 95/46/EG). Die Datenschutzrichtlinie gilt immer dann, wenn die Nutzung von Apps auf intelligenten Endgeräten mit einer Verarbeitung personenbezogener Daten von natürlichen Personen einhergeht. Im Zusammenhang mit der Verarbeitung über mobile Apps ist für die Ermittlung des anwendbaren Rechts besonders wichtig, dass der für die Verarbeitung Verantwortliche bestimmt wird. Die Feststellung des für die Verarbeitung Verantwortlichen ist für die Anwendung des EU-Datenschutzrechts zwar nicht der einzige, aber doch ein entscheidender Schritt. Gemäß Artikel 4 Absatz 1 Buchstabe a der Datenschutzrichtlinie gilt das nationale Recht eines Mitgliedstaats für alle Verarbeitungen personenbezogener Daten, die „im Rahmen einer Niederlassung" des für die Verarbeitung Verantwortlichen im Hoheitsgebiet dieses Mitgliedstaats durchgeführt werden. Gemäß Artikel 4 Absatz 1 Buchstabe c der Datenschutzrichtlinie gilt das nationale Recht eines Mitgliedstaats auch in Fällen, in denen der für die Verarbeitung Verantwortliche *nicht* im Gebiet der Gemeinschaft *niedergelassen* ist und auf Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind. Dieses Kriterium ist normalerweise erfüllt, da das Endgerät an der Verarbeitung personenbezogener Daten vom Nutzer und über den Nutzer maßgeblich

---

[8] „*89 % [der Nutzer] finden es wichtig, zu wissen, wenn ihre personenbezogenen Informationen von einer App weitergegeben werden, und wie sie die entsprechende Funktion aktivieren und deaktivieren zu können.*" Quelle: *User perspectives on mobile privacy*, September 2011, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf.

[9] Wall Street Journal, *Your Apps Are Watching You*, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

beteiligt ist.[10] Dies ist jedoch nur relevant, wenn der für die Verarbeitung Verantwortliche nicht in der EU niedergelassen ist.

Entsprechend gilt: Wenn eine an der Entwicklung, der Verbreitung und dem Betrieb von Apps beteiligte Partei als für die Verarbeitung Verantwortlicher angesehen wird, ist sie - allein oder gemeinsam mit anderen - dafür verantwortlich, die Einhaltung sämtlicher in der Datenschutzrichtlinie festgelegten Anforderungen zu gewährleisten. Die Ermittlung der Rollen der an mobilen Apps beteiligten Parteien wird in Abschnitt 3.3 eingehender behandelt.

Ergänzend zur Datenschutzrichtlinie legt die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG, geändert durch Richtlinie 2009/136/EG) weltweit einen spezifischen Standard für alle Parteien fest, die auf den Endgeräten von Nutzern im Europäischen Wirtschaftsraum (EWR) gespeicherte Informationen ihrerseits speichern oder auf diese Informationen zugreifen wollen.

Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation sieht vor, dass „*die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. (...)*“

Während viele Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation nur auf Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste und auf Betreiber öffentlicher Kommunikationsnetze in der Gemeinschaft anwendbar sind, gilt Artikel 5 Absatz 3 für jede Rechtsperson, die Informationen auf intelligente Endgeräte überträgt oder auf diesen Geräten liest. Er gilt unabhängig von der Art der Rechtsperson (öffentliche oder private Rechtsperson, einzelner Programmierer oder Großunternehmen, für die Verarbeitung Verantwortlicher, Auftragsverarbeiter oder Dritter).

Die Einwilligungsanforderung nach Artikel 5 Absatz 3 gilt unabhängig von der Art der zu speichernden oder zu lesenden Daten für sämtliche Informationen. Der Anwendungsbereich ist nicht auf personenbezogene Daten beschränkt. Die Informationen können jegliche Art von auf dem Gerät gespeicherten Daten sein.

Die Einwilligungsanforderung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation gilt für Dienste, die „*in der Gemeinschaft*“ angeboten werden, d. h. unabhängig vom Standort des Dienstebetreibers für alle im Europäischen Wirtschaftsraum lebenden Personen. Es ist wichtig, dass App-Entwickler wissen, dass die beiden Richtlinien insofern zwingende Vorschriften darstellen, als die Rechte natürlicher Personen nicht übertragbar sind und keinem vertraglichen Verzicht unterliegen. Das bedeutet,

[10] Sofern die App die Übertragung personenbezogener Daten an die für die Verarbeitung Verantwortlichen bewirkt; dieses Kriterium ist möglicherweise nicht erfüllt, wenn die Daten ausschließlich lokal auf dem eigentlichen Endgerät verarbeitet werden.

dass die Anwendbarkeit des europäischen Rechts zum Schutz der Privatsphäre nicht durch eine einseitige Erklärung oder eine vertragliche Vereinbarung ausgeschlossen werden kann.[11]

3.2 Von Apps verarbeitete personenbezogene Daten

Viele Arten von Daten, die auf einem intelligenten mobilen Endgerät gespeichert sind oder von diesem Gerät erstellt werden, sind personenbezogene Daten. Erwägungsgrund 24 der Datenschutzrichtlinie für elektronische Kommunikation besagt:

> *„Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt.“*

Informationen sind als personenbezogene Daten zu betrachten, wenn sie sich auf eine natürliche Person beziehen, die für den für die Verarbeitung Verantwortlichen oder einen Dritten direkt (z. B. durch den Namen) oder indirekt identifizierbar ist. Sie können sich auf den Besitzer des Geräts oder auf beliebige andere natürliche Personen beziehen (z. B. die Kontaktdaten von Freunden in einem Adressbuch).[12] Daten können auf dem Gerät oder – nach der Übertragung – an anderen Orten erfasst und verarbeitet werden: auf der Infrastruktur von App-Entwicklern oder Dritten, über die Verbindung mit einer externen Programmierschnittstelle, in Echtzeit und ohne Kenntnis des Endnutzers.

Beispiele für solche personenbezogenen Daten, die erhebliche Auswirkungen auf die Privatleben der Nutzer und anderer Personen haben können:

- Standortinformationen,
- Kontakte,
- eindeutige Geräte- und Kundenkennungen (z. B. IMEI,[13] IMSI,[14] UDID[15] und Mobiltelefonnummer),
- Identität der betroffenen Person,
- Identität des Telefons (d. h. Name des Telefons),[16]
- Kreditkarten- und Zahlungsdaten,

---

[11] Zum Beispiel durch Erklärungen, dass ausschließlich das Recht eines außerhalb des EWR liegenden Rechtssystems gilt.

[12] Daten können (i) vom Gerät automatisch auf aufgrund von Funktionen erstellt werden, die vom Betriebssystem und/oder dem Gerätehersteller oder vom jeweiligen Mobilfunkbetreiber im Voraus festgelegt werden (z. B. Geolokalisierungsdaten, Netzeinstellungen, IP-Adresse), (ii) vom Nutzer durch Apps erstellt werden (Kontaktlisten; Notizen, Fotos) und (iii) von den Apps erstellt werden (z. B. Browserverlauf).

[13] *International Mobile Equipment Identity* (eindeutige Nummer des Endgeräts).

[14] *International Mobile Subscriber Identity* (eindeutige Nummer des Netzteilnehmers).

[15] *Unique Device Identifier* (eindeutige Gerätenummer für Apple-Produkte).

[16] Nutzer neigen dazu, ihr Telefon unter Verwendung ihres eigenen Namens zu benennen, z. B. „Max Mustermanns iPhone“.

- Anruflisten, SMS oder Instant Messaging,

- Browserverlauf,

- E-Mail,

- Authentifizierungsdaten für Dienste der Informationsgesellschaft (insbesondere Dienste mit sozialen Funktionen),

- Bilder und Videos und

- biometrische Daten (z. B. Muster für Gesichtserkennung und Fingerabdrücke).

3.3 An der Datenverarbeitung beteiligte Parteien

Viele verschiedene Parteien sind an der Entwicklung, der Verbreitung und dem Betrieb von Apps beteiligt, und jede dieser Parteien kann hinsichtlich des Datenschutzes unterschiedliche Pflichten haben.

Vier wichtige Parteien sind zu unterscheiden: (i) App-Entwickler (einschließlich der App-Eigentümer),[17] Hersteller von Betriebssystemen und Endgeräten,[18] (iii) App-Stores (Vertreiber der Apps) und (iv) sonstige an der Verarbeitung personenbezogener Dateien beteiligte Parteien. In einigen Fällen sind die Datenschutzpflichten verteilt, insbesondere, wenn ein und dieselbe Rechtsperson auf mehreren Ebenen beteiligt ist, zum Beispiel wenn der Hersteller des Betriebssystems auch den App-Store kontrolliert.

Die Endnutzer müssen in angemessener Weise eigenverantwortlich entscheiden, in welchem Umfang sie personenbezogene Daten über ihre mobilen Endgeräte erstellen und speichern. Wenn eine solche Verarbeitung rein persönlichen oder familiären Zwecken dient, gilt die Datenschutzrichtlinie nicht (Artikel 3 Absatz 2), und der Nutzer ist von formalen Datenschutzverpflichtungen ausgenommen. Wenn Nutzer jedoch beschließen, Daten über die App weiterzugeben, indem sie beispielsweise über eine App für soziale Netzwerke Informationen für eine unbestimmte Zahl von Personen veröffentlichen,[19] geht die betreffende Verarbeitung von Informationen über die Bedingungen der Ausnahme für familiäre Tätigkeiten hinaus.[20]

---

[17] Die Datenschutzgruppe verwendet die allgemeine Terminologie von App-Entwicklern, betont jedoch, dass der Begriff nicht auf die Programmierer oder die technischen Entwickler von Apps beschränkt ist, sondern die App-Eigentümer einschließt. Diese sind Unternehmen und Organisationen, die die Entwicklung von Apps in Auftrag geben und die Zwecke der Apps festlegen.

[18] In einigen Fällen bestehen Überschneidungen zwischen dem Hersteller des Betriebssystems und dem Hersteller des Endgeräts. In anderen Fällen ist der Hersteller des Geräts nicht gleichzeitig auch der Anbieter des Betriebssystems.

[19] Siehe Europäischer Gerichtshof, Rechtssache C-101/01, Strafverfahren gegen Bodil Lindqvist, Urteil vom 6. November 2003, und Rechtssache C-73/07, Tietosuojavaltuutettu gegen Satakunnan Markkinapörssi Oy und Satamedia Oy, Urteil vom 16. Dezember 2008.

[20] Siehe Stellungnahme 5/2009 der Artikel-29-Datenschutzgruppe zur Nutzung sozialer Online-Netzwerke (Juni 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf.

3.3.1 App-Entwickler

App-Entwickler erstellen Apps und/oder stellen Endnutzern Apps zur Verfügung. Diese Kategorie beinhaltet Organisationen des privaten und des öffentlichen Sektors, die die App-Entwicklung extern vergeben, sowie die Unternehmen und die natürlichen Personen, die Apps erstellen und implementieren. Sie konzipieren und/oder erstellen die Software, die auf den Smartphones läuft, und entscheiden so über den Umfang, in dem die App auf die verschiedenen Kategorien personenbezogener Daten zugreift und diese auf dem Gerät und/oder über entfernte Rechenressourcen (Rechnereinheiten von App-Entwicklern oder Dritten) verarbeitet.

In dem Umfang, in dem ein App-Entwickler die Zwecke und die Mittel der Verarbeitung personenbezogener Daten auf intelligenten Endgeräten festlegt, ist er der für die Verarbeitung Verantwortliche gemäß der Definition in Artikel 2 Buchstabe d der Datenschutzrichtlinie. In diesem Fall muss er die Bestimmungen der gesamten Datenschutzrichtlinie einhalten. Die wichtigsten Bestimmungen sind in den Abschnitten 3.4 bis 3.10 der vorliegenden Stellungnahme erläutert.

Selbst wenn die Ausnahmebestimmung für familiäre Tätigkeiten für einen Nutzer gilt, kommt dem App-Entwickler die Rolle des für die Verarbeitung Verantwortlichen zu, wenn er die Daten für seine eigenen Zwecke verarbeitet. Dies ist beispielsweise dann relevant, wenn eine App Zugriff auf das gesamte Adressbuch erfordert, um den jeweiligen Dienst (Instant Messaging, Telefonanrufe, Videoanrufe) zu erbringen.

Die Verpflichtungen des App-Entwicklers werden als eingeschränkt angesehen, wenn keine personenbezogenen Daten außerhalb des Geräts verarbeitet und/oder verfügbar gemacht werden oder wenn der App-Entwickler mit angemessenen technischen und organisatorischen Maßnahmen sichergestellt hat, dass Daten auf dem Gerät irreversibel anonymisiert und aggregiert werden, bevor sie vom Gerät übertragen werden.

Wenn der App-Entwickler Zugriff auf Informationen erhält, die auf dem Gerät gespeichert sind, gilt in jedem Fall auch die Datenschutzrichtlinie für elektronische Kommunikation, und der App-Entwickler muss die in Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation vorgesehene Einwilligungsanforderung erfüllen.

