

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Dr. Alexander Golland

Die Meisterschaft des FC Schalke 04

Seite 1

Stichwort des Monats

Kevin Leibold

Führt ein DSGVO-Verstoß zur Nichtigkeit eines Vertrages?

Seite 2

Datenschutz im Fokus

Dr. Thomas Schwenke

Direktmarketing: Zulässigkeit der Messung von Öffnungs- und Klickraten sowie der Bildung von Empfängerprofilen

Seite 7

Philipp Quiel

Rechtfertigung von Datenübermittlungen im Zusammenhang mit dem Einsatz von Cookies

Seite 12

Markus Schröder

„Sale of Data“ nach dem California Consumer Privacy Act

Seite 15

Björn Früh und Josua Neudeck

App Privacy Labels – Wie gehe ich als App-Anbieter mit Apples „Nährwerttabelle“ um?

Seite 18

Aktuelles aus den Aufsichtsbehörden

Kristof Kamm

Videokonferenzen – im Spagat zwischen betrieblicher Notwendigkeit und aufsichtsbehördlicher Einhegung

Seite 23

Rechtsprechung

Jana Gooth und Theresia Rasche

OLG München erklärt Klarnamenpflicht von Facebook für zulässig – eine Kritik an den Urteilsgründen

Seite 27

▪ Nachrichten Seite 5 ▪ Service Seite 32

Björn Früh und Josua Neudeck

App Privacy Labels – Wie gehe ich als App-Anbieter mit Apples „Nährwerttabelle“ um?

Apple zwingt seit Dezember 2020 Anbieter im App Store zur Anzeige von „App Privacy Labels“ und baut damit ihr „Soft Law“ als zusätzliche Compliance-Anforderung weiter aus. App-Anbieter sollten sich mit der vorgegebenen Struktur der App Privacy Labels sowie den verwendeten Begrifflichkeiten vertraut machen und auf eine saubere Verzahnung mit den gesetzlich geforderten Datenschutzinformationen nach DSGVO und TMG achten. Perspektivisch sind die App Privacy Labels nur ein Vorgeschmack auf weitere Datenschutzvorgaben, die Apple Entwicklern im Jahr 2021 machen wird.

Hintergrund

Datenschutz-„Nährwerttabellen“ sind seit Dezember 2020 Voraussetzung für jede Einreichung einer neuen App sowie von Updates einer bestehenden App in Apples hauseigenem App Store. Sie sind Teil einer größeren Datenschutzoffensive, zu der auch die Bemühungen um eine einheitliche Opt-in-Lösung für die bislang standardmäßig aktivierte Apple Werbe-ID (die sog. Identifier for Advertisers, IDFA) gehören. Nach Protest aus der AdTech-Branche um Facebook & Co. wurde die Opt-in-Pflicht vorerst auf Frühjahr 2021 verschoben. Über die Privacy Labels müssen Nutzer bereits jetzt vor dem Download auf der jeweiligen Produktseite im Apple App Store in Kurzform durch Bildsymbole und Stichworte über die Datenverarbeitung in der jeweiligen App aufgeklärt werden.

In der Praxis bedeutet der Vorstoß von Apple für verantwortliche App-Anbieter vor allem eins: Neben Datenschutzhinweisen und Consent-Bannern nach DSGVO und TMG kommen weitere Compliance-Anforderungen durch Apples „Soft Law“ hinzu. Der nachfolgende Beitrag zeigt auf, wie der Einstieg in die Privacy Labels für App-Anbieter gelingt und welche Risiken bei der Beantwortung von Apples Fragenkatalog bestehen.

Was müssen App-Anbieter wissen?

