Richtlinien für Rechtsverfahren

Regierungs- und Strafverfolgungsbehörden außerhalb der USA

Diese Richtlinien werden für den Gebrauch durch Regierungs- und Strafverfolgungsbehörden außerhalb der USA im Falle von Auskunftsersuchen in Bezug auf Benutzer von Geräten, Produkten und Dienstleistungen von Apple gegenüber maßgeblichen Entitäten von Apple, die in der jeweiligen Region bzw. dem jeweiligen Land Dienste anbieten, bereitgestellt. Apple aktualisiert diese Richtlinien nach Bedarf.

In diesen Richtlinien bezeichnet „Apple“ die jeweilige Entität, die für Kunden- bzw. Benutzerdaten in einer bestimmten Region bzw. in einem bestimmten Land verantwortlich ist. Als globales Unternehmen verfügt Apple in verschiedenen Rechtsgebieten über eine Reihe von Rechtsträgern, die verantwortlich sind für die persönlichen Daten, die erfasst und für Apple Inc. verarbeitet werden. Beispielsweise werden Point-of-Sale-Informationen in den Retail-Einrichtungen von Apple außerhalb der USA durch Apples jeweilige Retail-Einrichtungen in jedem Land kontrolliert. Persönliche Daten hinsichtlich des Apple Online Store und iTunes können auch wie in den jeweiligen Servicebedingungen innerhalb eines spezifischen Rechtsgebiets festgelegt durch juristische Personen außerhalb der USA kontrolliert werden. In der Regel tragen juristische Personen von Apple außerhalb der USA in Australien, Kanada, Irland und Japan innerhalb der Gebiete, für die sie verantwortlich sind, Verantwortung für Benutzerdaten im Zusammenhang mit Apple Services.

Alle anderen Auskunftsersuchen in Bezug auf Apple Kunden/Nutzer, einschließlich Fragen von Kunden/Nutzern hinsichtlich der Offenlegung von Informationen, sind an https://www.apple.com/privacy/contact/ zu richten. Diese Richtlinien gelten nicht für Anfragen der US-Regierung und der US-Strafverfolgungsbehörden an Apple Inc.

Im Falle von Auskunftsersuchen seitens Regierungs- bzw. Strafverfolgungsbehörden hält sich Apple an die für internationale Unternehmen einschlägigen Gesetze über die Offenlegung und den Schutz von Daten und legt Informationen entsprechend den gesetzlichen Vorschriften offen. Alle Anfragen von Regierungs- und Strafverfolgungsbehörden außerhalb der USA nach Inhalten müssen den geltenden Gesetzen, einschließlich des US-Gesetzes über den Datenschutz bei elektronischer Kommunikation (United States Electronic Communications Privacy Act, ECPA) entsprechen. Ausnahmen gelten nur bei Notfällen (im Folgenden unter „Notfallanfragen“ definiert). Eine Anfrage im Rahmen eines gegenseitigen Rechtshilfeabkommens mit den Vereinigten Staaten erfolgt in Übereinstimmung mit dem ECPA.

Bei Auskunftsersuchen von privaten Parteien hält Apple sich an die Gesetzgebung in Bezug auf lokale Entitäten, die mit Benutzerdaten umgehen, und stellt die Daten soweit rechtlich erforderlich zur Verfügung.

Apple verwendet einen zentralisierten Prozess für das Empfangen, Nachverfolgen, Verarbeiten und Beantworten von berechtigten rechtlichen Anfragen seitens der Regierung, Strafverfolgungsbehörden und privaten Parteien, der vom Eingang der Anfrage bis zu deren Beantwortung zum Einsatz kommt. Ein geschultes Team unserer Rechtsabteilung prüft und bewertet alle eingegangenen Anfragen. Anfragen, die nach Apples Einschätzung keine gültige rechtliche Grundlage besitzen oder die Apple als unklar, unangemessen oder zu weit gefasst erachtet, werden angefochten oder abgelehnt.

INDEX

I. Allgemeine Informationen

Apple entwickelt, produziert und vertreibt mobile Kommunikations- und Mediengeräte, Computer und tragbare digitale Musikplayer. Außerdem verkauft Apple zugehörige Software, Dienste, Peripheriegeräte, Netzwerklösungen sowie digitale Inhalte und Programme anderer Anbieter. Produkte und Dienste von Apple sind Mac, iPhone, iPad, iPod, Apple TV, Apple Watch, eine Reihe von Softwareprogrammen für Privat- und Geschäftskunden, die Betriebssysteme iOS und Mac OS X, iCloud und verschiedene Zubehör-, Dienstleistungs- und Supportangebote. Apple verkauft und vertreibt außerdem über den iTunes Store, den App Store, den iBooks Store und den Mac App Store digitale Inhalte und Programme. Apple speichert Nutzerinformationen gemäß der Apple Datenschutzrichtlinie und den gültigen Nutzungsbedingungen/Allgemeinen Geschäftsbedingungen für den jeweils angebotenen Dienst. Apple nimmt den Schutz der Privatsphäre der Nutzer von Apple-Produkten und -Diensten („Apple-Nutzer“) ernst. Dementsprechend werden Informationen über Apple-Nutzer nicht ohne korrektes Rechtsverfahren offengelegt.

Die in diesen Richtlinien enthaltenen Informationen richten sich an Regierungs- und Strafverfolgungsbehörden außerhalb der USA und beziehen sich auf das Rechtsverfahren, das Apple benötigt, um elektronische Informationen gegenüber Regierungs- und Strafverfolgungsbehörden außerhalb der USA offenlegen zu können. Diese Richtlinien stellen keine Rechtsberatung dar. Der Abschnitt „Fragen und Antworten“ (FAQ) dieser Richtlinien soll Antworten auf einige der häufigsten Fragen geben, die Apple erhält. Weder diese Richtlinien noch der Abschnitt „Fragen und Antworten“ decken alle Umstände ab, die sich ergeben können.

Wenden Sie sich bei weiteren Fragen bitte an lawenforcement@apple.com.