In dem Umfang, in dem der App-Entwickler die tatsächliche Datenverarbeitung teilweise oder vollständig extern an einen Dritten vergeben hat und diesem Dritten die Rolle eines für die Verarbeitung Verantwortlichen zukommt, muss der App-Entwickler alle Verpflichtungen erfüllen, die sich aus dem Einsatz eines Auftragsverarbeiters ergeben. Dies gilt auch für die Nutzung eines Cloud-Computing-Anbieters (z. B. zur externen Datenspeicherung).[21]

In dem Umfang, in dem der App-Entwickler Dritten Zugriff auf Nutzerdaten gestattet (z. B. durch Online-Werbenetzwerke („Advertising Networks“), die auf die Standortdaten des Endgeräts zugreifen, um auf der Basis von Behavioural Targeting Werbung betreiben zu

[21] Siehe Stellungnahme 05/2012 der Artikel-29-Datenschutzgruppe zum Cloud Computing (Juli 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf.

können), muss er angemessene Mechanismen einsetzen, um die Anforderungen des EU-Rechtsrahmens zu erfüllen. Wenn ein Dritter auf Daten zugreift, die auf dem Endgerät gespeichert sind, muss er die betreffende Einwilligung in Kenntnis der Sachlage gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation einholen. Wenn ein Dritter personenbezogene Daten für seine eigenen Zwecke verarbeitet, kann er darüber hinaus gemeinsam mit dem App-Entwickler als für die Verarbeitung Verantwortlicher betrachtet werden und muss daher die Beachtung des Grundsatzes der Zweckbindung und der Sicherheitsverpflichtungen[22] für den Teil der Verarbeitung gewährleisten, für den er die jeweiligen Zwecke und Mittel festlegt. Da zwischen App-Entwicklern und Dritten verschiedene (wirtschaftliche und technische) Vereinbarungen bestehen können, müssen die Verantwortlichkeiten der jeweiligen Partei im Einzelfall unter Berücksichtigung der spezifischen Umstände der entsprechenden Verarbeitung ermittelt werden.

Ein App-Entwickler kann Programmbibliotheken Dritter mit Software-Komponenten für allgemeine Funktionen nutzen (z. B. die Programmbibliothek einer Social-Gaming-Plattform). In diesem Fall muss der App-Entwickler gegebenenfalls u. a. unter Einholung der Einwilligung der Nutzer sicherstellen, dass den Nutzern jegliche von diesen Programmbibliotheken durchgeführte Datenverarbeitung bekannt ist sowie dass die betreffende Datenverarbeitung dem EU-Rechtsrahmen entspricht. In diesem Sinne müssen App-Entwickler die Nutzung von Funktionen verhindern, die für den Nutzer nicht offensichtlich sind.

3.3.2 Hersteller von Betriebssystemen und Endgeräten

Die Hersteller von Betriebssystemen und Endgeräten sind für sämtliche personenbezogenen Daten, die für ihre eigenen Zwecke verarbeitet werden (z. B. für ein reibungsloses Funktionieren des Geräts oder für die Sicherheit), ebenfalls als für die Verarbeitung Verantwortliche (sowie gegebenenfalls als gemeinsam für die Verarbeitung Verantwortliche) zu betrachten. Diese Verarbeitung umfasst vom Nutzer erstellte Daten (z. B. Nutzerangaben bei der Registrierung), vom Gerät automatisch erstellte Daten (z. B. wenn das Gerät eine Phone-Home-Funktion in Bezug auf seinen Standort hat) oder personenbezogene Daten, die im Rahmen der Installation oder der Nutzung von Apps erstellt wurden und vom Hersteller des Betriebssystems oder des Geräts verarbeitet werden. Wenn der Hersteller des Betriebssystems oder des Geräts zusätzliche Funktionen (z. B. zur Datensicherung oder Fernstandortsbestimmung) bereitstellt, ist er auch für die zu diesem Zweck verarbeiteten personenbezogenen Daten der für die Verarbeitung Verantwortliche.

---

[22] Siehe Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe zur Werbung auf Basis von Behavioural Targeting (Juni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf, sowie Stellungnahme 1/2010 der Artikel-29-Datenschutzgruppe zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ (Februar 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

Apps, die einen Zugriff auf die Geolokalisierung erfordern, müssen die Standortsbestimmungsdienste des Betriebssystems nutzen. Wenn eine App die Geolokalisierung verwendet, kann das Betriebssystem einerseits personenbezogene Daten erfassen, um den Apps die erforderlichen Geolokalisierungsinformationen zur Verfügung zu stellen, und andererseits die Daten zur Verbesserung der eigenen Standortsbestimmungsdienste verwenden. Für den letztgenannten Zweck ist der Hersteller des Betriebssystems der für die Verarbeitung Verantwortliche.

Die Hersteller von Betriebssystemen und Endgeräten sind auch für die Programmierschnittstelle (API) verantwortlich, die die Verarbeitung personenbezogener Daten auf dem intelligenten Endgerät durch Apps ermöglicht. Die App-Entwickler können auf diese Funktionen, die die Hersteller von Betriebssystemen und Endgeräten über die Programmierschnittstelle verfügbar machen, zugreifen. Da die Hersteller von Betriebssystemen und Endgeräten die Mittel (und den Umfang) des Zugriffs auf personenbezogene Daten festlegen, müssen sie gewährleisten, dass App-Entwicklern hinreichend differenzierte Kontrollmöglichkeiten gewährt werden, um sicherstellen zu können, dass sich Zugriffe auf die für die Funktion der Apps tatsächlich erforderlichen Daten beschränken. Die Hersteller von Betriebssystemen und Geräten sollten zudem gewährleisten, dass dieser Zugriff einfach und wirksam unterbunden werden kann.

Das Konzept des eingebauten Datenschutzes (Privacy by Design) ist ein wichtiger Grundsatz, der indirekt bereits in der Datenschutzrichtlinie[23] berücksichtigt wird und der – in Verbindung mit dem Konzept datenschutzfreundlicher Voreinstellungen (Privacy by Default) – in der Datenschutzrichtlinie für elektronische Kommunikation[24] eingehender erläutert wird. Dieser Grundsatz verlangt, dass die Hersteller eines Endgeräts oder einer Applikation den Datenschutz schon in der Anfangsphase der Konzeption integrieren müssen. Der eingebaute Datenschutz ist gemäß der Richtlinie über Funkanlagen und Telekommunikationsendeinrichtungen[25] für die Konzeption von Telekommunikationseinrichtungen ausdrücklich vorgeschrieben. Daher kommt den Herstellern von Betriebssystemen und Endgeräten gemeinsam mit den App-Stores wesentliche Verantwortung für die Bereitstellung von Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre von App-Nutzern zu. Im Rahmen dieser Verantwortung ist auch zu gewährleisten, dass angemessene Mechanismen verfügbar sind, um die Endnutzer darüber zu informieren und aufzuklären, welche Funktionen Apps ausführen und auf welche Daten sie zugreifen können. Außerdem sind angemessene

---

23 Siehe Erwägungsgrund 46 und Artikel 17.

24 Siehe Artikel 14 Absatz 3.

25 Richtlinie 1999/5/EG vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität. Amtsblatt L 91/10 der Europäischen Gemeinschaften, 7.4.1999; nach Artikel 3 Absatz 3 Buchstabe c kann die Europäische Kommission festlegen, dass die Endnutzergeräte so hergestellt sein müssen, dass sie über Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre des Benutzers und des Teilnehmers verfügen.

Einstellungen bereitzustellen, mit denen App-Nutzer die Verarbeitungsparameter ändern können.[26]

3.3.3 App-Stores

Die am weitesten verbreiteten Arten intelligenter Endgeräte haben jeweils einen eigenen App-Store, und häufig ist ein bestimmtes Betriebssystem eng mit einem bestimmten App-Store verzahnt. App-Stores verarbeiten häufig Vorabzahlungen für Apps und können auch in Apps integrierte Kaufvorgänge unterstützen; daher erfordern sie eine Nutzerregistrierung mit Namen, Anschrift und Angaben für die Zahlung. Diese (direkt) identifizierbaren Daten können mit Daten über das Kauf- und Nutzungsverhalten sowie mit aus dem jeweiligen Gerät ausgelesen oder von diesem Gerät erstellten Daten (z. B. eindeutigen Kennungen) abgeglichen werden. Für die Verarbeitung dieser personenbezogenen Daten ist ein App-Store wahrscheinlich der für die Verarbeitung Verantwortliche; dies gilt auch, wenn er solche Informationen an die App-Entwickler weiterleitet. Wenn der App-Store Informationen über die heruntergeladenen Apps eines Endnutzers, den Nutzungsverlauf oder ähnliche Funktionen verarbeitet, um bereits heruntergeladene Apps wiederherzustellen, ist er auch der für die Verarbeitung Verantwortliche für die zu diesem Zweck verarbeiteten personenbezogenen Daten.

Ein App-Store speichert Anmeldedaten sowie die Verlaufsdaten bereits erworbener Apps. Er fordert den Nutzer auch auf, eine Kreditkartennummer anzugeben, die zusammen mit dem Nutzerkonto gespeichert wird. Der App-Store ist der für die Verarbeitung Verantwortliche für diese Vorgänge.

Websites, die das Herunterladen einer App zur Installation auf dem Endgerät ohne Authentifizierung erlauben, verarbeiten unter Umständen keine personenbezogenen Daten.

App-Stores spielen insofern eine wichtige Rolle, als sie App-Entwicklern ermöglichen können, angemessene Informationen über die App bereitzustellen (u. a. über die Arten von Daten, die die App verarbeiten kann, und über die Zwecke, zu denen die Daten verarbeitet werden). App-Stores können diese Regeln durch ihre Strategie zur Aufnahme der zu vertreibenden Apps (auf Grundlage von Ex-Ante- oder Ex-Post-Kontrollen) durchsetzen. In Zusammenarbeit mit dem Betriebssystemhersteller kann der App-Store einen Rahmen entwickeln, mit dem App-Entwickler konsistente und aussagekräftige Informationsmitteilungen erstellen können (z. B. Symbole für bestimmte Arten des Zugriffs auf Sensordaten); die betreffenden Symbole kann er gut sichtbar in seinem Katalog darstellen.

[26] Die Datenschutzgruppe begrüßt in diesem Zusammenhang die Empfehlungen der FTC in ihrem in Fußnote 6 erwähnten Bericht „Mobile Privacy Disclosures“ (Datenschutzerklärungen bei mobilen Endgeräten), zum Beispiel auf Seite 15: „(…) *Plattformen [sind] in einer einzigartigen Position, einheitliche [Datenschutz-]Erklärungen für Apps bereitstellen zu können, und werden dazu ermutigt. Entsprechend den Workshop-Anmerkungen könnten sie auch in Erwägung ziehen, diese Erklärungen zu verschiedenen Zeitpunkten anzuzeigen (…).*“

3.3.4 Dritte

An der Verarbeitung von Daten durch die Nutzung von Apps sind viele verschiedene Dritte beteiligt.

Beispielsweise finanzieren sich viele kostenlose Apps durch Werbung, die unter Verwendung von Protokollierungsvorrichtungen (Tracking-Vorrichtungen) wie Cookies oder andere Geräte-Identifikatoren auf Zusammenhänge oder Personen bezogen werden kann. Die Werbung kann in verschiedenen Formen erfolgen: Banner innerhalb der App, Werbeanzeigen außerhalb der App, die durch die Änderung von Browsereinstellungen eingeblendet werden, Platzierung von Symbolen auf dem Desktop des mobilen Endgeräts oder personalisierte Organisation der App-Inhalte (z. B. gesponserte Suchergebnisse).

Die Werbung für Apps erfolgt im Allgemeinen über Online-Werbenetzwerke oder ähnliche Vermittler, die mit der Rechtsperson des Betriebssystem-Herstellers oder des App-Store verknüpft oder identisch sein können. Wie in der Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe[27] erläutert, bringt Online-Werbung häufig die Verarbeitung personenbezogener Daten mit sich, wie sie in Artikel 2 der Datenschutzrichtlinie definiert und durch die Artikel-29-Arbeitsgruppe ausgelegt wurden.[28]

Weitere Beispiele für Dritte sind Analyse- und Kommunikationsdienstleister. Analysedienstleister ermöglichen den App-Entwicklern, Erkenntnisse über die Nutzung, die Beliebtheit und die Nutzbarkeit ihrer Apps zu gewinnen. Kommunikationsdienstleister[29] können eine wichtige Rolle auch bei der Festlegung der Standardeinstellungen und der Sicherheitsaktualisierungen vieler Endgeräte spielen und Daten über die Nutzung von Apps verarbeiten. Ihre spezifische Anpassung (Markenkennzeichnung) kann Auswirkungen auf mögliche technische und funktionelle Maßnahmen haben, die der Nutzer zum Schutz seiner personenbezogenen Daten anwenden kann.

Im Vergleich zu App-Entwicklern können Dritten zwei verschiedene Rollen zukommen. Eine Rolle besteht in der Durchführung von Vorgängen für den App-Eigentümer (etwa in der Bereitstellung von Analysen innerhalb der App). Wenn die betreffenden Dritten in diesem Fall ausschließlich im Namen des App-Entwicklers handeln und keine Daten zu ihren eigenen Zwecken verarbeiten und/oder Daten an andere Entwickler weiterleiten, handeln sie wahrscheinlich als Auftragsverarbeiter.