Apple sieht für die Erstellung der Privacy Labels einen geführten Erfassungsprozess im Online-Entwicklerbereich des App Stores („App Store Connect“) vor, der sich grob in vier Schritte unterteilen lässt: 1. Datentypen, 2. Verarbeitungszwecke, 3. Verknüpfung mit Nutzeridentität, 4. Tracking (Einzelheiten siehe unten). Diese Angaben sind nicht nur faktische Voraussetzung zur Einreichung einer jeden App auf der App Store-Plattform, sondern auch in Apples „Soft Law“ (bestehend aus Vertragsbedingungen, Policies und Review Guidelines) eingebettet. App-Anbieter sind nach den Review Guidelines dafür verantwortlich, dass die Angaben korrekt und auf dem neuesten Stand sind. Die Erklärungen der App-Anbieter zu den Privacy Labels sind im Vertragsverhältnis zu Apple damit verbindlich und Apple behält sich vor,

Verstöße zu ahnden. Apple kann Falschangaben durch die Einblicke als Plattformbetreiber dabei leicht nachvollziehen.

Als Hilfestellung zur Beantwortung der Fragelisten in App Store Connect stellt Apple Definitionen und Beispiele zur Verfügung, unter anderem zu den Datentypen, den Verarbeitungszwecken oder dem Begriff des Trackings. Die recht starren Vorgaben und Abfragen von Apple zu den Privacy Labels sind meist nur mit „Ja“ oder „Nein“ zu beantworten oder bieten nur die Möglichkeit, vorgegebene Antworten auszuwählen. Dies kann zu Unschärfen, Zuordnungsschwierigkeiten oder gar Widersprüchen führen. Freitextfelder oder weitergehende Konfigurationsmöglichkeiten, welche eine Konkretisierung der Privacy Labels ermöglichen würden, sind nicht vorgesehen.

Die von den App-Anbietern gemachten Angaben werden von Apple kategorisiert und dem Nutzer grafisch in drei Bereichen angezeigt: „Daten, die zum Tracking der Person verwendet werden“, „mit dem Nutzer verknüpfte Daten“ sowie „nicht verknüpfte Daten“.

Die Privacy Labels sind kein Ersatz für Datenschutzhinweise nach Art. 13, 14 DSGVO und stellen auch keine Einwilligungserklärung dar. Zur Vermeidung von Missverständnissen sei auch klargestellt, dass es sich hierbei nicht um standardisierte Bildsymbole im Sinne von Art. 12 Abs. 7 DSGVO handelt. Privacy Labels sind aber in aller Regel das erste und manchmal auch das letzte „piece of information“ zum Datenschutz, das der Nutzer zur Kenntnis nimmt. Ihnen kommt also im Hinblick auf die Transparenz der Datenverarbeitung und der vernünftigen Erwartungen der betroffenen Personen (vgl. ErwGr. 47 zur DSGVO) eine besondere Bedeutung zu. Werden Nutzer bereits auf dieser Ebene transparent informiert, kann sich dies beispielsweise positiv darauf auswirken, ob im Rahmen einer Interessenabwägung eine hiermit verfolgte Datenverarbeitung auf die Rechtsgrundlage der berechtigten Interessen gestützt werden kann (siehe zur Methodik instruktiv auch Herbrich, DSB 2020, 146 ff.).

Welche Fragen müssen App-Anbieter beantworten?




App-Anbieter müssen angeben, ob und welche Daten sie oder ihre Drittanbieter-Partner („third-party partners“) wie z. B. Analytics-Tools, Werbenetzwerke oder SDK-Anbieter erfassen, wie sie diese nutzen, ob eine Verknüpfung mit dem Nutzer besteht sowie ob die App-Nutzer hierdurch getrackt werden.

Apples Definition von „Erfassen“ („collect“) ist zwar enger als die weite gesetzliche Definition der Verarbeitung in Art. 4 Nr. 2 DSGVO und versucht darüber hinaus Grenzfälle der nur „flüchtigen“ Verarbeitung auszunehmen. Um Wertungswidersprüche und Intransparenz zu vermeiden, sind App-Anbieter jedoch gut beraten, grundsätzlich alle Vorgänge in der App, die der gesetzlichen Definition einer Datenverarbeitung entsprechen, im Rahmen der Privacy Labels offenzulegen.