Die oben genannte E-Mail-Adresse ist ausschließlich zur Verwendung durch Regierungs- und Strafverfolgungsmitarbeiter gedacht. Wenn Sie eine E-Mail an diese Adresse senden, muss dies von einer gültigen und offiziellen E-Mail-Adresse einer Regierungs- oder Strafverfolgungsbehörde aus geschehen.

Bei dem Großteil der bei Apple eingehenden Anfragen von Ermittlungsbehörden handelt es sich um Anfragen nach Informationen zu einem bestimmten Apple Gerät oder Kunden sowie zu den spezifischen Diensten, die Apple diesem Kunden ggf. bereitgestellt hat. Sofern Apple die angefragten Informationen gemäß seinen Datenaufbewahrungsrichtlinien noch besitzt, kann Apple Geräte- oder Kundendaten zur Verfügung stellen. Apple speichert bestimmte Daten wie unter „Verfügbare Informationen“ unten dargestellt. Alle anderen Daten werden für den Zeitraum aufbewahrt, der zur Erfüllung der in unserer Datenschutzrichtlinie aufgeführten Zwecke erforderlich ist. Zur Vermeidung von Missverständnissen und/oder einer Ablehnung infolge unklarer, unangemessener oder zu weit gefasster Anfragen sollten Anfragen von Regierungs- und Strafverfolgungsbehörden möglichst eng gefasst und spezifisch formuliert werden. Alle Anfragen von Regierungs- und Strafverfolgungsbehörden außerhalb der USA nach Inhalten müssen den geltenden Gesetzen, einschließlich des US-Gesetzes über den Datenschutz bei elektronischer Kommunikation (United States Electronic Communications Privacy Act, ECPA) entsprechen. Ausnahmen gelten nur bei Notfällen (im Folgenden unter „Notfallanfragen“ definiert). Eine Anfrage im Rahmen eines gegenseitigen Rechtshilfeabkommens mit den Vereinigten Staaten erfolgt in Übereinstimmung mit dem ECPA.

Keine der hier aufgeführten Richtlinien bildet eine Grundlage für einklagbares Recht gegenüber Apple. Zudem können die Richtlinien von Apple in Zukunft aktualisiert oder verändert werden, ohne dass Regierungs- oder Strafverfolgungsbehörden darüber informiert werden.

II. Rechtliche Anfragen an Apple

A. Auskunftsersuchen von Regierungs- und Strafverfolgungsbehörden

Apple akzeptiert rechtsgültige Auskunftsersuchen von Regierungs- und Strafverfolgungsbehörden per E-Mail, sofern es sich bei der Absenderadresse um die offizielle E-Mail-Adresse der betreffenden Behörde handelt. Regierungs- und Strafverfolgungsmitarbeiter außerhalb der USA, die ein Auskunftsersuchen an Apple richten, müssen eine Vorlage für ein Auskunftsersuchen von Regierungs- und Strafverfolgungsbehörden ausfüllen und diese direkt von ihrer jeweils offiziellen E-Mail-Adresse der Regierungs- bzw. Strafverfolgungsbehörde an die im Folgenden genannte E-Mail-Adresse richten: lawenforcement@apple.com.

Die oben genannte E-Mail-Adresse ist ausschließlich zur Verwendung durch Regierungs- und Strafverfolgungsmitarbeiter gedacht. Wenn Sie eine E-Mail an diese Adresse senden, muss dies von einer gültigen und offiziellen E-Mail-Adresse einer Regierungs- oder Strafverfolgungsbehörde aus geschehen. Wenn die Anfragen mindestens fünf identifizierende Angaben enthalten, z. B. Serien-/IMEI-Nummern von Geräten, Apple-IDs, E-Mail-Adressen oder Rechnungs- bzw. Auftragsnummern, müssen diese in einem editierbaren Format übertragen werden. Solche identifizierenden Angaben sind in der Regel erforderlich, um Informationssuchen im Zusammenhang mit Geräten, Accounts oder Finanztransaktionen durchführen zu können.

Apple erachtet Auskunftsersuchen seitens einer Strafverfolgungsbehörde dann als rechtsgültig, wenn das Ersuchen unter Umständen erfolgt, bei denen eine präzise rechtliche Grundlage im inländischen Recht des anfragenden Landes gegeben ist und es sich auf im guten Glauben erfolgende Verhinderung, Aufdeckung oder Ermittlung von Rechtsverstößen bezieht. Beispiele für Anfragen, die Apple für rechtsgültig erachtet und international erhält, sind: Production Orders (Australien, Kanada), Tribunal Orders (Neuseeland), Requisition oder Judicial Rogatory Letters (Frankreich), Solicitud Datos (Spanien), Ordem Judicial (Brasilien), Auskunftsersuchen (Deutschland), Obligation de dépôt (Schweiz), 個人情報の開示依頼 (Japan), Personal Data Request (Großbritannien) sowie gleichwertige Gerichtsbeschlüsse und/oder Anfragen aus anderen Ländern.

B. Umgang mit und Beantworten von Auskunftsersuchen von Regierungs- und Strafverfolgungsbehörden

Apple prüft sämtliche Anfragen von Regierungs- und Strafverfolgungsbehörden bzw. von privaten Parteien sorgfältig, um sicherzustellen, dass jede Anfrage eine gültige Rechtsgrundlage besitzt. Gültigen Anfragen wird entsprochen. In Fällen, in denen Apple feststellt, dass keine gültige Rechtsgrundlage vorliegt, oder eine Anfrage als unklar, unangemessen oder zu weit gefasst ansieht, wird Apple die entsprechende Anfrage anfechten oder ablehnen.

C. Anfragen zur Datensicherstellung

Alle Anfragen von Regierungs- und Strafverfolgungsbehörden außerhalb der USA nach Inhalten müssen den geltenden Gesetzen, einschließlich des US-Gesetzes über den Datenschutz bei elektronischer Kommunikation (United States Electronic Communications Privacy Act, ECPA) entsprechen. Ausnahmen gelten nur bei Notfällen (im Folgenden unter „Notfallanfragen“ definiert). Eine Anfrage im Rahmen eines gegenseitigen Rechtshilfeabkommens mit den Vereinigten Staaten erfolgt in Übereinstimmung mit dem ECPA. Eine Anfrage zur Sicherstellung von Daten im Vorgriff auf

eine folgende ECPA-konforme Anfrage ist per E-Mail an Apple Inc. zu richten, und zwar an folgende E-Mail-Adresse: lawenforcement@apple.com.