Die zweite Rolle besteht im Sammeln von Informationen von verschiedenen Apps, um weitere Dienste anzubieten, z. B. die Bereitstellung von Analysewerten in größerem Maßstab (Beliebtheit von Apps, personalisierte Empfehlung) oder die Vermeidung der wiederholten Einblendung von Werbeanzeigen für den gleichen Nutzer. Wenn Dritte personenbezogene

---

[27] Siehe Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe zur Werbung auf Basis von Behavioural Targeting (Juni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf.

[28] Siehe auch die Auslegung des Begriffs „personenbezogene Daten“ in der Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe (Juni 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.

[29] Kommunikationsdienstleister unterliegen auch branchenspezifischen Datenschutzverpflichtungen, die außerhalb des Gegenstandsbereichs der vorliegenden Stellungnahme liegen.

Daten zu ihren eigenen Zwecken verarbeiten, handeln sie als für die Verarbeitung Verantwortliche und müssen sämtliche anwendbaren Bestimmungen der Datenschutzrichtlinie einhalten.[30] Bei Werbung auf Basis von Behavioural Targeting muss der für die Verarbeitung Verantwortliche eine gültige Einwilligung des Nutzers für die Erfassung und die Verarbeitung personenbezogener Daten einholen. Diese Verarbeitung umfasst beispielsweise die Analyse und Kombination personenbezogener Daten und die Erstellung und/oder Anwendung von Profilen. Wie die Datenschutzgruppe bereits in der Stellungnahme 2/2012 zur Werbung auf Basis von Behavioural Targeting erläutert hat, wird eine solche Einwilligung am besten durch die Verwendung eines vorgeschalteten Opt-in-Mechanismus veranlasst.

Ein Unternehmen stellt App-Eigentümern und Werbetreibenden durch die Verwendung von Tracking-Vorrichtungen Parameter zur Verfügung, die der App-Entwickler in die Apps integriert hat. Die Tracking-Vorrichtungen des Unternehmens können daher in zahlreichen Apps und auf zahlreichen Endgeräten installiert werden. Eine der Dienstleistungen des Unternehmens besteht darin, App-Entwickler durch Erfassung einer eindeutigen Kennung darüber zu informieren, welche sonstigen Apps von einem Nutzer verwendet werden. Das Unternehmen legt die Mittel (d. h. die Tracking-Vorrichtungen) und die Zwecke seiner Hilfsmittel fest, bevor das Unternehmen den App-Entwicklern, den Werbetreibenden und anderen Akteuren die betreffenden Mittel bereitstellt, und handelt daher als für die Verarbeitung Verantwortlicher.

In dem Umfang, in dem Dritte auf Informationen auf dem intelligenten Endgerät zugreifen oder Informationen auf dem Gerät speichern, müssen sie die Einwilligungsanforderung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erfüllen.

In diesem Zusammenhang ist darauf hinzuweisen, dass Nutzer Software zur Kontrolle der Verarbeitung personenbezogener Daten (wie im Umfeld der Internetnutzung auf Desktop-Geräten allgemein verbreitet) auf intelligenten Endgeräten normalerweise nur in beschränktem Umfang installieren können. Alternativ zur Verwendung von HTTP-Cookies greifen Dritte häufig auf eindeutige Kennungen zu, um Nutzer bzw. Gruppen von Nutzern auszuwählen und diesen gezielte Dienstleistungen, einschließlich Werbung, zu übermitteln. Da viele dieser Kennungen von den Nutzern nicht gelöscht oder geändert werden können (z. B. IMEI, IMSI, MSISDN[31] und spezifische vom Betriebssystem erstellte eindeutige Gerätekennungen), können diese Dritten große Mengen personenbezogener Daten erfassen, ohne dass der Endnutzer eine Kontrolle darüber hat.

[30] Stellungnahme 2/2010 der Artikel-29-Datenschutzgruppe zur Werbung auf Basis von Behavioural Targeting, S. 10-11.

[31] *Mobile Station Integrated Services Digital Network* (weltweit eindeutige Mobilfunk-Rufnummer).

3.4 Rechtsgrundlage

Die Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage, deren Elemente in Artikel 7 der Datenschutzrichtlinie aufgezählt sind. Artikel 7 unterscheidet sechs Rechtsgrundlagen für die Datenverarbeitung: die ohne jeden Zweifel gegebene Einwilligung der betroffenen Person, die Notwendigkeit der Verarbeitung für die Erfüllung eines Vertrags mit der betroffenen Person, die Wahrung lebenswichtiger Interessen der betroffenen Person, die Notwendigkeit für die Erfüllung einer rechtlichen Verpflichtung, (für Behörden) die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, und die Notwendigkeit aufgrund berechtigter (geschäftlicher) Interessen.

In Bezug auf das Speichern von Informationen oder den Zugriff auf bereits auf dem Endgerät gespeicherte Informationen entsteht durch Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation (d. h. die Einwilligungsanforderung für die Speicherung von Informationen und das Auslesen von Informationen aus einem Gerät) eine detailliertere Einschränkung der Rechtsgrundlagen, die berücksichtigt werden kann.

3.4.1 Einwilligung vor Installation und Verarbeitung personenbezogener Daten

Im Fall von Apps ist die wichtigste anwendbare Rechtsgrundlage die Einwilligung. Bei der Installation einer App werden Informationen auf dem Endnutzergerät gespeichert. Viele Apps greifen auch auf Daten zu, die auf dem Gerät gespeichert sind: Kontakte im Adressbuch, Bilder, Videos und andere personenbezogene Dokumente. In allen diesen Fällen setzt Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation die Einwilligung des Nutzers auf der Grundlage klarer und umfassender Informationen voraus, bevor Informationen auf dem Gerät gespeichert oder vom Gerät gelesen werden.

Es ist wichtig, zwischen der für das Speichern und Lesen von Informationen auf dem Gerät erforderlichen Einwilligung und der Einwilligung zu unterscheiden, die als Rechtsgrundlage für die Verarbeitung verschiedener Arten personenbezogener Daten erforderlich ist. Beide Anforderungen gelten gleichzeitig (mit jeweils unterschiedlicher Rechtsgrundlage). Außerdem muss die Einwilligung in beiden Fällen ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgen (nach Artikel 2 Buchstabe h der Datenschutzrichtlinie). Daher können beide Einwilligungen in der Praxis gemeinsam eingeholt werden, entweder während der Installation oder bevor die App mit der Erfassung personenbezogener Daten vom Gerät beginnt; Voraussetzung ist allerdings, dass der Nutzer unmissverständlich darüber informiert wird, wofür er seine Einwilligung erteilt.

Viele App-Stores ermöglichen den App-Entwicklern, die Endnutzer vor der Installation über die Grundfunktionen einer App zu informieren und eine aktive Eingabe von den Nutzern zu fordern, bevor die App heruntergeladen und installiert wird (z. B. Tippen auf eine Schaltfläche „Installieren“). Obwohl diese Eingabe unter bestimmten Umständen die Einwilligungsanforderung nach Artikel 5 Absatz 3 erfüllen könnte, werden Informationen wahrscheinlich nicht in hinreichendem Umfang bereitgestellt; in diesem Fall wäre eine gültige Einwilligung für die Verarbeitung personenbezogener Daten nicht gegeben. Die

Datenschutzgruppe hat diese Thematik bereits in ihrer Stellungnahme 15/2011 zur Definition von Einwilligung[32] erörtert.

Im Zusammenhang mit intelligenten Endgeräten bedeutet „ohne Zwang", dass einem Nutzer die Möglichkeit eingeräumt werden muss, die Verarbeitung seiner personenbezogenen Daten zu akzeptieren oder abzulehnen. Wenn eine App auf die Verarbeitung personenbezogener Daten angewiesen ist, muss dem Nutzer daher die diese Verarbeitung akzeptieren oder ablehnen können. Der Nutzer sollte nicht mit einem Bildschirm konfrontiert werden, über den die Installation ausschließlich mit der Option „Ja, ich bin einverstanden" abgeschlossen werden kann. Die Installation muss auch etwa über die Option „Abbrechen" abgebrochen werden können.

„In Kenntnis der Sachlage" bedeutet, dass die betroffene Person über die erforderlichen Informationen verfügen muss, um sich ein korrektes Urteil bilden zu können.[33] Zur Vermeidung jeglicher Mehrdeutigkeit müssen solche Informationen bereitgestellt werden, bevor personenbezogene Daten verarbeitet werden. Dazu gehört auch die Datenverarbeitung, die während der Installation erfolgen könnte, zum Beispiel zu Zwecken der Fehlerbeseitigung oder zum Tracking. Inhalt und Form dieser Informationen sind in Abschnitt 3.7 der vorliegenden Stellungnahme erläutert.

„Für den konkreten Fall" bedeutet, dass die Willensbekundung sich auf die Verarbeitung eines bestimmten Datenelements oder einer eingeschränkten Kategorie der Datenverarbeitung beziehen muss. Daher kann ein einfaches Tippen auf eine Schaltfläche „Installieren" nicht als gültige Einwilligung für die Verarbeitung personenbezogener Daten betrachtet werden, da eine Einwilligung nicht auf einer allgemein formulierten Autorisierung beruhen kann. In einigen Fällen können Nutzer eine differenzierte Einwilligung erteilen, wenn eine Einwilligung für jede Datenart eingeholt wird, auf die die App zugreifen soll.[34] Mit einem solchen Ansatz werden zwei wichtige rechtliche Anforderungen erfüllt: erstens die angemessene Unterrichtung der Nutzer über wichtige Elemente der Dienstleistung und zweitens die Einholung der Einwilligung für jeden konkreten Fall.[35] Der alternative Ansatz, bei dem ein App-Entwickler seine Nutzer auffordert, einen langen Text mit Nutzungsbedingungen und/oder eine lange Datenschutzerklärung zu akzeptieren, stellt keine Einwilligung für den konkreten Fall dar.[36]

---

[32] Stellungnahme 15/2011 der Artikel-29-Datenschutzgruppe zur Definition von Einwilligung (Juli 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf.

[33] Ebenda, S. 19.

[34] Eine differenzierte Einwilligung bedeutet, dass Personen genau (spezifisch) kontrollieren können, welche von der App gebotenen Verarbeitungsfunktionen für personenbezogene Daten sie aktivieren möchten.

[35] Die Notwendigkeit einer solchen differenzierten Einwilligung wird auch von der FTC in ihrem aktuellen Bericht (siehe Fußnote 6), S. 15-16, ausdrücklich befürwortet: „(…) *die Plattformen sollten in Erwägung ziehen, Datenschutzerklärungen jeweils zum relevanten Zeitpunkt einzublenden und ausdrückliche positive Einwilligungen für die Erfassung anderer Inhalte einzuholen, die viele Verbraucher in vielen Zusammenhängen als sensibel einstufen würden, wie z. B. Fotos, Kontakte, Kalendereinträge oder Aufnahme von Audio- oder Videoinhalten.*"

[36] Ebenda, S. 34-35: „*Eine allgemeine Einwilligung ohne genaue Angabe des Ziels der Verarbeitung, der die betroffene Person zustimmt, entspricht dieser Anforderung nicht. Das bedeutet, dass die Informationen über*

Das Konzept „für den konkreten Fall“ betrifft auch die Praxis von Werbetreibenden und anderen Dritten, das Nutzerverhalten zu verfolgen (Tracking). Die von den Betriebssystemen und Apps vorgegebenen Standardeinstellungen müssen so gestaltet sein, dass jegliches Tracking vermieden wird, um es den Nutzern zu ermöglichen, für diese Art der Datenverarbeitung eine Einwilligung für den konkreten Fall zu erteilen. Diese Standardeinstellungen dürfen von Dritten nicht umgangen werden (wie derzeit häufig bei in Browsern implementierten „Do Not Track“-Mechanismen).

Beispiele für Einwilligung für den konkreten Fall

Eine App stellt Informationen über in der Umgebung befindliche Restaurants bereit. Der App-Entwickler muss eine Einwilligung für die Installation der App einholen. Für den Zugriff auf Geolokalisierungsdaten muss der App-Entwickler eine gesonderte Einwilligung einholen, z. B während der Installation oder vor Zugriff auf die Geolokalisierung.

„Für den konkreten Fall“ bedeutet, dass die Einwilligung auf den spezifischen Zweck, dem Nutzer nahe gelegene Restaurants mitzuteilen, beschränkt sein muss. Ein Zugriff auf die Standortdaten des Endgeräts darf daher nur erfolgen, wenn der Nutzer die App für diesen Zweck verwendet. Die Einwilligung des Nutzers für die Verarbeitung von Geolokalisierungsdaten ist keine Erlaubnis dafür, dass die App fortlaufend Standortdaten vom Endgerät erfasst. Für diese weitere Verarbeitung wären eine zusätzliche Unterrichtung des Nutzers und eine gesonderte Einwilligung erforderlich.

Damit eine Kommunikations-App auf die Kontaktliste zugreifen kann, muss der Nutzer daher Kontakte auswählen können, mit denen er kommunizieren möchte, und darf nicht gezwungen sein, den Zugriff auf das gesamte Adressbuch (einschließlich der Kontaktdaten von Nichtnutzern dieses Dienstes, die der Verarbeitung der sie betreffenden Daten nicht zugestimmt haben können) zu gewähren.