In vier Schritten fragt Apple konkret die nachfolgenden Angaben ab (vgl. <https://developer.apple.com/app-store/app-privacy-details/>):

Datentypen

Datentyp	Auswählbare Datenkategorien/ Beispiele von Apple
 Kontaktinformationen	Name, E-Mail-Adresse, Telefonnummer, physische Adresse sowie sonstige Kontaktinformationen des Benutzers
 Gesundheit und Fitness	Gesundheitsdaten und Fitnessdaten
 Finanzinformationen	Zahlungsdaten, Bonitätsinformationen sowie sonstige Finanzinformationen
 Standort	genauer sowie ungefährer Standort
 Vertrauliche Daten	z. B. Daten zur ethnischen Herkunft, Informationen über die sexuelle Orientierung, Schwangerschaft oder Geburt u. a.
 Kontakte	z. B. Adressbuch, Kontaktliste, soziales Diagramm
 Benutzerinhalte	E-Mails und Textnachrichten, Fotos, Videos, Audiodaten, Gameplay-Inhalte, Supportanfragen, sonstige vom Nutzer generierte Inhalte
 Browserverläufe	Inhalte, die nicht Teil der App sind wie z. B. Webseitensuchverläufe
 Suchverlauf	mit der App durchgeführte Suchen
 Kennungen	User-ID, Geräte-ID
 Kaufhistorie	z. B. Käufe und Kauf Tendenzen

 Nutzungsdaten	Produktinteraktionen, Werbedaten sowie sonstige Nutzungsdaten
 Diagnose	Absturzprotokolle, Leistungsdaten sowie sonstige Diagnosedaten
 Sonstige Daten	andere, nicht aufgeführte Datentypen

Zu jedem Datentyp (linke Spalte) hat der App-Anbieter weitere genauere Datenkategorien (rechte Spalte) anzukreuzen. Möglichkeiten für Freitext gibt es hier nicht.

Verarbeitungszwecke

Zweck	Definitionen/Beispiele von Apple
Drittanbieter-Werbung	das Anzeigen von Drittanbieter-Werbung in der App oder das Weitergeben von Daten an Partner, die Drittanbieter-Anzeigen schalten
Werbung oder Marketing des Entwicklers	die Anzeige von Werbung des App-Betreibers, das direkte Senden von Marketing oder die Weitergabe von Daten an Unternehmen, die Werbung anzeigen
Analyse	Verwendung von Daten zur Auswertung des Benutzerverhaltens, z. B. um die Effektivität bestehender Produktfunktionen zu verstehen, neue Funktionen zu planen oder die Größe oder Eigenschaften der Zielgruppe zu messen
Produktpersonalisierung	Anpassen von Inhalten, die der Benutzer sieht, z. B. eine Liste mit empfohlenen Produkten, Beiträgen oder Vorschlägen
App-Funktionalität	Authentifizierung des Benutzers, Aktivierung von Funktionen, Verhinderung von Betrug, Implementierung von Sicherheitsmaßnahmen, Sicherstellung der Serverbetriebszeit, Minimierung von App-Abstürzen, Verbesserung der Skalierbarkeit und Leistung sowie Durchführung des Kundensupports
Sonstige Zwecke	jede andere, nicht aufgeführte Nutzung

Insbesondere die Datentypen „Gesundheit und Fitness“, „Vertrauliche Daten“ und „Nutzungsdaten“ sowie die Zwecke, die (Drittanbieter-)Werbung, Marketing oder Analyse betreffen, sind starke Indikatoren für das Erfordernis einer Einwilligung nach ePrivacy-RL (TMG) bzw. DSGVO. Entsprechende Angaben sollten also mit dem (gegebenenfalls gestuften) Einwilligungsprozedere (siehe dazu auch Moos/Strassemeyer, DSB 2020, 207 ff.) sowie den Darstellungen

in den Datenschutzhinweisen abgeglichen werden, damit es nicht zu Widersprüchen kommt.