Anfragen zur Datensicherstellung müssen die relevante Apple ID/Account E-Mail-Adresse oder den vollständigen Namen **und** die Telefonnummer und/oder den vollständigen Namen **und** die Wohnanschrift des betreffenden Apple Accounts enthalten. Nach Eingang einer Anfrage zur Datensicherstellung erstellt Apple Inc. einen einmaligen Auszug der zum Anfragezeitpunkt vorhandenen angefragten Nutzerdaten und stellt diesen für einen Zeitraum von 90 Tagen sicher. Nach dieser 90-Tage-Frist wird die Datensicherstellung automatisch vom Speicherserver entfernt. Allerdings kann dieser Zeitraum mit einer erneuten Anfrage um weitere 90 Tage verlängert werden. Mehr als zwei Anfragen zur Datensicherstellung für denselben Account werden wie Anfragen zur Verlängerung der Aufbewahrungsdauer der ursprünglich sichergestellten Daten behandelt, d. h., Apple Inc. stellt im Anschluss an solche Anfragen keine neuen Daten sicher.

D. Notfallanfragen

Apple versteht unter einer Notfallanfrage eine Anfrage, die sich auf Umstände bezieht, die eine unmittelbare und ernsthafte Bedrohung für Folgendes darstellen:

1) das Leben/die Sicherheit von Einzelpersonen,
2) die Sicherheit von Bundesländern/-staaten,
3) die Sicherheit wichtiger Infrastruktureinrichtungen.

Kann der Regierungs- oder Ermittlungsbeamte zufriedenstellend nachweisen, dass sich die Anfrage auf einen Notfall nach einem der oben angeführten Kriterien bezieht, geht Apple der Anfrage umgehend nach und behandelt sie als Notfall.

Um eine Notfallanfrage an Apple zu stellen, muss der die Anfrage stellende Regierungs- oder Ermittlungsbeamte das Formular Emergency Government & Law Enforcement Information Request ausfüllen und es direkt vom offiziellen E-Mail-Account der Regierungs- oder Strafverfolgungsbehörde aus mit Betreff „Emergency Request“ an folgende Adresse senden: exigent@apple.com

Sollte Apple in seiner Antwort auf ein solches Notfall-Auskunftsersuchen der Regierungs- oder Strafverfolgungsbehörde (Emergency Government & Law Enforcement Information Request) Kundendaten vorlegen, muss ein namentlich zu nennender Dienstvorgesetzter des Ermittlungsbeamten, der die Notfallanfrage eingereicht hat, gegenüber Apple bestätigen, dass es sich um eine berechtigte Notfallanfrage handelt. Der Regierungs- oder Ermittlungsbeamte, der die Notfallanfrage einreicht, muss die Kontaktdaten seines Vorgesetzten bereits in der Anfrage nennen.

Wenn eine Regierungs- oder Strafverfolgungsbehörde Apple außerhalb der Geschäftszeiten (vor 8.00 Uhr oder nach 17.00 Uhr PST) für eine Notfallanfrage erreichen muss, kann sich der entsprechende Mitarbeiter unter 001 408 974-2095 an das Global Security Operations Center (GSOC) von Apple wenden. Unter dieser Rufnummer erhalten Sie Hilfe in mehreren Sprachen.

E. Anfragen zur Einschränkung/Löschung von Accounts

Wenn eine Regierungs- oder Strafverfolgungsbehörde von Apple die Einschränkung bzw. Löschung der Apple-ID eines Kunden verlangt, benötigt Apple dazu einen Gerichtsbeschluss oder einen gleichwertigen inländischen Rechtsvorgang (einschließlich Verurteilung oder Haftbefehl), der belegt,

dass der einzuschränkende bzw. zu löschende Account rechtswidrig verwendet wurde. Apple führt keine Einschränkung/Löschung von Kunden-Accounts auf eine inoffizielle/ungültige Anfrage hin durch.

Apple prüft sämtliche Anfragen von Regierungs- und Strafverfolgungsbehörden sorgfältig, um sicherzustellen, dass jede Anfrage eine gültige Rechtsgrundlage besitzt. In Fällen, in denen Apple feststellt, dass keine gültige Rechtsgrundlage vorliegt, oder in denen der Gerichtsbeschluss nicht hinreichend belegt, dass der einzuschränkende bzw. zu löschende Account rechtswidrig verwendet wurde, wird Apple die Anfrage ablehnen bzw. anfechten.

Wenn Apple einen zufriedenstellenden Gerichtsbeschluss oder einen gleichwertigen inländischen Rechtsvorgang (einschließlich einer Verurteilung oder eines Haftbefehls) von der Regierungs- oder Strafverfolgungsbehörde erhält, der belegt, dass der einzuschränkende bzw. zu löschende Accountrechtswidrig betrieben wurde, wird Apple die notwendigen Maßnahmen zur dem Gerichtsbeschluss entsprechenden Einschränkung/Löschung des Accounts ergreifen und den anfragenden Mitarbeiter entsprechend informieren.

F. Benachrichtigung des Benutzers

Apple informiert betroffene Kunden/Nutzer, wenn deren Apple Account Informationen im Zuge einer gültigen rechtlichen Anfrage von Regierungs- oder Strafverfolgungsbehörden ermittelt werden. Ausgenommen hiervon sind jedoch Fälle, in denen ein solches Informieren durch die gültige rechtliche Anfrage, durch einen Apple zugestellten Gerichtsbeschluss oder durch geltende Gesetze ausdrücklich untersagt ist oder in denen Apple nach eigenem Ermessen der Auffassung ist, dass ein solches Informieren das Risiko einer Verletzung oder des Zutodekommens einer identifizierbaren Person nach sich zöge, in Situationen, in denen der Fall in Zusammenhang mit einer Kindesgefährdung steht oder in denen ein solches Informieren nicht den zugrundeliegenden Tatsachen des Falls entspricht, oder wenn Apple zur begründeten Auffassung kommt, dass ein solches Informieren den Rechtsablauf behindern oder der Rechtsprechung schaden könnte.