Es ist jedoch zu beachten, dass selbst auch eine Einwilligung, die die vorstehenden Anforderungen erfüllt, keine Zustimmung zu einer Verarbeitung entgegen dem Gebot von Treu und Glauben und dem Gebot der Rechtmäßigkeit darstellt. Wenn der Zweck der Datenverarbeitung übermäßig und/oder unverhältnismäßig ist, besteht für den App-Entwickler selbst dann keine gültige Rechtsgrundlage für die Verarbeitung, wenn der Nutzer seine Einwilligung erteilt hat, und entsprechend ist in diesem Fall wahrscheinlich von einem Verstoß gegen die Datenschutzrichtlinie auszugehen.

Beispiel für übermäßige und unrechtmäßige Datenverarbeitung

Eine Wecker-App bietet eine optionale Funktion, mit der der Nutzer per Sprachbefehl den Weckton ausschalten oder den Schlummerstatus aktivieren kann. In diesem Beispiel ist die Einwilligung für die Aufnahmefunktion auf den Zeitraum beschränkt, in dem der Weckton

---

das Ziel der Verarbeitung nicht Teil der allgemeinen Bestimmungen sein dürfen, sondern in einer gesonderten Einwilligungsklausel angeführt sein müssen.“

erklingt. Jegliche Audioüberwachung oder -aufnahme in der Zeit, in der der Weckton nicht erklingt, wird als übermäßig und unrechtmäßig angesehen.

Bei Apps, die standardmäßig auf dem Endgerät installiert sind (bevor der Endnutzer das Gerät erwirbt), und bei sonstigen vom Betriebssystem durchgeführten Verarbeitungen, die einer Einwilligung als Rechtsgrundlage bedürfen, müssen die für die Verarbeitung Verantwortlichen sorgfältig abwägen, ob diese Einwilligung wirklich gültig ist. In vielen Fällen sollte ein gesonderter Einwilligungsmechanismus erwogen werden, zum Beispiel beim ersten Aufruf der App, um dem für die Verarbeitung Verantwortlichen eine ausreichende Gelegenheit zu geben, den Endnutzer vollständig zu informieren. Wenn es sich bei den Daten um spezielle Datenkategorien gemäß Artikel 8 der Datenschutzrichtlinie handelt, muss eine ausdrückliche Einwilligung vorliegen.

Und schließlich müssen Nutzer die Möglichkeit erhalten, ihre Einwilligung einfach und wirksam zu widerrufen. Dies wird in Abschnitt 3.8 der vorliegenden Stellungnahme näher ausgeführt.

3.4.2 Rechtsgrundlagen für Datenverarbeitung während der Nutzung der App

Wie bereits erläutert, bildet die Einwilligung die Rechtsgrundlage dafür, dass der App-Entwickler Informationen rechtmäßig lesen und/oder schreiben und daher personenbezogene Daten verarbeiten darf. In einer späteren Phase kann sich der App-Entwickler während der Nutzung der App für andere Arten der Datenverarbeitung auf weitere Rechtsgrundlagen berufen, sofern keine sensiblen personenbezogenen Daten verarbeitet werden.

Solche Rechtsgrundlagen können nach Artikel 7 Buchstaben b und f der Datenschutzrichtlinie die Notwendigkeit für die Erfüllung eines Vertrags mit der betroffenen Person oder die Notwendigkeit für rechtmäßige (geschäftliche) Interessen sein.

Diese Rechtsgrundlagen sind auf die Verarbeitung nicht sensibler Daten eines spezifischen Nutzers beschränkt und können nur in dem Umfang geltend gemacht werden, in dem eine bestimmte Datenverarbeitung für die Erbringung des gewünschten Dienstes erforderlich ist, bzw. – im Fall von Artikel 7 Buchstabe f – wenn die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Beispiele für vertragliche Rechtsgrundlagen

Ein Nutzer erteilt seine Einwilligung für die Installation einer Mobile-Banking-App. Um eine Anforderung für die Durchführung einer Zahlung zu erfüllen, benötigt die Bank keine gesonderte Einwilligung des Nutzers zur Weitergabe seines Namens und seiner Kontonummer an den Zahlungsempfänger. Diese Weitergabe ist für die Erfüllung des Vertrags mit diesem spezifischen Nutzer unbedingt erforderlich, und daher hat die Bank eine Rechtsgrundlage gemäß Artikel 7 Buchstabe b der Datenschutzrichtlinie. Die gleiche Argumentation gilt für Kommunikations-Apps. Wenn Kommunikations-Apps einer anderen Person, mit der der Nutzer kommunizieren möchte, wichtige Informationen wie einen Kontonamen, eine E-Mail-Adresse oder eine Telefonnummer übermitteln, ist diese Weitergabe von Daten naturgemäß für die Erfüllung des Vertrags erforderlich.

3.5 Zweckbindung und Datenminimierung

Die Zweckbindung und die Datenminimierung sind Grundprinzipien der Datenschutzrichtlinie. Aufgrund der jeweiligen Zweckbindung können Nutzer bewusst entscheiden, ob sie ihre personenbezogenen Daten einer Partei anvertrauen möchten, da sie erfahren, wie ihre Daten verwendet werden, und da sie aufgrund der Beschreibung der Zweckbindung verstehen können, wozu ihre Daten verwendet werden. Die Zwecke der Datenverarbeitung müssen daher genau festgelegt und für einen durchschnittlichen Nutzer ohne rechtliche oder technische Fachkenntnisse verständlich sein.

Gleichzeitig bedeutet die Zweckbindung, dass App-Entwickler einen guten Überblick über ihren Business Case haben, bevor sie mit der Erfassung personenbezogener Daten von Nutzern beginnen. Personenbezogene Daten dürfen nur für Zwecke verarbeitet werden, die dem Gebot von Treu und Glauben und dem Gebot der Rechtmäßigkeit entsprechen (Artikel 6 Absatz 1 Buchstabe a der Datenschutzrichtlinie). Diese Zwecke müssen vor Durchführung der Datenverarbeitung festgelegt sein.

Der Grundsatz der Zweckbindung schließt plötzliche Änderungen in den wichtigen Bedingungen der Verarbeitung aus.

Beispiel: Eine App hatte sollte den Nutzern ursprünglich ermöglichen, per E-Mail miteinander zu kommunizieren. Der Entwickler beschließt jedoch, sein Geschäftsmodell zu ändern und führt die E-Mail-Adressen seiner Nutzer mit den Telefonnummern von Nutzern einer anderen App zusammen. In diesem Fall müssten die jeweiligen für die Verarbeitung Verantwortlichen alle Nutzer einzeln verständigen und ihre vorherige ohne jeden Zweifel gegebene Einwilligung für diesen neuen Zweck der Verarbeitung ihrer personenbezogenen Daten einholen.

Die Zweckbindung ist mit dem Grundsatz der Datenminimierung eng verknüpft. Um eine unnötige und potenziell unrechtmäßige Datenverarbeitung zu verhindern, müssen App-Entwickler sorgfältig abwägen, welche Daten für die Durchführung der gewünschten Funktion unbedingt erforderlich sind.

Apps können einen Zugriff auf viele Funktionen des Endgeräts erlangen und daher viele Aktionen durchführen (z. B. eine Stealth SMS senden oder auf Bilder und das gesamte Adressbuch zugreifen). Viele App-Stores unterstützen (halb-)automatische Aktualisierungen, bei denen der App-Entwickler unter geringen Eingaben des Endnutzers oder sogar ohne jegliche Eingaben des Endnutzers neue Funktionen integrieren und verfügbar machen kann.

Die Datenschutzgruppe betont an dieser Stelle, dass Dritte, die über Apps Zugriff auf die Nutzerdaten erlangen, die Grundsätze der Zweckbindung und der Datenminimierung beachten müssen. Eindeutige und häufig unveränderliche Gerätekennungen sollten nicht zur interessenbezogenen Werbung und/oder Analyse verwendet werden, da die Nutzer keine Möglichkeit haben, ihre Einwilligung zu widerrufen. App-Entwickler sollten gewährleisten, dass eine schleichende Ausweitung der Zweckbestimmung verhindert wird, indem sie die Verarbeitung von einer App-Version zur nächsten nicht ändern, ohne den Endnutzern angemessene Informationsmeldungen zu senden und Gelegenheiten einzuräumen, entweder die Verarbeitung zu unterbinden oder den gesamten Dienst zu kündigen. Außerdem sollten technische Mittel bereitgestellt werden, mit denen die Nutzer die Angaben über die erklärten

Zwecke überprüfen können, indem sie Zugriff auf die Informationen über die ausgehende Datenverkehrsmenge pro App im Verhältnis zum nutzerinitiierten Datenverkehr erhalten.

Die Unterrichtung der Nutzer und Nutzerkontrollen sind die wichtigsten Funktionen, mit den die Beachtung der Grundsätze der Datenminimierung und der Zweckbindung gewährleistet werden kann.

Indem die Hersteller von Betriebssystemen und Endgeräten sowie App-Stores über Programmierschnittstellen auf die zugrunde liegenden Daten auf dem Endgerät zugreifen, erhalten sie die Möglichkeit, spezifische Regeln durchzusetzen und den Endnutzern angemessene Informationen bereitzustellen. Beispielsweise sollten die Hersteller von Betriebssystemen und Endgeräten eine Programmierschnittstelle mit präzisen Kontrollfunktionen zur Differenzierung zwischen den verschiedenen Datenarten bereitstellen und gewährleisten, dass App-Entwickler Zugriff nur zu den Daten anfordern können, die für die (rechtmäßige) Funktion ihrer App unbedingt erforderlich sind. Die von den App-Entwicklern angeforderten Datenarten können dann im App-Store deutlich angezeigt werden, um die Nutzer vor der Installation entsprechend zu informieren.

In dieser Hinsicht beruht die Kontrolle des Zugriffs auf die Daten, die auf dem Endgerät gespeichert sind, auf verschiedenen Mechanismen:

a. Hersteller von Betriebssystemen und Endgeräten legen **Regeln** fest, die für das Angebot von Apps in ihrem App-Store gelten: App-Entwickler müssen diese Regeln beachten oder das Risiko eingehen, dass ihre Apps in diesen App-Stores nicht angeboten werden können.[37]

b. Die **Programmierschnittstellen (APIs)** der Betriebssysteme legen Standardmethoden für den Zugriff von Apps auf die auf dem Telefon gespeicherten Daten fest. Sie wirken sich auch auf die serverseitige Erfassung von Daten aus.

c. **Ex-ante-Kontrollen** sind Kontrollen, die vor der Installation einer App durchgeführt werden.[38]

d. **Ex-post-Kontrollen** sind Kontrollen, die nach der Installation einer App durchgeführt werden.

3.6 Sicherheit

Gemäß Artikel 17 der Datenschutzrichtlinie müssen die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung des Schutzes der von ihnen verarbeiteten personenbezogenen Daten durchführen. Insoweit müssen alle in Abschnitt 3.3 genannten

---

[37] Endgeräte, die mittels eines „Jailbreak“ entsperrt wurden, erlauben die Installation von Apps außerhalb offizieller App-Stores; Android-Geräte erlauben ebenfalls die Installation von Apps, die von anderen Quellen erworben wurden.

[38] Sonderfall: vorinstallierte Apps.

Akteure Maßnahmen entsprechend ihrer jeweiligen Rolle und Verantwortlichkeit durchführen.

Durch die Erfüllung der Sicherheitsverpflichtung werden zwei Ziele erreicht: Die Nutzer werden in die Lage versetzt, ihre Daten besser zu kontrollieren, und das Vertrauen in die Rechtspersonen, die die Nutzerdaten tatsächlich nutzen oder verarbeiten, wird erhöht.

Um ihren jeweiligen Sicherheitsverpflichtungen als für die Verarbeitung Verantwortliche nachzukommen, müssen App-Entwickler, App-Stores, Hersteller von Betriebssystemen und Endgeräten sowie Dritte die Grundsätze des eingebauten Datenschutzes (Privacy by Design) und der datenschutzfreundlichen Voreinstellungen (Privacy by Default) beachten. Dies setzt die fortlaufende Bewertung bestehender wie zukünftiger Datenschutzrisiken sowie die Einführung und Bewertung wirksamer Maßnahmen zur Minimierung dieser Risiken voraus (u. a. durch Datenminimierung).

App-Entwickler

Hersteller von Betriebssystemen und Endgeräten sowie unabhängige Dritte (z. B. die ENISA) haben zahlreiche Leitlinien zur Sicherheit mobiler Apps veröffentlicht.[39]

Ein Überblick über sämtliche bewährten Praktiken im Bereich der Sicherheit bei der Entwicklung von Apps würde den Rahmen dieser Stellungnahme sprengen. Die Datenschutzgruppe nutzt diese Gelegenheit jedoch für einen Überblick über die Sicherheitspraktiken, die mit schwerwiegenden Auswirkungen auf die Grundrechte von App-Nutzern verbunden sein können.