Die Beschränkung auf die Verarbeitungskategorien „App-Funktionalität“ und „Produktpersonalisierung“ kann dafür sprechen, dass eine Einwilligung nach TMG bzw. DSGVO verzichtbar ist. Allerdings versteht Apple die Begrifflichkeiten hier recht weit, weshalb auch bei Auswahl dieser Kategorien ein Augenmerk auf die konkrete technische Umsetzung gelegt werden sollte. Der Einsatz nicht unbedingt notwendiger Cookies und ähnlicher Technologien (z. B. auf Basis von Werbe-ID, Vendor-ID, Universally Unique Identifier/UUID) im Sinne der ePrivacy-RL wird in aller Regel einer aktiven Einwilligung nach TMG bedürfen. Im Bereich der bedarfsgerechten Gestaltung im Sinne von § 15 Abs. 3 TMG und bei einzelnen Arten des Trackings, die kein Setzen oder Auslesen von Informationen auf dem Endgerät erfordern (z. B. Device Fingerprinting), kann es weiterhin vereinzelt Spielräume geben (siehe dazu instruktiv Moos/Strassemeyer, DSB 2020, 207, 209 f.).

Verknüpfung mit Nutzeridentität

Für jeden Datentyp fragt Apple ab, ob dieser „mit dem Benutzer verknüpft“ ist. Apple weist darauf hin, dass „von einer App erfasste Daten normalerweise mittels dieser mit der Identität des Benutzers verknüpft werden, es sei denn, vor der Erfassung werden spezifische Datenschutzvorkehrungen getroffen, um sie unkenntlich zu machen oder zu anonymisieren“.

Als Beispiele der „Anonymisierung“ führt Apple die Möglichkeiten an, identifizierende Merkmale (wie z. B. Benutzer-ID oder Name) zu löschen oder Daten so zu „manipulieren“, dass die Verknüpfung mit einer natürlichen Person unterbrochen wird. Außerdem sollen Aktivitäten des App-Anbieters zur „Re-Identifizierung“ ausdrücklich unterbleiben. Dies lässt die hohen Ansprüche der Art.-29-Datenschutzgruppe in ihren Empfehlungen zu Anonymisierungstechniken zumindest anklingen (vgl. Art.-29-Datenschutzgruppe, WP 216, S. 28 ff.). Es spricht daher einiges dafür, dass Apple von einem weiten Verständnis des Begriffs der „Verknüpfung mit der Nutzeridentität“ ausgeht und dem gesetzlichen Konzept des Personenbezugs, wie es Art. 4 Nr. 1 DSGVO statuiert, zumindest nahekommt. Eine Orientierung am Begriff des Personenbezugs aus der DSGVO ergibt sich zudem aus folgendem Hinweis von Apple: „ ‚Persönliche Daten‘ und ‚Personenbezogene Daten‘, wie sie gemäß den relevanten Datenschutzgesetzen definiert sind, werden als ‚mit dem Benutzer verknüpft‘ verstanden.“

Vor diesem Hintergrund dürfte für App-Anbieter der sicherste Weg darin bestehen, immer dann von einer „Verknüpfung mit der Nutzeridentität“ auszugehen, wenn die Daten nicht nach den Anforderungen der DSGVO als anonym(-isiert) gelten.

Tracking

Auf Tracking legt Apple ein besonderes Augenmerk, wobei das Verständnis hier eher eng auf eine werbliche Auswertung abstellt. So heißt es in den Erklärungen zu den Privacy Labels: „Beim Tracking werden von Ihrer App erfasste Daten über einen bestimmten Endbenutzer oder ein bestimmtes Gerät, z. B. eine Benutzer- bzw. Geräte-ID oder ein Profil, mit Daten von Drittanbietern für gezielte Werbung oder Werbemaßnahmen verknüpft.“ Apple nennt insbesondere die Beispiele des Ad Targeting, der Weitergabe an Datenbroker oder an Werbenetzwerke sowie des Einbindens des SDK eines Drittanbieters, das Daten zu Werbezwecken zusammenführt (siehe dazu auch Siebelmann, DSB 2020, 246 ff.). Insbesondere bei Integration des Facebook SDK wird ein Tracking daher stets bejaht werden müssen. Ähnlich dürfte es sich in der Regel auch mit den Google Ad-Diensten sowie dem in der Praxis häufig anzutreffenden Google Firebase Framework verhalten, wobei insbesondere bei Letzterem je nach dem genutzten Funktionsumfang im Einzelfall Spielräume bestehen können.