Nach Ablauf von 90 Tagen übermittelt Apple eine verzögerte Benachrichtigung über die Notfallanfrage. Ausgenommen hiervon sind jedoch Fälle, in denen ein solches Informieren durch einen Gerichtsbeschluss oder durch geltende Gesetze untersagt ist oder in denen Apple nach eigenem Ermessen der Auffassung ist, dass ein solches Informieren das Risiko einer Verletzung oder des Zutodekommens einer identifizierbaren Person oder Personengruppe nach sich zöge, oder in Situationen, in denen der Fall in Zusammenhang mit einer Kindesgefährdung steht. Apple übermittelt eine solche verzögerte Benachrichtigung über Anfragen nach Ablauf der in einem Gerichtsbeschluss festgelegten Vertraulichkeitsfrist, es sei denn, Apple gelangt nach eigenem Ermessen zur begründeten Auffassung, dass ein solches Informieren das Risiko einer Verletzung oder des Zutodekommens einer identifizierbaren Person oder Personengruppe nach sich zöge, in Situationen, in denen der Fall in Zusammenhang mit einer Kindesgefährdung steht oder in denen ein solches Informieren nicht den zugrundeliegenden Tatsachen des Falls entspricht, oder wenn Apple zur begründeten Auffassung kommt, dass ein solches Informieren den Rechtsablauf behindern oder der Rechtsprechung schaden könnte.

Apple informiert seine Kunden, wenn deren Apple Account infolge eines Apple zugestellten Gerichtsbeschlusses (einschließlich einer Verurteilung oder eines Haftbefehls), aus dem hervorgeht, dass der einzuschränkende bzw. zu löschende Account rechtswidrig oder in Verletzung der Nutzungsbedingungen von Apple betrieben wurde, eingeschränkt oder gelöscht wurde. Ausgenommen hiervon sind jedoch Fälle, in denen ein solches Informieren durch den Rechtsprozess selbst, durch einen Apple zugestellten Gerichtsbeschluss oder durch geltende Gesetze ausdrücklich untersagt ist, in

Situationen, in denen der Fall in Zusammenhang mit einer Kindesgefährdung steht oder in denen Apple nach eigenem Ermessen der begründeten Auffassung ist, dass ein solches Informieren das Risiko einer Verletzung oder des Zutodekommens einer identifizierbaren Person oder Personengruppe nach sich zöge, oder in Situationen, in denen ein solches Informieren nicht den zugrundeliegenden Tatsachen des Falls entspricht, oder wenn Apple zur begründeten Auffassung kommt, dass ein solches Informieren den Rechtsablauf behindern oder der Rechtsprechung schaden könnte.

III. Von Apple verfügbare Informationen

In diesem Abschnitt werden die allgemeinen Arten von Informationen abgedeckt, die von Apple zum Zeitpunkt der Veröffentlichung dieser Richtlinien, zur Verfügung gestellt werden können.

A. Geräteregistrierung

Bei der Registrierung von Apple-Geräten mit Betriebssystemversionen vor iOS 8 und macOS Sierra 10.12 stellen Kunden Apple grundlegende Registrierungs- oder Kundeninformationen wie Name, Adresse, E-Mail-Adresse und Telefonnummer bereit. Diese Informationen werden von Apple nicht überprüft und sind möglicherweise nicht genau und geben ggf. keinen Aufschluss über den Besitzer des Geräts. Bei Geräten mit iOS 8 und neueren Versionen sowie Mac-Computern mit macOS Sierra 10.12 und neueren Versionen werden Registrierungsinformationen übermittelt, sobald ein Kunde ein Gerät einer iCloud-Apple-ID zuordnet. Diese Informationen sind möglicherweise nicht genau und geben ggf. keinen Aufschluss über den Besitzer des Geräts. Sofern verfügbar, können Registrierungsinformationen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Hinweis: Die Buchstaben „O“ und „I“ kommen in Seriennummern von Apple-Geräten nicht vor. Vielmehr werden dort die Zahlen 0 (null) und 1 (eins) verwendet. Anfragen nach Seriennummern mit den Buchstaben „O“ und „I“ liefern keine Ergebnisse.

B. Kunden-Serviceeinträge

Kontakte, die Kunden mit dem Apple Kundenservice bezüglich eines Geräts oder einer Dienstleistung hatten, können von Apple bezogen werden. Diese Informationen können Aufzeichnungen über Support-Interaktionen mit Kunden bezüglich eines bestimmten Apple Geräts oder einer bestimmten Serviceleistung enthalten. Darüber hinaus können auch Informationen über das Gerät, die Garantie und die Reparatur verfügbar sein. Sofern verfügbar, können diese Informationen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

C. iTunes

iTunes ist eine kostenlose Softwareanwendung, mit der Kunden digitale Musik und Videos auf ihren Computern ordnen und abspielen können. Außerdem können Kunden hier Inhalte kaufen und auf ihre Computer oder iOS-Geräte laden. Beim Eröffnen eines iTunes-Accounts kann der Kunde grundlegende Abonnenteninformationen wie Name, Wohnanschrift, E-Mail-Adresse und Telefonnummer angeben. Zudem sind ggf. Informationen zu iTunes-Kauf-/Downloadtransaktionen und -verbindungen, Verbindungen zum Zweck von Aktualisierung/erneutem Download sowie iTunes

Match-Verbindungen verfügbar. Sofern verfügbar, können iTunes-Abonnenteninformationen und Verbindungsprotokolle mit IP-Adressen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Anfragen nach iTunes-Daten müssen die Apple-Gerätekennzeichnung (Seriennummer, IMEI, MEID oder GUID) oder die betroffene E-Mail-Adresse zur Apple-ID bzw. zum Apple-Account enthalten. Ist die E-Mail-Adresse zur Apple ID/zum Account nicht bekannt, benötigt Apple iTunes-Abonnenteninformationen in Form des vollständigen Namens **und** der Telefonnummer und/oder des vollständigen Namens **und** der Wohnanschrift, um den entsprechenden Account des iTunes-Abonnenten identifizieren zu können. Regierungs- oder Ermittlungsbeamte können auch eine gültige iTunes-Auftragsnummer oder eine vollständige Debit- oder Kreditkartennummer, mit der iTunes-Käufe getätigt wurden, vorlegen. In Verbindung mit diesen Parametern kann auch ein Kundenname angegeben werden. Der Kundenname allein reicht zur Offenlegung der Informationen jedoch nicht aus.