Eine wichtige Entscheidung vor der Konzeption einer App ist die Frage, wo die Daten gespeichert werden. In einigen Fällen werden Nutzerdaten auf dem Endgerät gespeichert, aber App-Entwickler können auch eine Client-Server-Architektur nutzen. In diesem Fall werden personenbezogene Daten auf die Systeme der Dienstleister übertragen oder kopiert. Wenn die Speicherung und Verarbeitung der Daten auf dem Gerät erfolgt, haben die Endnutzer die größte Kontrolle über diese Daten. Sie können die Daten beispielsweise löschen, wenn sie ihre Einwilligung für ihre Verarbeitung widerrufen. Eine sichere Speicherung von Daten an einem entfernten Standort kann jedoch eine Wiederherstellung der Daten nach Diebstahl oder Verlust eines Geräts erleichtern. Mischlösungen sind ebenfalls möglich.

App-Entwickler müssen eine klare Strategie für die Entwicklung und die Verbreitung der Software festlegen. Auch die Hersteller der Betriebssysteme und der Endgeräte spielen bei der Förderung einer sicheren Verarbeitung durch Apps eine Rolle; diese Rolle wird in einem späteren Abschnitt näher ausgeführt. Außerdem müssen App-Entwickler und App-Stores eine sicherheitsfördernde Umgebung erarbeiten und einführen, in der geeignete Hilfsmittel die Verbreitung bösartiger Apps verhindern und die einfache Installation/Deinstallation einzelner Apps ermöglichen.

---

[39] ENISA „Smartphone Secure Development Guideline“: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

Bewährte Praktiken, die während der Konzeption einer App implementiert werden können, beinhalten die Minimierung der Länge und der Komplexität des Codes sowie die Implementierung von Kontrollen, durch die eine unbeabsichtigte Datenübertragung oder ein unberechtigter Datenzugriff ausgeschlossen wird. Ferner sollten alle Eingaben validiert werden, um einen Pufferüberlauf oder Injection-Angriffe zu verhindern. Weitere erwähnenswerte Sicherheitsmechanismen sind angemessene Strategien für Sicherheitspatches und regelmäßige unabhängige Systemsicherheitsprüfungen. Außerdem sollten die Kriterien für die Konzeption von Apps regelmäßig das Prinzip der geringstmöglichen Berechtigungsvergabe („Least Privilege"-Prinzip) beinhalten, nach dem Apps nur auf die Daten zugreifen können, die sie tatsächlich benötigen, um eine Funktion für den Nutzer bereitzustellen. App-Entwickler und App-Stores sollten die Nutzer auch durch Warnhinweise motivieren, diese bewährten Konzeptionspraktiken durch gute Nutzerpraktiken (z. B. Aktualisierung der Apps auf die neuesten verfügbaren Versionen) zu ergänzen, und durch wiederholte Hinweise daran erinnern, die Verwendung des gleichen Passworts für verschiedene Dienste zu vermeiden.

In der Konzeptionsphase von Apps müssen die App-Entwickler auch Maßnahmen zur Verhinderung eines unberechtigten Zugriffs auf personenbezogene Daten treffen, indem sie sicherstellen, dass die Daten gegebenenfalls sowohl bei der Übertragung als auch nach Speicherung geschützt sind.

Mobile Apps sollten innerhalb spezifischer Speicherbereiche des Endgeräts („Sandboxes"[40]) laufen, um die Folgen von Schadprogrammen/bösartigen Apps zu verringern. Die App-Entwickler müssen in enger Zusammenarbeit mit dem Hersteller des Betriebssystems und/oder dem App-Store verfügbare Mechanismen einsetzen, durch die die Nutzer zum einen sehen können, welche Daten von welchen Apps verarbeitet werden, und zum anderen Berechtigungen gezielt aktivieren und deaktivieren können. Die Verwendung verborgener Funktionen sollte nicht zugelassen sein.

App-Entwickler müssen ihre Methoden der Nutzeridentifizierung und -authentifizierung bewusst wählen. Sie sollten keine persistenten (gerätespezifischen) Kennungen, sondern stattdessen appspezifische oder temporäre Kennungen mit niedriger Entropie verwenden, um ein langfristiges Tracking der Nutzer zu verhindern. Es sollten datenschutzfreundliche Authentifizierungsmechanismen in Erwägung gezogen werden. Bei der Authentifizierung von Nutzern müssen die App-Entwickler besondere Sorgfalt auf die Verwaltung von Nutzerkennungen und Passwörtern verwenden. Passwörter müssen verschlüsselt und sicher als verschlüsselte kryptografische Hashwerte gespeichert werden. Die Bereitstellung eines Tests für die Sicherheit der gewählten Passwörter für die Nutzer ist ebenfalls eine gute Methode für die Förderung besserer Passwörter (Entropieprüfung). Gegebenenfalls (beim Zugriff auf sensible Daten, aber auch beim Zugriff auf zahlungspflichtige Ressourcen) könnte eine erneute Authentifizierung in Betracht gezogen werden. Dabei könnten mehrere Faktoren einbezogen und unterschiedliche Kanäle (z. B. Senden des Zugangscodes per SMS) und/oder auf den Endnutzer (und nicht auf das Endgerät) bezogene Authentifizierungsdaten genutzt werden. Außerdem sollten bei der Wahl von Sitzungskennungen nicht-vorhersagbare

[40] Eine „Sandbox" ist ein Sicherheitsmechanismus zur Trennung laufender Programme.

Zeichenfolgen verwendet werden, möglicherweise kombiniert mit Kontextinformationen wie Datum und Uhrzeit, aber auch IP-Adresse oder Geolokalisierungsdaten.

App-Entwickler sollten auch die Anforderungen der Datenschutzrichtlinie in Bezug auf Verletzungen des Schutzes personenbezogener Daten und die Notwendigkeit einer proaktiven Unterrichtung der Nutzer beachten. Diese Anforderungen gelten derzeit zwar nur für Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste. Es wird jedoch erwartet, dass die Verpflichtung entsprechend den Vorschlägen der Kommission im Rahmen der zukünftigen Datenschutzrichtlinie (COM 2012/0011/COD) auf alle für die Verarbeitung Verantwortlichen (und Auftragsverarbeiter) ausgeweitet wird. Auch dies unterstreicht die Notwendigkeit der Erstellung und der fortlaufenden Bewertung eines umfassenden „Sicherheitsplans", der die Erfassung, Speicherung und Verarbeitung sämtlicher personenbezogener Daten abdeckt, um solche Datenschutzverletzungen sowie die Verhängung der für solche Fälle vorgesehenen hohen Geldstrafen zu vermeiden. Der Sicherheitsplan muss unter anderem ein Schwachstellenmanagement (Vulnerability Management) und sichere Freigabeabläufe für zuverlässige Aktualisierungen zur Fehlerbehebung (Bugfixes) vorsehen.

Die Verantwortung der App-Entwickler für die Sicherheit ihrer Produkte endet nicht mit der Freigabe einer Arbeitsversion auf dem Markt. Wie jedes Software-Produkt können Apps Sicherheitsmängel und Schwachstellen aufweisen, und die App-Entwickler müssen entsprechende Fixes oder Patches entwickeln und entweder den Nutzern direkt zur Verfügung stellen oder den Akteuren übermitteln, die diese Fixes oder Patches den Nutzern bereitstellen.

App-Stores

App-Stores sind ein wichtiger Vermittler zwischen Endnutzern und App-Entwicklern und sollten die Apps einer Reihe robuster und wirksamer Kontrollen unterziehen, bevor sie Apps für den Markt freigeben. Sie sollten Informationen über die tatsächlich durchgeführten Kontrollen bereitstellen (u. a. Informationen über die Art der durchgeführten Datenschutzprüfungen).

Diese Maßnahme kann zwar die Verbreitung bösartiger Apps nicht vollständig unterbinden, aber die Statistik zeigt, dass die Verfügbarkeit bösartiger Funktionen in „offiziellen" App-Stores durch diese Praxis stark reduziert wird.[41] Zur Bewältigung der großen Mengen von Apps, die täglich neu angeboten werden, könnte dieser Prozess durch die Verfügbarkeit automatischer Analysewerkzeuge und durch die Einführung von Informationsaustausch-Kanälen zwischen Sicherheitsfachleuten und Software-Spezialisten sowie durch die Einführung wirksamer Verfahren und Strategien für die Handhabung gemeldeter Probleme optimiert werden.

Zusätzlich zur Prüfung von Apps vor der Aufnahme in den App-Store könnte auch ein öffentlicher Reputationsmechanismus für Apps eingeführt werden. Die Nutzer sollten sich nicht nur daran orientieren, wie „cool" eine App ist, sondern auch Grundlage der angebotenen Funktionen berücksichtigen; dabei sind insbesondere die Mechanismen zur Gewährleistung

---

[41] *„Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets"*, Y Zhou u. a., Network and Distributed System Security Symposium (NDSS) 2012.

des Datenschutzes und des Schutzes der Privatsphäre zu beachten. Außerdem sollten Reputationsmechanismen so gestaltet sein, dass falsche Bewertungen verhindert werden. Die Qualifizierungs- und Reputationsmechanismen für Apps können wirksam zum Vertrauensaufbau zwischen den verschiedenen Akteuren beitragen, besonders wenn die Daten über eine lange Kette von Dritten ausgetauscht werden.

App-Stores verfügen häufig über eine Methode zur Fern-Deinstallation bösartiger oder unsicherer Apps. Bei ungeeigneter Konzipierung kann dieser Mechanismus allerdings kontraproduktiv für das angestrebte Ziel sein, dass die Nutzer ihre Daten besser kontrollieren können sollen. Ein datenschutzfreundliches Mittel zur Fern-Deinstallation von Apps durch einen App-Store sollte daher auf der Unterrichtung und der Einwilligung der Nutzer beruhen. Unter eher praktischen Aspekten sollte den Nutzern darüber hinaus die Übermittlung von Rückmeldungen ermöglicht werden, damit die Nutzer Informationen über Sicherheitsprobleme bei ihren Apps und über die Wirksamkeit möglicher Fern-Deinstallationsverfahren mitteilen können.

Ebenso wie die App-Entwickler sollten auch die App-Stores zukünftige Mitteilungspflichten bei Verletzungen des Schutzes personenbezogener Daten berücksichtigen und eng mit den App-Entwicklern zusammenarbeiten, um entsprechende Verletzungen zu vermeiden.

Hersteller von Betriebssystemen und Endgeräten

Hersteller von Betriebssystemen und Endgeräten sind ebenfalls wichtige Akteure bei der Festlegung von Mindeststandards und bewährten Praktiken für App-Entwickler, nicht nur in Bezug auf die Sicherheit der zugrunde liegenden Software und der Programmierschnittstellen, sondern auch in Bezug auf die Werkzeuge, Leitlinien und Referenzmaterialien, die sie bereitstellen. Hersteller von Betriebssystemen und Endgeräten sollten sichere und bekannte Verschlüsselungsalgorithmen bereitstellen und angemessene Schlüssellängen unterstützen. Außerdem sollten sie strenge und sichere Authentifizierungsmechanismen für die App-Entwickler bereitstellen (z. B. die Verwendung von seitens vertrauenswürdiger Zertifizierungsbehörden signierten Zertifikaten zur Prüfung der Autorisierung einer entfernten Ressource). Dadurch würde auch die Notwendigkeit der Entwicklung proprietärer Authentifizierungsmechanismen durch App-Entwickler entfallen. In der Praxis werden diese Mechanismen häufig unzureichend umgesetzt und können eine gravierende Schwachstelle sein.[42]

Der Zugriff auf personenbezogene Daten und die Verarbeitung solcher Daten durch Apps sollten über in die Programmierschnittstelle integrierte Klassen und Methoden erfolgen, die angemessene Kontrollen und Sicherheitsvorrichtungen bieten. Die Hersteller von Betriebssystemen und Endgeräten sollten sicherstellen, dass die Methoden und Funktionen für den Zugriff auf personenbezogene Daten Funktionen umfassen, die auf die Implementierung

---

[42] Vor Kurzem wurde darauf hingewiesen, dass fehlende visuelle Sicherheitshinweise für die SSL-/TLS-Verwendung sowie die unzureichende Verwendung von SSL/TLS für Man-in-the-Middle-Angriffe (MITM-Angriffe) genutzt werden können. Aktuellen Forschungsergebnissen zufolge umfasst die gesamte installierte Basis der Apps mit bestätigten Schwachstellen in Bezug auf MITM-Angriffe mehrere Millionen Nutzer. „*Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security*“, Bernd Freisleben und Matthew Smith, 19th ACM Conference on Computer and Communications Security (ACM CCS 2012).

differenzierter Einwilligungsanfragen abzielen. Ferner sollten Maßnahmen ergriffen werden, um den Zugriff auf personenbezogene Daten unter Verwendung von Low-Level-Funktionen oder anderen Mitteln (die in die Programmierschnittstellen integrierte Kontrollen und Sicherheitsvorrichtungen umgehen könnten) auszuschließen oder einzuschränken.

Die Hersteller von Betriebssystemen und Endgeräten müssen klare Prüfpfade für die Geräte entwickeln, damit die Endnutzer eindeutig feststellen können, welche Apps auf die Daten auf ihren Geräten zugegriffen haben.