Beanstandungsrisiken

Hinsichtlich der Risiken und Folgen von Falschangaben in den Privacy Labels lässt sich zwischen der Compliance mit dem „Soft Law“ von Apple einerseits sowie den „harten“ gesetzlichen Verpflichtungen andererseits unterscheiden.

Werden falsche oder unzureichende Angaben gemacht, kann Apple diesen Vertragsverstoß sanktionieren. Dies kann für den App-Anbieter eine Ablehnung des konkreten App-Releases (im besten Fall mit Chance zur Nachbesserung) oder einen vorübergehenden oder dauerhaften Ausschluss aus dem App Store zur Folge haben. Dass Apple durchaus „Zähne zeigt“ bei der Durchsetzung ihrer App Store-Richtlinien, haben in der Vergangenheit nicht nur kleinere Entwickler, sondern zuletzt auch Branchengrößen wie Epic Games (der Anbieter von Fortnite) zu spüren bekommen. Wie das Enforcement von Apple konkret in Sachen Datenschutz aussehen wird, ist noch offen: Vorerst rechnet die Entwickler-Community auch wegen der kurzen Vorankündigungsfrist von wenigen Wochen wohl noch mit einer gewissen Schonfrist. Andererseits ist nicht zu vergessen, dass Apple im Rahmen des standardmäßigen App Review-Prozesses ausreichende Einblicke in die App(-Architektur), SDK-/API-Verknüpfungen sowie den Datenverkehr erhält. Vor allem Falschangaben hinsichtlich der Einbindung von sog. SDK (Software Development Kit) von Drittanbietern oder sonstigen Drittdiensten sind unschwer von Apple festzustellen.

Inkonsistenzen oder Widersprüche der jeweiligen Angaben in den Privacy Labels einerseits sowie den Datenschutzhinweisen und Einwilligungserklärungen andererseits können zu Intransparenz führen und im schlimmsten

Fall Beanstandungen von Aufsichtsbehörden nach sich ziehen. Diverse Landesdatenschutzbeauftragte in Deutschland haben für 2021 angekündigt, Apps und die darin implementierten Tracking-Technologien näher unter die Lupe nehmen zu wollen. Auch in Auseinandersetzungen mit verärgerten Nutzern können Widersprüche zwischen den einzelnen Dokumenten zum Stein des Anstoßes werden, etwa wenn Betroffene diese zum Anlass nehmen, ihre Rechte nach Art. 15 ff. DSGVO geltend zu machen. Praktisch dürfte dies vor allem Fälle betreffen, in denen der App-Anbieter Verarbeitungen fälschlicherweise als „nicht mit dem Nutzer verknüpft“ deklariert oder diese gar nicht in den Privacy Labels ausweist.

Praxisempfehlungen

Sorgsame Prüfung der Apple-Anforderungen für jede App mit ihren konkreten Besonderheiten:

Hier sollten sich das Datenschutz-Team und das Entwickler-Team möglichst eng abstimmen, um ein gemeinsames Verständnis für Datenkategorien und Zwecke zu schaffen. Die Bereitstellung der Privacy Labels an Apple kann darüber hinaus als Gelegenheit dienen, die Software auf bisher vernachlässigten „third-party source code“ hin durchzusehen, der z. B. bisher nicht angegebene Tracker enthält. Apple weist darauf hin, dass Angaben nicht nur die Ebene der App selbst betreffen, sondern auch die Praktiken über alle Plattformen (z. B. den Google Play Store oder die eigene Webpräsenz) hinweg wiedergeben sollen.