Bitte beachten: Insoweit Ihre rechtliche Anfrage vollständige Kredit- bzw. Debitkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument bzw. einer entsprechenden Datei an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen.

D. Transaktionen im Apple Store

Bargeld-, Kredit-/Bankkarten- oder Geschenkkartentransaktionen, die im Apple Store stattfinden, sind sogenannte Verkaufsstellentransaktionen. Anfragen nach Verkaufsstellenaufzeichnungen müssen die vollständige Nummer der verwendeten Kredit- bzw. Debitkarte enthalten, können jedoch auch weitere Angaben umfassen, z. B. Datum und Uhrzeit der Transaktion, Betrag und gekaufte Artikel. Sofern verfügbar, können Informationen in Bezug auf den mit einem bestimmten Einkauf verknüpften Kartentyp, den Namen des Käufers, die E-Mail-Adresse, Datum/Uhrzeit und Betrag der Transaktion und Standort des Stores über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Anfragen nach Kaufbelegkopien müssen die mit den jeweiligen Käufen verknüpften Einzelhandels-Transaktionsnummern umfassen. Sofern verfügbar, können diese Informationen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Bitte beachten: Insoweit Ihre rechtliche Anfrage vollständige Kredit- bzw. Debitkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument bzw. einer entsprechenden Datei an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen.

E. Einkäufe im Apple Online Store

Apple pflegt Informationen über Einkäufe im Apple Online Store. Diese können unter anderem den Namen des Käufers, die Lieferadresse, die Telefonnummer, die E-Mail-Adresse, gekaufte Produkte, den Kaufbetrag und die beim Kauf verwendete IP-Adresse umfassen. Auskunftsersuchen hinsichtlich Bestellungen im Apple Online Store müssen eine vollständige Kredit- bzw. Debitkartennummer oder eine Auftragsnummer, eine Referenznummer oder die Seriennummer des gekauften Artikels

enthalten. In Verbindung mit diesen Parametern kann auch ein Kundenname angegeben werden. Der Kundenname allein reicht zur Offenlegung der Informationen jedoch nicht aus. Alternativ können Auskunftsersuchen über Bestellungen im Apple Online Store die E-Mail-Adresse der betroffenen Apple ID bzw. des betroffenen Accounts enthalten. Ist die E-Mail-Adresse zur Apple ID/zum Account nicht bekannt, benötigt Apple Abonnenteninformationen in Form des vollständigen Namens **und** der Telefonnummer und/oder des vollständigen Namens **und** der Wohnanschrift, um den entsprechenden Apple Account identifizieren zu können. Sofern verfügbar, können Informationen über Käufe im Apple Online Store über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Bitte beachten: Insoweit Ihre rechtliche Anfrage vollständige Kredit- bzw. Debitkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument bzw. einer entsprechenden Datei an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen.

F.Geschenkkarten

Apple Store-Geschenkkarten und iTunes Store-Geschenkkarten besitzen sowohl eine Seriennummer als auch einen PIN-Code (auch Einlöse-PIN-Code genannt). Apple Store-Geschenkkarten und iTunes Store-Geschenkkarten können verschiedene Formate bei der Seriennummer aufweisen. Dies hängt von Variablen wie etwa dem Design und/oder dem Ausstellungsdatum ab. Mit dem Einlöse-PIN-Code kann bei beiden Geschenkkartenarten auf das Guthaben der jeweiligen Geschenkkarte zugegriffen werden. Der PIN-Code der Geschenkkarte ist für Apple der zuverlässigste Parameter für eine Suche nach Informationen im Zusammenhang mit der jeweiligen Geschenkkarte. Wenn eine rechtliche Anfrage 5 oder mehr PIN-Codes von Geschenkkarten enthält, benötigt Apple diese PIN-Codes außerdem in einem editierbaren elektronischen Format.

i. Apple Store-Geschenkkarten

Apple Store-Geschenkkarten können für Einkäufe im Apple Online Store oder in einem Apple Store verwendet werden. Der PIN-Code auf einer Apple Store-Geschenkkarte beginnt mit dem Buchstaben „Y“. In manchen Fällen können ältere Apple Store-Geschenkkarten ein achtstelliges PIN-Code-Format aufweisen. Zu den möglicherweise verfügbaren Aufzeichnungen gehören Informationen über den Käufer der Geschenkkarte (sofern von Apple und nicht von einem Dritthändler erworben), die damit verknüpften Kauftransaktionen und die gekauften Artikel. In einigen Fällen kann Apple eine Apple Store-Geschenkkarte möglicherweise stornieren oder sperren. Dies hängt vom Status der betroffenen Karte ab. Sofern verfügbar, können Informationen über Apple Store-Geschenkkarten über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Bitte beachten: Insoweit Ihre rechtliche Anfrage vollständige Apple Store-Geschenkkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument bzw. einer entsprechenden Datei an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen.

ii. iTunes Store-Geschenkkarten

iTunes Store-Geschenkkarten können im iTunes Store, App Store, iBooks Store und Mac App Store verwendet werden. Der PIN-Code auf einer iTunes Store-Geschenkkarte beginnt mit dem Buchstaben „X“. Anhand des PIN-Codes kann Apple bestimmen, ob die iTunes Store-Geschenkkarte aktiviert (d. h. sie wurde an einer Einzelhandels-Verkaufsstelle gekauft) oder eingelöst wurde (d. h. sie wurde auf das Guthaben eines iTunes-Accounts aufgebucht).