Alle Parteien müssen rasch auf Sicherheitsschwachstellen reagieren, damit Endnutzer nicht unnötig lange mit Sicherheitsmängeln konfrontiert sind. Einige Hersteller von Betriebssystemen und Endgeräten (sowie Telekommunikationsbetreiber, die Markengeräte verbreiten) stellen leider keine langfristige Unterstützung für Betriebssystem-Versionen bereit; in diesen Fällen sind die Nutzer in Bezug auf bekannte Sicherheitsschwachstellen nicht geschützt. Gemeinsam mit den App-Entwicklern müssen die Hersteller von Betriebssystemen und Endgeräten die Endnutzer im Voraus über den Zeitraum informieren, in dem sie regelmäßige Sicherheitsaktualisierungen erwarten können. Zudem sollten sie die Nutzer schnellstmöglich unterrichten, wenn ein Sicherheitsproblem mithilfe einer Aktualisierung behoben werden muss.

Dritte

Die vorstehend genannten Sicherheitsfunktionen und -überlegungen gelten auch für Dritte, wenn diese personenbezogene Daten für ihre eigenen Zwecke erfassen und verarbeiten (d. h. in erster Linie Werbetreibende und Analysedienstleister). Dies umfasst die sichere Übertragung und die verschlüsselte Speicherung von eindeutigen Gerätekennungen und von Kennungen der App-Nutzer sowie von sonstigen personenbezogenen Daten.

3.7 Information

3.7.1 Informationspflicht und vorgeschriebener Inhalt

Gemäß Artikel 10 der Datenschutzrichtlinie hat jede betroffene Person das Recht, die Identität des für die Verarbeitung Verantwortlichen zu erfahren, der ihre personenbezogenen Daten verarbeitet. In Bezug auf Apps hat der Endnutzer zudem das Recht, zu erfahren, welche Art personenbezogener Daten verarbeitet wird und für welchen Zweck die Daten verwendet werden sollen. Wenn die personenbezogenen Daten des Nutzers aus den Datenbeständen anderer Akteure im App-Ökosystem erfasst werden (entsprechend der Beschreibung in Abschnitt 3.3 der vorliegenden Stellungnahme), hat der Endnutzer gemäß Artikel 11 der Datenschutzrichtlinie trotzdem das Recht, über eine solche Datenverarbeitung in gleicher Weise unterrichtet zu werden. Wenn der entsprechende für die Verarbeitung Verantwortliche personenbezogene Daten verarbeitet, muss er potenzielle Nutzer zumindest mitteilen,

- wer er ist (Identität und Kontaktdaten),
- welche Kategorien personenbezogener Daten der App-Entwickler im Einzelnen erfassen und verarbeiten wird,
- warum die betreffenden personenbezogenen Daten erfasst und verarbeitet werden (genaue Zwecke),

- ob die Daten an Dritte weitergegeben werden,

- wie Nutzer ihre Rechte in Bezug auf Widerruf der Einwilligung und Löschung von Daten wahrnehmen können.

Die Verfügbarkeit dieser Informationen über die Verarbeitung personenbezogener Daten ist entscheidend für die Einholung der Einwilligung für die Datenverarbeitung vom Nutzer. Eine Einwilligung kann nur gültig sein, wenn die betroffene Person zuvor über die wichtigsten Elemente der Datenverarbeitung informiert wurde. Wenn diese Informationen erst bereitgestellt werden, nachdem die App bereits mit der Verarbeitung personenbezogener Daten begonnen hat (was häufig schon während der Installation geschieht), wird dies nicht als ausreichend erachtet und ist rechtlich unwirksam. In Übereinstimmung mit dem FTC-Bericht betont die Datenschutzgruppe die Notwendigkeit, Informationen zu dem Zeitpunkt bereitzustellen, an dem sie für die Verbraucher relevant sind: direkt vor der Erfassung von Daten durch Apps. Die Unterrichtung darüber, welche Daten verarbeitet werden, ist besonders wichtig in Anbetracht des umfassenden Zugriffs, den Apps normalerweise auf Sensoren und Datenstrukturen auf dem Gerät haben, wobei dieser Zugriff in vielen Fällen nicht intuitiv offensichtlich ist. Eine angemessene Unterrichtung ist auch dann von entscheidender Bedeutung, wenn die App besondere Kategorien personenbezogener Daten verarbeitet, z. B. Daten über den Gesundheitszustand, politische Überzeugungen, sexuelle Ausrichtung usw. Und schließlich sollte der App-Entwickler deutlich zwischen obligatorischen und optionalen Informationen unterscheiden, und das System sollte dem Nutzer ermöglichen, mit datenschutzfreundlichen Standardoptionen den Zugriff auf optionale Informationen zu verweigern.

Hinsichtlich der Identität des für die Verarbeitung Verantwortlichen ist festzustellen, dass die Nutzer wissen müssen, wer für die Verarbeitung ihrer personenbezogenen Daten rechtlich verantwortlich ist und wie der für die Verarbeitung Verantwortliche kontaktiert werden kann. Ansonsten können sie ihre Rechte (z. B. das Recht auf Zugang zu den (an einem entfernten Standort) über sie gespeicherten Daten) nicht wahrnehmen. Aufgrund der Fragmentierung im App-Umfeld ist es überaus wichtig, dass für jede App ein einziger Ansprechpartner besteht, der für die gesamte Datenverarbeitung über die jeweilige App die Verantwortung übernimmt. Es darf nicht dem Endnutzer überlassen bleiben, die Beziehungen zwischen App-Entwicklern und anderen Parteien zu recherchieren, die personenbezogene Daten über die App verarbeiten.

In Bezug auf den Zweck/die Zwecke müssen die Nutzer angemessen darüber informiert werden, welche Daten über sie erfasst werden und warum die Daten erfasst werden. Die Nutzer sollten in klarer und verständlicher Sprache darüber unterrichtet werden, ob die Daten von Dritten weiterverwendet werden können, und wenn ja, für welche Zwecke. Ungenau festgelegte Zwecke wie „Produktinnovation“ sind für die Unterrichtung der Nutzer unzureichend. Es sollte klar mitgeteilt werden, ob die Nutzer zu einem späteren Zeitpunkt um ihre Einwilligung zur Weitergabe von Daten an Dritte zu Werbe- und/oder Analysezwecken gebeten werden. Den App-Stores obliegt die wesentliche Verantwortung, sicherzustellen, dass diese Informationen für jede App verfügbar und leicht zugänglich sind.

Die App-Stores tragen wesentliche Verantwortung dafür, eine angemessene Unterrichtung der Nutzer sicherzustellen. Es wird nachdrücklich empfohlen, visuelle Hinweise oder Symbole in Bezug auf die Datenverwendungen einzusetzen, um die Nutzer über die Arten der Datenverarbeitung zu informieren.

Zusätzlich zu dem genannten Mindestumfang der Informationen, die für die Einholung einer Einwilligung der App-Nutzer erforderlich sind, empfiehlt die Datenschutzgruppe zum Zwecke einer Verarbeitung nach Treu und Glauben nachdrücklich, dass die für die Verarbeitung Verantwortlichen den Nutzern auch folgende Informationen bereitstellen:

- Erwägungen zur Verhältnismäßigkeit für die Arten der Daten auf dem Gerät, die erfasst werden oder auf die zugegriffen wird,
- Speicherfristen für die Daten,
- vom für die Verarbeitung Verantwortlichen ergriffene Sicherheitsmaßnahmen.

Außerdem empfiehlt die Datenschutzgruppe, dass App-Entwickler in ihren für europäische Nutzer bestimmten Datenschutzerklärungen Informationen darüber aufnehmen, in welcher Weise die App dem europäischen Datenschutzrecht entspricht. In diesem Zusammenhang sollten auch mögliche Übertragungen personenbezogener Daten aus Europa beispielsweise in die USA berücksichtigt werden. Außerdem sollte erläutert werden, ob und wie die App in solchen Fällen der Safe-Harbor-Vereinbarung entspricht.

3.7.2 Form der Aufklärung

Die entscheidenden Informationen über die Datenverarbeitung müssen den Nutzern vor der Installation der App über den App-Store zur Verfügung stehen. Außerdem müssen die relevanten Informationen über die Datenverarbeitung auch nach der Installation innerhalb der App zugänglich sein.

Hinsichtlich der Aufklärung der Nutzer kommt den App-Stores zusammen mit den Entwicklern der Apps die Rolle eines gemeinsam für die Verarbeitung Verantwortlichen zu. In dieser Eigenschaft müssen sie sicherstellen, dass jede App die entscheidenden Informationen über die Verarbeitung personenbezogener Daten bereitstellt. Sie sollten die Hyperlinks zu Seiten mit Datenschutzinformationen überprüfen und Apps mit fehlerhaften Links oder anderweitig nicht zugänglichen Informationen über die Datenverarbeitung entfernen.

Nach Auffassung der Datenschutzgruppe sollten Informationen über die Verarbeitung personenbezogener Daten ebenfalls verfügbar und leicht auffindbar sein, beispielsweise innerhalb des App-Store und vorzugsweise auf den regulären Websites des für die App verantwortlichen App-Entwicklers. Es ist nicht akzeptabel, dass Nutzer vom App-Entwickler oder einem sonstigen für die Verarbeitung Verantwortlichen nicht direkt informiert werden, sondern genötigt werden, im Internet nach Informationen über die Datenverarbeitungsstrategie einer App zu suchen.

Zumindest sollte jede App eine lesbare, verständliche und leicht zugängliche Datenschutzerklärung beinhalten, in der sämtliche vorstehend genannten Informationen enthalten sind. Viele Apps erfüllen diese Mindestanforderung an die Transparenz nicht. Nach einer FPF-Studie vom Juni 2012 haben 56 % der kostenpflichtigen Apps und fast 30 % der kostenlosen Apps keine Datenschutzerklärung.

Apps, die keine personenbezogenen Daten verarbeiten oder nicht für eine solche Verarbeitung bestimmt sind, sollten dies in ihrer Datenschutzerklärung klar angeben.

Natürlich ist der Umfang der auf einem kleinen Display darstellbaren Informationen beschränkt. Dies ist jedoch keine Entschuldigung für eine unzureichende Information der Endnutzer. Mit unterschiedlichen Strategien kann sichergestellt werden, dass den Nutzern die wichtigsten Elemente des Dienstes bekannt sind. Die Datenschutzgruppe hält die Verwendung von Mehrebenen-Erklärungen für hilfreich (siehe Stellungnahme 10/2004 der Datenschutzgruppe),[43] bei denen die zuerst angezeigte Erklärung die im EU-Rechtsrahmen vorgeschriebenen Mindestinformationen enthält, und weitere Informationen über Hyperlinks zur vollständigen Datenschutzerklärung abzurufen sind. Die Informationen sollten direkt auf dem Bildschirm angezeigt werden und leicht zugänglich und gut sichtbar sein. Neben verständlichen Informationen, die für das kleine Display mobiler Endgeräte geeignet sind, müssen die Nutzer die Möglichkeit haben, über Links zu umfassenderen Erläuterungen – beispielsweise in der Datenschutzerklärung – zu wechseln, in denen ausgeführt wird, wie die App personenbezogene Daten verwendet, wer der für die Verarbeitung Verantwortliche ist und wo ein Nutzer seine Rechte geltend machen kann.

Dieser Ansatz kann mit der Verwendung von Symbolen und Bildern sowie von Video- und Audiodaten kombiniert werden und kontextbezogene Echtzeitmeldungen nutzen, wenn eine App auf das Adressbuch oder auf Fotos zugreift.[44] Diese Symbole müssen aussagekräftig sein (d. h. klar, selbsterklärend und eindeutig). Naturgemäß kommt in diesem Zusammenhang auch dem Hersteller des Betriebssystems wesentliche Mitverantwortung im Hinblick auf die Unterstützung der Nutzung solcher Symbole zu.

App-Entwickler verfügen über hervorragende Kenntnisse in der Programmierung und Konzeption komplexer Benutzeroberflächen für kleine Displays, und die Datenschutzgruppe fordert die Branche dazu auf, diese Kreativität für die Bereitstellung weiterer innovativer Lösungen für die wirksame Unterrichtung von Nutzern mobiler Endgeräte zu nutzen. Um sicherzustellen, dass die Informationen tatsächlich für Nutzer ohne technischen oder rechtlichen Hintergrund verständlich sind, empfiehlt die Datenschutzgruppe (in Übereinstimmung mit dem FTC-Bericht) dringend, Verbrauchertests für ausgewählte Informationsstrategien durchzuführen.[45]

3.8 Rechte der betroffenen Person

Nach den Artikeln 12 und 14 der Datenschutzrichtlinie müssen App-Entwickler und andere für die Verarbeitung Verantwortliche den Nutzern im Ökosystem mobiler Apps ermöglichen, ihre Rechte auf Auskunft, Berichtigung und Löschung sowie das Recht auf Widerspruch gegen die Datenverarbeitung wahrzunehmen. Wenn ein Nutzer seinen Auskunftsanspruch geltend macht, muss der für die Verarbeitung Verantwortliche dem Nutzer Informationen über die verarbeiteten Daten und über die Quelle dieser Daten bereitstellen. Wenn der für die Verarbeitung Verantwortliche auf der Grundlage der gesammelten Daten automatisierte Entscheidungen trifft, muss er den Nutzer auch über die diesen Entscheidungen zugrunde liegende Logik informieren. Dies kann etwa der Fall sein, wenn aufgrund finanzieller oder

---

[43] Stellungnahme 10/2004 der Artikel-29-Datenschutzgruppe zu einheitlicheren Bestimmungen über Informationspflichten (Juli 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf.