Abgleich mit Datenschutzhinweisen und Einwilligungserklärungen:

Die Angaben in den unterschiedlichen Rechtstexten sollten sauber ineinandergreifen. Die aufgrund der starren Auswahlmöglichkeiten teils unscharfen Angaben in den Privacy Labels sollten bei Bedarf in den App-Datenschutzhinweisen näher erklärt werden. Je nach Struktur des Dokuments kann beispielsweise ein erläuternder und vertiefender Abschnitt zu den Privacy Labels sinnvoll sein. Privacy Labels sollten jedenfalls nicht ungeprüft in die Datenschutzhinweise übernommen werden. Etwaige Widersprüche sind selbstverständlich stets zugunsten gesetzlicher Vorgaben aufzulösen.

Nutzen der Gelegenheit zur Aktualisierung der anderen Datenschutzdokumente in der App:

Die im Vergleich zu den entsprechenden Website-Texten meist etwas stiefmütterlich behandelten Datenschutzhinweise und Einwilligungserklärungen in Apps können „in einem Aufwasch“ auf den aktuellen Stand gebracht werden. Hierbei sollte auch auf eine Verlinkung auf die korrekten App-Datenschutzhinweise auf der Produktseite im App Store geachtet werden. In der Praxis finden sich häufig bloß Verlinkungen auf die allgemeinen Datenschutzhinweise der Website ohne App-spezifische Angaben.

Sensibilisierung für Datenschutz in Apps:

Vor allem in Apples Ökosystem empfiehlt es sich, verstärkt auf Datenschutz zu achten und die eigenen Produkt- bzw. Entwickler-Teams entsprechend zu sensibilisieren. Der typische Apple-Nutzer gilt als deutlich datenschutzaffiner als sein Android-Pendant. Ferner stehen inzwischen nicht nur Aufsichtsbehörden, sondern auch technischen Laien Tools wie etwa „mitmproxy“ zur Verfügung, mit denen der Datenverkehr von Apps unschwer nachvollzogen werden kann. Angaben in Datenschutzhinweisen oder Privacy Labels sind also durchaus auch von Dritten verifizierbar.

Fazit und Ausblick

Unabhängig davon, wie die Nutzer Apples Datenschutz-„Nährwerttabellen“ annehmen werden und ob auch hier ein Abstumpfungseffekt wie bei Online-Consent-Bannern zu beobachten sein wird, sind die Vorgaben von Apples „Soft Law“ jedenfalls als zusätzlicher Faktor der Legal Compliance von Apps zu berücksichtigen. Perspektivisch ist damit zu rechnen, dass sich die Anforderungen im Hinblick auf die Gesamtstrategie des Konzerns beim Thema „Privacy“ dynamisch weiterentwickeln. Bereits im Frühjahr 2021 beabsichtigt Apple, als nächsten Schritt einen eigenen Opt-in-Mechanismus für Tracking einzuführen. Hier wird sich zeigen, inwiefern dieser den gesetzlichen Anforderungen an eine aktive, informierte, bestimmte und freiwillige Einwilligung nach Art. 7 DSGVO genügt (siehe dazu im Einzelnen Moos/Strassemeyer, DSB 2020, 207 ff.) und weitere Consent-Screens entbehrlich machen kann.

Als nationaler gesetzlicher Maßstab mag sich bis dahin dann möglicherweise auch der Entwurf eines „TTDSG“ (Telekommunikations-Telemedien-Datenschutz-Gesetz) konkretisiert haben. Ebenso bleibt abzuwarten, ob Google als Hauptkonkurrentin für ihren Play Store mit ähnlichen Anforderungen in Kürze nachzieht. Unter Umständen verleihen die Privacy Labels auch neuen Schwung in der Debatte um standardisierte Bildsymbole zur Visualisierung der Angaben nach Art. 13 f. DSGVO.

Autoren: Björn Früh, CIPP/E, ist Fachanwalt für IT-Recht bei der auf IP-, IT- und Datenschutzrecht spezialisierten Boutique Vogel & Partner Rechtsanwälte mbB in Stuttgart.



Josua Neudeck ist Rechtsanwalt in der Praxisgruppe IT-Recht und Datenschutz am Karlsruher Standort von Vogel & Partner.