Bei einer aktivierten iTunes Store-Geschenkkarte können die verfügbaren Aufzeichnungen den Namen des Stores, den Standort sowie Datum und Uhrzeit umfassen. Bei einer eingelösten iTunes Store-Geschenkkarte können die verfügbaren Aufzeichnungen Angaben zum Abonnenten des jeweiligen iTunes-Accounts, Datum und Uhrzeit der Aktivierung bzw. der Einlösung sowie die bei Einlösung verwendete IP-Adresse abdecken. In einigen Fällen kann Apple eine iTunes Store-Geschenkkarte möglicherweise deaktivieren. Dies hängt vom Status der jeweiligen Karte ab. Sofern verfügbar, können Informationen zu iTunes Store-Geschenkkarten über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Bitte beachten: Insoweit Ihre rechtliche Anfrage vollständige iTunes Store-Geschenkkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument bzw. einer entsprechenden Datei an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen.

G. iCloud

iCloud ist der Cloud-Dienst von Apple, mit dem die Nutzer von all ihren Geräten aus auf ihre Musik, Fotos, Dokumente und mehr zugreifen können. Außerdem können Abonnenten mit iCloud Inhalte von ihren iOS-Geräten in iCloud sichern. In Verbindung mit dem iCloud-Dienst können Abonnenten ein iCloud.com-E-Mail-Konto einrichten. iCloud-E-Mail-Domains können wie folgt lauten: @icloud.com, @me.com und @mac.com. Alle iCloud-Inhaltsdaten, die von Apple gespeichert werden, sind am Serverstandort verschlüsselt. Wenn andere Anbieter zur Speicherung von Daten genutzt werden, gibt Apple die Schlüssel nicht an diese weiter. Apple speichert die Verschlüsselungsschlüssel in seinen US-amerikanischen Rechenzentren.

iCloud ist ein Abonnement-basierter Service. Anfragen nach iCloud-Daten müssen die entsprechende E-Mail-Adresse zur Apple-ID/zum Account beinhalten. Ist die E-Mail-Adresse zur Apple ID/zum Account nicht bekannt, benötigt Apple Abonnenteninformationen in Form des vollständigen Namens und der Telefonnummer und/oder des vollständigen Namens und der Wohnanschrift, um den entsprechenden Apple Account identifizieren zu können.

Folgende Informationen sind ggf. in iCloud verfügbar:

i. Abonnenteninformationen

Wenn ein Kunde einen iCloud-Account einrichtet, kann er Apple grundlegende Abonnenteninformationen wie Name, Wohnanschrift, E-Mail-Adresse und Telefonnummer angeben. Zudem sind ggf. Verbindungsinformationen zu iCloud-Funktionen verfügbar. Sofern verfügbar, können iCloud-Abonnenteninformationen und Verbindungsprotokolle mit

IP-Adressen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden. Verbindungsprotokolle werden bis zu 30 Tage lang gespeichert.

ii. Mailprotokolle

iCloud-Mailprotokolle umfassen Aufzeichnungen zu ein- und ausgehender Kommunikation wie Uhrzeit, Datum sowie E-Mail-Adresse von Absender und Empfänger. iCloud-Mailprotokolle werden bis zu 30 Tage aufbewahrt und können, sofern verfügbar, über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

iii. E-Mail-Inhalte und andere iCloud-Inhalte. Mein Fotostream, iCloud-Fotomediathek, iCloud Drive, Kontakte, Kalender, Lesezeichen, Safari-Browserverlauf, Karten-Suchverlauf, Nachrichten, Backups von iOS-Geräten

iCloud speichert Inhalte für Dienste, die der Abonnent für die Pflege im Account ausgewählt hat, während der Account des Abonnenten aktiv bleibt. Apple speichert keine Inhalte, nachdem diese von den Apple-Servern gelöscht wurden. iCloud-Inhalte sind beispielsweise E-Mails, gespeicherte Fotos, Dokumente, Kontakte, Kalender, Lesezeichen, Safari-Browserverlauf, Karten-Suchverlauf, Nachrichten oder Backups von iOS-Geräten. Backups von iOS-Geräten können Fotos und Videos, Geräteeinstellungen, App-Daten, iMessage-Nachrichten, Geschäftschat, SMS- und MMS-Nachrichtensowie Voicemail enthalten. Alle iCloud-Inhaltsdaten, die von Apple gespeichert werden, sind am Serverstandort verschlüsselt. Wenn andere Anbieter zur Speicherung von Daten genutzt werden, gibt Apple die Schlüssel nicht an diese weiter. Apple speichert die Verschlüsselungsschlüssel in seinen US-amerikanischen Rechenzentren.

Alle Anfragen von Regierungs- und Strafverfolgungsbehörden außerhalb der USA nach Inhalten müssen den geltenden Gesetzen, einschließlich des US-Gesetzes über den Datenschutz bei elektronischer Kommunikation (United States Electronic Communications Privacy Act, ECPA), entsprechen. Ausnahmen gelten nur bei Notfällen (unter „Notfallanfragen“ weiter oben definiert). Eine Anfrage im Rahmen eines gegenseitigen Rechtshilfeabkommens mit den Vereinigten Staaten erfolgt in Übereinstimmung mit dem ECPA. Apple Inc. stellt Inhalte von Abonnenten ausschließlich infolge eines derartigen rechtsgültigen Verfahrens und nur in der im Account des Abonnenten vorliegenden Form zur Verfügung.

H. Mein iPhone suchen

„Mein iPhone suchen“ ist eine Funktion für Nutzer, mit der iCloud-Abonnenten verlorene oder verlegte iPhone-, iPad-, iPod touch-, Apple Watch- oder Mac-Geräte suchen und/oder bestimmte Maßnahmen ergreifen können. Sie können z. B. den Modus „Verloren“ für ein Gerät aktivieren, ein Gerät sperren oder alle Einstellungen und Inhalte löschen. Weitere Informationen über diesen Dienst finden Sie unter http://www.apple.com/icloud/find-my-iphone.html.