[44] Beispiel: Das auf iPhones verwendete Warnsymbol für die Verarbeitung von Geolokalisierungsdaten.

[45] FTC-Bericht (siehe Fußnote 6), S. 16.

gesundheitsbezogener Daten oder sonstiger Profildaten die Leistungsfähigkeit oder das Verhalten des Nutzers bewertet werden. Auf Aufforderung des Nutzers muss der für die Verarbeitung Verantwortliche die Berichtigung, Löschung oder Sperrung personenbezogener Daten ermöglichen, wenn diese Daten unvollständig oder unrichtig sind oder wenn die Verarbeitung der Daten unrechtmäßig ist.

Damit die Nutzer die Verarbeitung ihrer personenbezogenen Daten kontrollieren können, müssen Apps die Nutzer klar und gut sichtbar über das Bestehen dieser Auskunfts- und Korrekturmechanismen informieren. Die Artikel-29-Datenschutzgruppe empfiehlt die Konzeption und Implementierung einfacher, aber sicherer Online-Auskunftswerkzeuge. Auskunftswerkzeuge sollten vorzugsweise entweder in der eigentlichen App oder durch Bereitstellung eines Links zu einer Online-Funktion verfügbar sein, über die für die Nutzer sofort ersichtlich ist, welche ihrer Daten verarbeitet werden, und über die die Nutzer die jeweils erforderlichen Erläuterungen erhalten. Ähnliche Initiativen wurden von Online-Dienstleistern durchgeführt (z. B. unterschiedliche „Dashboards“ zur Darstellung erfasster Informationen oder sonstige Auskunftsmechanismen).

Die Notwendigkeit einer einfachen Online-Auskunft ist besonders groß bei Apps, die umfangreiche Nutzerprofile verarbeiten (z. B. bei sozialen Apps, Netzwerk- und Nachrichten-Apps oder Apps, die sensible oder finanzielle Daten verarbeiten). Die Auskunft sollte natürlich nur erteilt werden, wenn die Identität der betroffenen Person festgestellt wurde, um die Weitergabe personenbezogener Daten an Dritte zu verhindern. Diese Verpflichtung zur Prüfung der Identität sollte jedoch nicht zu einer zusätzlichen, übermäßigen Erfassung personenbezogener Daten über die betroffene Person führen. In vielen Fällen könnte eine Authentifizierung anstelle einer (vollständigen) Identifizierung ausreichen.

Außerdem sollten die Nutzer jederzeit die Möglichkeit haben, ihre Einwilligung einfach und unaufwendig zu widerrufen. Eine betroffene Person kann ihre Einwilligung für die Datenverarbeitung auf verschiedenen Wegen und aus verschiedenen Gründen widerrufen. Die Option für den Widerruf der Einwilligung sollte vorzugsweise über die vorstehend genannten, leicht zugänglichen Mechanismen verfügbar sein. Es muss möglich sein, Apps zu deinstallieren und gleichzeitig sämtliche personenbezogenen Daten von den Servern des/der für die Verarbeitung Verantwortlichen zu entfernen. Um den Nutzern zu ermöglichen, ihre Daten durch den App-Entwickler löschen zu lassen, hat der Hersteller des Betriebssystems die wichtige Aufgabe, eine Meldung an den App-Entwickler zu senden, wenn ein Nutzer die App deinstalliert. Eine solche Meldung könnte über die Programmierschnittstelle erfolgen. Wenn ein Nutzer eine App deinstalliert hat, besitzt der Entwickler der betreffenden App grundsätzlich keine Rechtsgrundlage mehr für die weitere Verarbeitung der diesen Nutzer betreffenden personenbezogenen Daten und muss entsprechend sämtliche Daten löschen. Ein App-Entwickler, der bestimmte Daten aufbewahren möchte (beispielsweise um eine erneute Installation der App zu vereinfachen), muss während der Deinstallation eine gesonderte Einwilligung einholen und den Nutzer ersuchen, einer festgelegten zusätzlichen Speicherfrist zuzustimmen. Die einzige Ausnahme von dieser Regel sind möglicherweise bestehende

rechtliche Verpflichtungen zur Speicherung gewisser Daten für spezifische Zwecke (z. B. steuerrechtliche Verpflichtungen im Zusammenhang mit Finanztransaktionen).[46]

3.9 Speicherfristen

App-Entwickler müssen die Speicherung der mit einer App erfassten Daten und die damit verbundenen Datenschutzrisiken abwägen. Die spezifischen Zeitrahmen hängen vom Zweck der App und von der Relevanz der Daten für den Endnutzer ab. Eine Kalender- oder Tagebuch-App oder eine App zum Tauschen von Fotos würde beispielsweise die Wahl der Speicherfrist dem Endnutzer überlassen, während es für eine Navigations-App ausreichen kann, nur die letzten zehn besuchten Standorte zu speichern. App-Entwickler sollten auch Überlegungen zu den Daten von Nutzern anstellen, die die App längere Zeit nicht verwendet haben. Diese Nutzer könnten ihr mobiles Endgerät verloren haben oder zu einem anderen Endgerät gewechselt haben, ohne auf dem ursprünglichen Gerät alle Apps aktiv zu deinstallieren. App-Entwickler sollten daher im Voraus einen Zeitraum der Inaktivität festlegen, nach dessen Ablauf das Konto als erloschen behandelt wird, und sicherstellen, dass der Nutzer über diesen Zeitraum unterrichtet wird. Bei Ablauf dieses Zeitraums sollte der für die Verarbeitung Verantwortliche dem Nutzer einen Warnhinweis senden und ihm die Möglichkeit geben, personenbezogene Daten abzurufen. Wenn der Nutzer auf den Warnhinweis nicht reagiert, sollten die den Nutzer und die App-Nutzung betreffenden personenbezogenen Daten unwiderruflich anonymisiert oder gelöscht werden. Die Erinnerungsfrist hängt vom Zweck der App und dem Standort der gespeicherten Daten ab. Wenn Daten betroffen sind, die auf dem Gerät selbst gespeichert sind (z. B. die Höchstpunktzahl bei einem Spiel), können die Daten aufbewahrt werden, solange die App installiert ist. Wenn Daten betroffen sind, die nur einmal im Jahr verwendet werden (z. B. Informationen über ein Skigebiet), könnte die Erinnerungsfrist bei 15 Monaten liegen.

3.10 Kinder

Kinder sind begeisterte App-Nutzer, entweder auf eigenen oder auf gemeinsam genutzten Endgeräten (z. B. den Geräten ihrer Eltern oder Geschwister oder in Bildungseinrichtungen), und es gibt offensichtlich einen großen und vielseitigen Markt für Apps, die auf Kinder ausgerichtet sind. Gleichzeitig haben Kinder jedoch nur ein geringes oder keinerlei Verständnis und Wissen in Bezug auf den Umfang und die Sensibilität der Daten, auf die Apps zugreifen können, oder den Umfang der Weitergabe von Daten an Dritte zu Werbezwecken.

---

[46] Im Zusammenhang mit sämtlichen Diensten der Informationsgesellschaft (u. a. mit Apps) erinnert die Datenschutzgruppe daran, dass die europäische Verpflichtung zur Vorratsspeicherung von Daten (Richtlinie 2006/24/EG) für diese Dienste nicht gilt und daher nicht als Rechtsgrundlage für die fortgesetzte Verarbeitung von Daten über App-Nutzer herangezogen werden kann, nachdem diese Nutzer die App gelöscht haben. Die Datenschutzgruppe nutzt diese Gelegenheit, um zu betonen, dass Verkehrsdaten besonders risikobehaftet sind und als solche spezielle Vorsichts- und Sicherheitsmaßnahmen erfordern. Dies wurde bereits im Bericht der Datenschutzgruppe über die Durchsetzung der Richtlinie über die Vorratsspeicherung von Daten (WP172) unterstrichen, in dem alle relevanten Beteiligten aufgefordert wurden, angemessene Sicherheitsmaßnahmen durchzuführen.

Die Datenschutzgruppe hat die Thematik der Verarbeitung von Daten von Kindern in der Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern behandelt und geht in diesem Abschnitt nur auf einige appspezifische Risiken und Empfehlungen ein.[47]

App-Entwickler und andere für die Verarbeitung Verantwortliche sollten die Altersgrenzen für die Definition von Kindern und Minderjährigen in den nationalen Rechtsvorschriften beachten, bei denen die Einwilligung der Eltern für die Datenverarbeitung eine Voraussetzung für die rechtmäßige Datenverarbeitung durch Apps ist.[48]

Wenn die Einwilligung rechtmäßig von einem Minderjährigen eingeholt werden kann und die App für die Nutzung durch ein Kind oder einen Minderjährigen bestimmt ist, sollte der für die Verarbeitung Verantwortliche beachten, dass ein Minderjähriger die Bedeutung der Datenverarbeitung vielleicht nur eingeschränkt erfasst und nur in beschränktem Umfang entsprechend sensibilisiert ist. Aufgrund der allgemeinen Schutzbedürftigkeit von Kindern und unter Berücksichtigung der Tatsache, dass personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen, sollten für die Verarbeitung Verantwortliche, die Kinder als Zielgruppe ansprechen, die Grundsätze der Datenminimierung und der Zweckbindung besonders strikt beachten. Konkret sollten für die Verarbeitung Verantwortliche Daten von Kindern weder direkt noch indirekt für Zwecke der Werbung auf Basis von Behavioural Targeting verarbeiten, da dies über das Verständnis eines Kindes hinausgehen und damit die Grenzen der rechtmäßigen Verarbeitung überschreiten würde.

Die Datenschutzgruppe teilt die Bedenken, die die FTC in ihrem Bericht über mobile Apps für Kinder zum Ausdruck gebracht hat.[49]

App-Entwickler sollten in Zusammenarbeit mit App-Stores und Herstellern von Betriebssystemen und Endgeräten die relevanten Informationen auf einfache Weise und in altersgerechter Sprache bereitstellen. Die für die Verarbeitung Verantwortlichen sollten konkret auch jegliche Erfassung von Daten unterlassen, die die Eltern oder Familienmitglieder des minderjährigen Nutzers betreffen, zum Beispiel Finanzinformationen oder Informationen zu speziellen Datenkategorien (etwa medizinische Daten).

4 Schlussfolgerungen und Empfehlungen

Zahlreiche auf einem intelligenten mobilen Endgerät verfügbare Daten sind personenbezogene Daten. Der geltende Rechtsrahmen in diesem Bereich besteht in der Datenschutzrichtlinie in Verbindung mit der spezifischen Einwilligungsanforderung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation. Diese

---

[47] Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen) (WP 160, 11. Februar 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_de.pdf.

[48] In den EU-Mitgliedstaaten liegt diese Altergrenze zwischen 12 und 18 Jahren.

[49] FTC-Bericht *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Februar 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf: „*Die FTC hat ein vielseitiges Spektrum von Apps für Kinder ermittelt, die von Hunderten verschiedener Entwickler erstellt wurden. Auf den App-Vertriebsplattformen hat sie Informationen über die Praktiken zur Verarbeitung und Weitergabe von Daten durch diese Apps jedoch allenfalls in geringem Umfang gefunden.*“

Vorschriften gelten unabhängig vom Standort des App-Entwicklers oder des App-Store für jede App, die an App-Nutzer in der EU vertrieben wird.

Die Fragmentierung des App-Ökosystems, das breite Spektrum technischer Möglichkeiten für den Zugriff auf Daten, die auf mobilen Endgeräten gespeichert sind oder von diesen erstellt werden, und die mangelnde Kenntnis der einschlägigen Rechtsvorschriften unter den Entwicklern führen zu einer Reihe ernsthafter Datenschutzrisiken für App-Nutzer. Diese Risiken reichen von einer mangelnden Transparenz und einem fehlenden Problembewusstsein der App-Nutzer bis hin zu unzureichenden Sicherheitsmaßnahmen, ungültigen Einwilligungsmechanismen, der Tendenz zur Datenmaximierung und einer ungenauen Festlegung der Verarbeitungszwecke.

Zwischen den Datenschutzverpflichtungen der verschiedenen an der Entwicklung, der Verbreitung und der Konzeption der technischen Möglichkeiten von Apps beteiligten Parteien bestehen Überschneidungen. Die meisten Schlussfolgerungen und Empfehlungen sind an App-Entwickler gerichtet (da die Entwickler am stärksten Einfluss darauf haben, wie die Verarbeitung erfolgt und wie Informationen in einer App dargestellt werden). Um die höchsten Standards für den Datenschutz und den Schutz der Privatsphäre zu erreichen, müssen die App-Entwickler jedoch häufig mit anderen Akteuren im App-Ökosystem zusammenarbeiten, z. B. mit den Herstellern von Betriebssystemen und Endgeräten, den App-Stores und Dritten wie z. B. Analysedienstleistern und Online-Werbenetzen.