Damit ein Nutzer, der sein Gerät verloren hat, die Funktion „Mein iPhone suchen“ verwenden kann, muss diese bereits vor dem Verlust auf dem betroffenen Gerät aktiviert gewesen sein. Ein Aktivieren der Funktion „Mein iPhone suchen“ ist nach dem Verlust des Geräts nicht mehr möglich. Sie kann auch nicht per Fernsteuerung oder auf Anfrage von Regierungs- oder Strafverfolgungsbehörden aktiviert werden. Daten aus Standortdiensten werden jeweils direkt auf dem fraglichen Gerät

gespeichert, und Apple hat keine Möglichkeit, solche Informationen von einem bestimmten Gerät abzufragen. Die Informationen der Standortdienste eines Geräts, das mit der App „Mein iPhone suchen“ aufgefunden wurde, werden den Nutzern angezeigt. Apple speichert keine Inhalte mit Karten oder Benachrichtigungen im Rahmen des Dienstes. Der folgende Support-Link liefert Informationen und Maßnahmen, die ein Nutzer bei Verlust oder Diebstahl eines iOS-Geräts ergreifen kann: https://support.apple.com/de-de/HT201472.

Verbindungsprotokolle zu „Mein iPhone suchen“ stehen für einen Zeitraum von zirka 30 Tagen zur Verfügung. Sind sie verfügbar, können sie über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden. Sofern verfügbar, können Transaktionsaktivitäten zu „Mein iPhone suchen“ zum Zwecke von Anfragen zum ferngesteuerten Sperren oder Löschen eines Geräts über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

I. Extrahieren von Daten aus mit Code gesperrten iOS-Geräten

Bei Geräten mit iOS 8.0 und später kann Apple keine Extraktion von iOS-Gerätedaten durchführen, da die Daten, die von Strafverfolgungsbehörden in der Regel ermittelt werden sollen, verschlüsselt sind und Apple den Verschlüsselungsschlüssel nicht besitzt. Ab dem iPhone 6 wird auf allen Geräten werksseitig iOS 8.0 oder eine spätere iOS-Version ausgeführt.

Bei Geräten mit iOS 4 bis iOS 7 kann Apple, je nach Status des Geräts, eine iOS-Datenextraktion durchführen. Dabei kommt das Datenschutzgesetz Kaliforniens zur elektronischen Kommunikation (California's Electronic Communications Privacy Act, CalECPA) zur Anwendung, das in den Paragrafen 1546–1546.4 des kalifornischen Strafgesetzbuchs (California Penal Code) definiert ist. Für die Durchführung einer iOS-Datenextraktion bei einem Gerät, das diese Kriterien erfüllt, benötigt Apple von den Strafverfolgungsbehörden einen Durchsuchungsbefehl, der aufgrund hinreichenden Verdachts unter dem CalECPA ausgestellt wurde. Abgesehen von CalECPA erkennt Apple keine etablierten Rechtsinstanzen, die von Apple eine Datenextraktion als Drittpartei bei einem Ermittlungsverfahren verlangen.

J. Weitere verfügbare Geräteinformationen

MAC-Adresse: Bei der MAC-Adresse („Media Access Control“) handelt es sich um einen eindeutigen Bezeichner, der Netzwerkschnittstellen zur Kommunikation im physikalischen Netzwerksegment zugeordnet ist. Alle Apple Produkte mit Netzwerkschnittstellen (z. B. Bluetooth, Ethernet, WLAN oder FireWire) weisen mindestens eine MAC-Adresse auf. Gegen Vorlage einer Seriennummer (bzw. der IMEI, MEID oder UDID bei einem iOS-Gerät) kann Apple ggf. sachdienliche Informationen abrufen. Sofern verfügbar, können diese über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

K. Anfragen nach Videoüberwachungsdaten aus Apple Stores

Videoüberwachungsdaten können je nach Store-Standort variieren. Solche Videoüberwachungsdaten werden in einem Apple Store maximal 30 Tage aufbewahrt. In vielen Rechtsgebieten beträgt die Aufbewahrungsdauer je nach einschlägiger Rechtslage lediglich 24 Stunden. Nach Verstreichen dieses Zeitraums stehen die Daten möglicherweise nicht mehr zur Verfügung. Anfragen, die nur Videoüberwachungsdaten betreffen, können an die folgende E-Mail-Adresse gesendet werden:

lossprevention@apple.com. Dabei sollten die Regierungs- oder Ermittlungsbehörden Datum, Uhrzeit und die zugehörigen Transaktionsinformationen in Bezug auf die angeforderten Daten angeben.

L. Game Center

Game Center ist das soziale Spielenetzwerk von Apple. Ggf. sind für einen Nutzer oder ein Gerät Informationen zu Game Center-Verbindungen verfügbar. Sofern verfügbar, können Verbindungsprotokolle mit IP-Adressen und Transaktionsdaten über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

M. iOS-Geräteaktivierung

Wenn ein Kunde ein iOS-Gerät aktiviert oder die Software aktualisiert, werden je nach Ereignis vom Dienstanbieter oder durch das Gerät bestimmte Informationen an Apple übermittelt. Gegebenenfalls sind IP-Adressen, ICCID-Nummern oder andere Gerätebezeichner verfügbar. Sofern verfügbar, können diese Informationen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

Dual-SIM: Bei Geräten mit einer Dual-SIM können die Mobilfunkanbieterdaten für die nano-SIM-Karte und/oder eSIM ggf. über eine Vorladung oder einen darüber hinausgehenden Rechtsweg eingeholt werden. Eine eSIM ist eine digitale SIM, die Nutzern ermöglicht, einen Mobilfunktarif von ihrem Mobilfunkanbieter zu aktivieren, ohne auf eine physische Nano-SIM-Karte angewiesen zu sein. Weitere Informationen finden sich unter https://support.apple.com/de-de/HT209044.

N. Authentifizierungsprotokolle

Aufzeichnungen von Authentifizierungsaktivitäten in Zusammenhang mit Apple Diensten (z. B. iTunes, iCloud, Meine Apple-ID oder Apple Diskussionen) für einen Nutzer oder ein Gerät können – sofern verfügbar – bei Apple angefragt werden. Sofern verfügbar, können Verbindungsprotokolle mit IP-Adressen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

O. Protokolle für „Meine Apple-ID“ und iForgot

Protokolle für Meine Apple-ID und iForgot für einen Nutzer können bei Apple angefragt werden. Die Protokolle für Meine Apple-ID und iForgot können Informationen über Passwortrücksetzungen enthalten. Sofern verfügbar, können Verbindungsprotokolle mit IP-Adressen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragsstellers abgefragt werden.

P. FaceTime

FaceTime-Kommunikationen sind durchgehend verschlüsselt. Apple verfügt über keine Möglichkeit FaceTime-Daten zu entschlüsseln, die zwischen Geräten gesendet werden. Apple kann FaceTime-Kommunikationen nicht abfangen. Apple verfügt über Protokolle, die Daten über die Einleitung von FaceTime-Anrufeinladungen enthalten. Diese Protokolle geben keinen Aufschluss darüber, ob zwischen Nutzern tatsächlich eine Kommunikation stattfand. Protokolle zu FaceTime-Anrufeinladungen werden bis zu 30 Tage lang gespeichert. Sofern verfügbar, können FaceTime-

Anrufeinladungen über einen Gerichtsbeschluss, eine richterliche Anordnung oder eine inländische Entsprechung abgefragt werden.

Q. iMessage

Kommunikationen über iMessage sind durchgehend verschlüsselt. Apple verfügt über keine Möglichkeit iMessage-Daten zu entschlüsseln, die zwischen Geräten gesendet werden. Apple kann keine iMessage-Kommunikationen abfangen, und Apple besitzt keine iMessage-Kommunikationsprotokolle. Apple besitzt jedoch iMessage-Fähigkeitsabfrageprotokolle. Diese Protokolle zeigen an, dass eine Abfrage von einer Geräteanwendung (Nachrichten, Kontakte, Telefon oder andere Geräteanwendungen) initiiert und an die Server von Apple geleitet wurde, wo nach einem Nachschlagziel (Lookup Handle) gesucht wird (z. B. eine Telefonnummer, eine E-Mail-Adresse oder eine Apple-ID), um festzustellen, ob dieses nachgeschlagene Element iMessage-fähig ist. Eine Abfrage der iMessage-Fähigkeit gibt keinen Aufschluss darüber, ob zwischen Nutzern tatsächlich eine Kommunikation stattfand. Anhand der Abfrageprotokolle zur iMessage-Fähigkeit kann Apple nicht bestimmen, ob eine tatsächliche iMessage-Kommunikation erfolgte. Außerdem kann Apple nicht die Anwendung bestimmen, die die Abfrage initiierte. Abfrageprotokolle der iMessage-Fähigkeit sind keine Bestätigung, dass tatsächlich der Versuch eines iMessage-Ereignisses unternommen wurde. iMessage-Fähigkeitsabfrageprotokolle werden bis zu 30 Tage aufbewahrt. Sofern verfügbar, können iMessage-Fähigkeitsabfrageprotokolle über einen Gerichtsbeschluss, eine richterliche Anordnung oder eine inländische Entsprechung abgefragt werden.

IV. Fragen und Antworten

F: Kann ich Fragen zu meinem Auskunftsersuchen im Zuge eines Ermittlungsverfahrens per E-Mail an Apple richten?
A: Ja, Fragen oder Ersuchen im Zusammenhang mit einem Ermittlungsverfahren können per E-Mail an lawenforcement@apple.com gerichtet werden.

F: Muss ein Gerät bei Apple registriert sein, damit es funktioniert oder verwendet werden kann?
A: Nein, ein Gerät muss nicht bei Apple registriert sein, damit es funktioniert oder verwendet werden kann.

F: Kann Apple den Code eines derzeit gesperrten iOS-Geräts bereitstellen?
A: Nein, Apple hat keinen Zugriff auf den Code eines Nutzers.

F: Kann Apple mir helfen, ein verlorenes oder gestohlenes Gerät dem rechtmäßigen Eigentümer zurückzugeben?
A: Wenden Sie sich in einem solchen Fall an lawenforcement@apple.com. Geben Sie dabei auch die Serien- oder IMEI-Nummer des Geräts sowie alle weiteren sachdienlichen Informationen an. Wenn die entsprechenden Kundeninformationen verfügbar sind, nehmen wir Kontakt mit dem Kunden auf, und bitten ihn oder sie, sich an die entsprechende Dienststelle zu wenden, um das Gerät zurückzuerhalten. Wenn sich der Kunde jedoch nicht anhand der verfügbaren Daten ermitteln lässt, werden Sie angewiesen, eine rechtsgültige Anfrage zu stellen.

F: Führt Apple eine Liste verlorener oder gestohlener Geräte?
A: Nein, Apple führt keine Liste verlorener oder gestohlener Geräte.

F: Wie sollte mit den bereitgestellten Informationen verfahren werden, nachdem die Behörde die Ermittlungen eingestellt bzw. abgeschlossen hat?
A: Alle Informationen und Daten, die für Regierungs- oder Strafverfolgungsbehörden bereitgestellt wurden und personenbezogene Informationen enthalten, sowie alle ggf. erstellten Kopien hiervon müssen vernichtet werden, sobald die Ermittlungen und das Verfahren abgeschlossen und alle Rechtsmittel vollständig ausgeschöpft wurden.

F: Werden die entsprechenden Nutzer informiert, wenn Anfragen durch Ermittlungsbehörden über sie eingehen?
A: Ja, die Benachrichtigungsrichtlinie von Apple gilt für Account-Anfragen von Strafverfolgungsbehörden, Regierungsbehörden und privaten Parteien. Apple benachrichtigt Kunden und Account-Inhaber, es sei denn, es liegt eine Vertraulichkeitsverfügung vor, oder geltende Gesetze verbieten eine solche Benachrichtigung, oder Apple gelangt nach alleinigem Ermessen zu der begründeten Auffassung, dass eine solche Benachrichtigung ein potenzielles Risiko einer ernsthaften Verletzung oder des Todes eines Bürgers birgt, oder der Fall steht im Zusammenhang mit einer Kindesgefährdung, oder eine solche Benachrichtigung entspricht nicht den zugrundeliegenden Tatsachen,oder Apple gelangt zur begründeten Auffassung, dass eine solche Benachrichtigung den Rechtsablauf behindern oder der Rechtsprechung schaden könnte.