App-Entwickler müssen

- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Verarbeitung der Daten von Nutzern und über Nutzer kennen und erfüllen;
- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Vertragsschließung mit Auftragsverarbeitern kennen und erfüllen (beispielsweise wenn sie die Erfassung und Verarbeitung personenbezogener Daten extern an Entwickler, Programmierer oder beispielsweise Cloud-Speicheranbieter vergeben);
- eine Einwilligung einholen, bevor die App beginnt, Informationen vom Endgerät zu lesen oder auf dem Gerät zu speichern (d. h. vor Installation der App). Eine solche Einwilligung muss ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erteilt werden;
- eine differenzierte Einwilligung für jede Datenart einholen, auf die die App zugreift – zumindest für die Kategorien Standort, Kontakte, eindeutige Gerätekennung, Identität der betroffenen Person, Identität des Telefons, Kreditkarten- und Zahlungsdaten, Telefonie und SMS, Browserverlauf, E-Mail, Authentifizierungsdaten für soziale Netzwerke und biometrische Daten;
- sich bewusst sein, dass eine Einwilligung keine übermäßige oder unverhältnismäßige Datenverarbeitung legitimiert;
- vor der Installation der App genau festgelegte und verständlich formulierte Zwecke für die Datenverarbeitung bereitstellen und dürfen diese Zwecke nicht ohne eine erneute Einwilligung ändern; sie umfassende Informationen bereitstellen, wenn die Daten für die Zwecke Dritter, z. B. Werbung oder Analyse, verwendet werden;
- den Nutzern ermöglichen, ihre Einwilligung zu widerrufen und die App zu deinstallieren und gegebenenfalls Daten löschen;
- den Grundsatz der Datenminimierung beachten, d. h., sie dürfen nur die Daten erfassen, die für die Durchführung der gewünschten Funktion unbedingt erforderlich sind;
- in allen Phasen der Konzeption und der Implementierung der App die erforderlichen organisatorischen und technischen Maßnahmen ergreifen, um den Schutz der von ihnen

verarbeiteten personenbezogenen Daten zu gewährleisten (siehe Abschnitt 3.6 dieser Stellungnahme (Privacy by Design));
- einen einzigen Ansprechpartner für die App-Nutzer benennen;
- eine lesbare, verständliche und leicht zugängliche Datenschutzerklärung bereitstellen, die die Nutzer zumindest darüber informiert,
  - wer sie sind (Identität und Kontaktdaten),
  - welche genauen Kategorien personenbezogener Daten die App erfassen und verarbeiten soll,
  - warum diese Verarbeitung erforderlich ist (genaue Zwecke),
  - ob die Daten an Dritte weitergegeben werden (nicht nur eine allgemeine Erklärung, sondern eine spezifische Beschreibung, an wen die Daten weitergegeben werden),
  - welche Rechte die Nutzer in Bezug auf den Widerruf der Einwilligung und die Löschung von Daten haben;
- den Nutzern ermöglichen, ihre Rechte auf Auskunft, Berichtigung und Löschung sowie das Recht auf Widerspruch gegen die Datenverarbeitung auszuüben, und die Nutzer über die entsprechenden Mechanismen informieren;
- eine angemessene Speicherfrist für die mit der App erfassten Daten festlegen und von vornherein einen Zeitraum der Inaktivität festlegen, nach dessen Ablauf das Konto als erloschen behandelt wird;
- in Bezug auf für Kinder bestimmte Apps die Altersgrenzen für die Definition von Kindern und Minderjährigen in den jeweils geltenden nationalen Rechtsvorschriften beachten; sie müssen unter strikter Beachtung der Grundsätze der Datenminimierung und der Zweckbindung den am stärksten eingeschränkten Ansatz für die Datenverarbeitung wählen. Die Daten von Kindern dürfen sie weder direkt noch indirekt für Zwecke der Werbung auf Basis von Behavioural Targeting verarbeiten; außerdem dürfen sie über die Kinder keine Daten über deren Verwandten und/oder Freunde erfassen.

Die Datenschutzgruppe empfiehlt, dass App-Entwickler

- die einschlägigen Leitlinien in Bezug auf spezifische Sicherheitsrisiken und -maßnahmen sorgfältig prüfen;
- die Nutzer gemäß den Anforderungen der Datenschutzrichtlinie für elektronische Kommunikation proaktiv über Verletzungen des Schutzes personenbezogener Daten informieren;
- die Nutzer über ihre Überlegungen hinsichtlich der Verhältnismäßigkeit der Daten, die auf dem betreffenden Gerät erfasst werden oder auf die zugegriffen wird, sowie über die Speicherfristen für die Daten und die durchgeführten Sicherheitsmaßnahmen unterrichten;
- Werkzeuge entwickeln, mit denen die Nutzer die Speicherfristen für ihre personenbezogenen Daten anhand ihrer spezifischen Präferenzen und Umstände anpassen können, anstatt vordefinierte Speicherfristen vorzugeben;
- in ihren für europäische Nutzer bestimmten Datenschutzerklärungen relevante Informationen angeben;
- einfache, aber sichere Online-Auskunftswerkzeuge ohne eine zusätzliche übermäßige Erfassung personenbezogener Daten konzipieren und implementieren;

- gemeinsam mit den Herstellern von Betriebssystemen und Endgeräten ihre Kreativität für die Bereitstellung innovativer Lösungen für die angemessene Unterrichtung von Nutzern mobiler Endgeräte nutzen, beispielsweise durch ein System von Mehrebenen-Informationshinweisen kombiniert mit aussagekräftigen Symbolen.

App-Stores müssen

- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Verarbeitung der Daten von Nutzern und über Nutzer kennen und erfüllen;
- die Informationspflichten der App-Entwickler durchsetzen (u. a. die Unterrichtung der Nutzer über die Arten von Daten, auf die die App zugreifen kann, über die Zwecke dieses Datenzugriffs und darüber, ob die Daten an Dritte weitergegeben werden);
- besondere Aufmerksamkeit auf Apps für Kinder verwenden, um eine unrechtmäßige Verarbeitung der Daten von Kindern zu verhindern, und insbesondere die Verpflichtung durchsetzen, die relevanten Informationen auf einfache Weise und in altersgerechter Sprache bereitzustellen;
- ausführliche Informationen über die tatsächlich durchgeführten Kontrollen neu aufgenommener Apps bereitstellen, einschließlich der Kontrollen zur Bewertung in Bezug auf den Datenschutz und den Schutz der Privatsphäre.

Die Datenschutzgruppe empfiehlt, dass App-Stores

- in Zusammenarbeit mit den Herstellern von Betriebssystemen für die Nutzer Instrumente zur Kontrolle ihrer Daten entwickeln, zum Beispiel Symbole zur Darstellung des Zugriffs auf Daten, die sich auf dem mobilen Endgerät befinden oder vom Gerät erstellt werden;
- die Bewertung aller Apps in einem öffentlichen Reputationsmechanismus ermöglichen;
- einen datenschutzfreundlichen Mechanismus für eine Fern-Deinstallation einführen;
- den Nutzern Möglichkeiten für die Äußerung von Rückmeldungen bereitstellen, damit diese Datenschutz- und/oder Sicherheitsprobleme melden können;
- in Zusammenarbeit mit den App-Entwicklern die Nutzer proaktiv über Verletzungen des Schutzes personenbezogener Daten informieren;
- die App-Entwickler auf die Besonderheiten des europäischen Rechts hinweisen, bevor eine App in Europa angeboten wird, zum Beispiel auf die Einwilligungsanforderung und gegebenenfalls auf die Regelung der Übermittlung personenbezogener Daten in Nicht-EU-Länder.

Hersteller von Betriebssystemen und Endgeräten müssen

- ihre Programmierschnittstellen, Regeln für App-Stores und Benutzeroberflächen aktualisieren, um den Nutzern eine ausreichende Kontrolle zu ermöglichen, damit diese eine gültige Einwilligung für die von Apps verarbeiteten Daten erteilen können;
- in ihren Betriebssystemen Mechanismen für die Einholung einer Einwilligung beim ersten Start der App oder beim ersten Zugriff der App auf eine der Datenkategorien mit wesentlichen Datenschutzauswirkungen implementieren;
- die Grundsätze des eingebauten Datenschutzes (Privacy by Design) beachten, um eine heimliche Überwachung der Nutzer zu verhindern;
- eine sichere Datenverarbeitung gewährleisten;
- sicherstellen, dass vorinstallierte Apps bzw. deren Standardeinstellungen dem europäischen Datenschutzrecht entsprechen;

- einen differenzierten Zugriff auf Daten, Sensoren und Dienstleistungen ermöglichen, um sicherzustellen, dass die App-Entwickler nur auf die Daten zugreifen können, die für ihre Apps tatsächlich erforderlich sind;
- anwenderfreundliche und wirksame Mittel bereitstellen, mit denen die Nutzer ein Tracking durch Werbetreibende oder sonstige Dritte verhindern können. Die Standardeinstellungen müssen jegliches Tracking ausschließen;
- die Verfügbarkeit angemessener Mechanismen zur Aufklärung der Endnutzer darüber gewährleisten, was Apps tun können und auf welche Daten sie Zugriff haben;
- sicherstellen, dass bei der Unterrichtung der Endnutzer vor der Installation der App alle Datenkategorien, auf die zugegriffen wird, klar und verständlich genannt werden;
- eine sicherheitsfördernde Umgebung einführen und Hilfsmittel verwenden, die eine Verbreitung bösartiger Apps verhindern und eine einfache Installation/Deinstallation einzelner Funktionen ermöglichen.

Die Datenschutzgruppe empfiehlt, dass die Hersteller von Betriebssystemen und Endgeräten

- den Nutzern ermöglichen, Apps zu deinstallieren, und eine Meldung an den App-Entwickler senden (z. B. über die Programmierschnittstelle), um die Löschung der entsprechenden Nutzerdaten zu ermöglichen;
- systematisch regelmäßige Sicherheitsaktualisierungen anbieten und die Nutzer bei ihrer Anwendung unterstützen;
- sicherstellen, dass die Methoden und Funktionen für den Zugriff auf personenbezogene Daten Funktionen beinhalten, die auf die Implementierung differenzierter Einwilligungsanfragen abzielen;
- aktiv zur Entwicklung von Symbolen beitragen, mit denen die Nutzer auf die verschiedenen Datenverwendungen durch Apps hingewiesen werden, und die Einführung dieser Symbole unterstützen;
- klare Prüfpfade für die Geräte entwickeln, damit die Endnutzer klar sehen können, welche Apps auf Daten auf ihren Geräten zugegriffen haben, und damit die Endnutzer Informationen über die ausgehende Datenverkehrsmenge pro App im Verhältnis zum nutzerinitiierten Datenverkehr erhalten können.

Dritte müssen

- ihre Verpflichtungen als für die Verarbeitung Verantwortliche bei der Verarbeitung personenbezogener Daten über Nutzer kennen und erfüllen;
- in Zusammenarbeit mit den App-Entwicklern und/oder App-Stores beim Lesen oder Schreiben von Daten auf mobilen Endgeräten die in Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation vorgeschriebene Einwilligungsanforderung erfüllen; App-Entwickler und/oder App-Stores haben dabei die wichtige Aufgabe, die Nutzer über die Zwecke der Datenverarbeitung zu informieren;

- dafür sorgen, dass keine Mechanismen zur Verhinderung von Tracking umgangen werden (wie derzeit häufig bei in Browsern implementierten „Do Not Track“-Mechanismen der Fall);

- soweit sie als Kommunikationsdienstleister Markengeräte verbreiten, eine gültige Einwilligung der Nutzer für vorinstallierte Apps sicherstellen und die entsprechende Verantwortung übernehmen, wenn sie an der Festlegung bestimmter Funktionen des

Endgeräts und des Betriebssystems beteiligt sind; dazu können sie beispielsweise den Zugriff der Nutzer auf bestimmte Konfigurationsparameter beschränken oder (sicherheits- und funktionsbezogene) Aktualisierungen der Hersteller der Endgeräte oder der Betriebssysteme filtern;

- soweit sie als Werbetreibende tätig sind, ausdrücklich davon absehen, Werbung außerhalb der App einzublenden. Beispiele sind die Einblendung von Werbung durch Modifizierung der Browsereinstellungen oder die Platzierung von Symbolen auf dem Desktop des mobilen Endgeräts. Sie dürfen eindeutige Geräte- oder Teilnehmerkennungen nicht zum Zwecke des Tracking verwenden;
- dafür sorgen, dass die Daten von Kindern weder direkt noch indirekt für Zwecke der Werbung auf Basis von Behavioural Targeting verarbeitet werden. Sie müssen angemessene Sicherheitsmaßnahmen durchführen. Dazu gehören die sichere Übertragung und die verschlüsselte Speicherung von eindeutigen Gerätekennungen und Kennungen der App-Nutzer sowie sonstigen personenbezogenen Daten.

Die Datenschutzgruppe empfiehlt, dass Dritte

- einfache, aber sichere Online-Auskunftswerkzeuge ohne eine zusätzliche übermäßige Erfassung personenbezogener Daten konzipieren und implementieren und
- nur die Daten erfassen und verarbeiten, die sich tatsächlich auf den Kontext beziehen, in dem die Nutzer diese Daten bereitstellen.