



Richtlinien für Rechtsverfahren

EMEIA-Ermittlungsbehörden

Diese Richtlinien werden für Ermittlungsbehörden und andere Regierungsstellen der EMEIA-Region (Europa, Naher Osten, Indien, Afrika) bereitgestellt, die bei dort tätigen Apple Niederlassungen Informationen über die Nutzer von Apple Produkten und Diensten anfragen oder Informationen von Apple Geräten erlangen möchten. In diesen Richtlinien bezeichnet „Apple“ die jeweilige Tochtergesellschaft, die gemäss unseren Datenschutzrichtlinien <http://www.apple.com/legal/privacy/de-ww/> in einer bestimmten Region für Kundeninformationen zuständig ist. Apple aktualisiert diese Richtlinien nach Bedarf. Diese Version wurde am 29. September 2015 veröffentlicht.

Alle anderen Anfragen zu Informationen in Bezug auf Apple Nutzer, einschliesslich Fragen von Nutzern bezüglich der Offenlegung von Informationen, sind an <https://www.apple.com/chde/privacy/contact/> zu richten. Diese Richtlinien gelten nicht für Anfragen, die Ermittlungsbehörden an Apple Inc. oder zuständige lokale Tochtergesellschaften von Apple ausserhalb der EMEIA-Region richten.

Im Falle von Informationsanfragen der Regierung befolgen wir die für internationale Unternehmen einschlägigen Gesetze über die Offenlegung und den Schutz von Daten und legen Informationen entsprechend den gesetzlichen Vorschriften offen. Bei Inhaltsanfragen von Ermittlungsbehörden ausserhalb der USA legt Apple – mit Ausnahme von Notfallsituationen (weiter unten unter „Notfall-Anfragen“ definiert) – Inhalte nur dann offen, wenn ein Durchsuchungsbeschluss gemäss einem geltenden Rechtshilfeabkommen (Mutual Legal Assistance Treaty) oder anderweitigen Kooperationen mit dem Justizministerium der USA vorliegt.

Inhaltsverzeichnis

I: Allgemeine Informationen

II. Richtlinien zur Zustellung

- A. Informationsanfragen von Ermittlungsbehörden
- B. Anfragen zur Datensicherstellung
- C. Notfall-Anfragen
- D. Anfragen zur Accountlöschung
- E. Benachrichtigung betroffener Nutzer

III. Bei Apple verfügbare Informationen

- A. Geräteregistrierung
- B. Kundendienstaufzeichnungen
- C. iTunes
- D. Transaktionen im Apple Store
- E. Einkäufe im Apple Online Store
- F. iTunes Geschenkkarten
- G. iCloud
- H. Mein iPhone suchen
- I. Extrahieren von Daten aus mit Code gesperrten iOS Geräten
- J. Weitere verfügbare Geräteinformationen
- K. Anfragen nach Überwachungsvideos aus dem Apple Store
- L. Game Center
- M. iOS Geräteaktivierung
- N. Authentifizierungsprotokolle
- O. Protokolle für Meine Apple ID und iForgot
- P. FaceTime

IV. Fragen und Antworten

V. Anhang A

VI. Anhang B

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, 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 [Datenschutzrichtlinie von Apple](#) und den gültigen [Nutzungsbedingungen/Allgemeinen Geschäftsbedingungen](#) für den jeweils angebotenen Service. 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 vorliegenden Richtlinien enthalten Informationen für Ermittlungsbehörden in der EMEIA-Region zu dem Rechtsverfahren, das Apple benötigt, um elektronische Informationen gegenüber Ermittlungsbehörden und Regierungsstellen der EMEIA-Region offenlegen zu können. Diese Richtlinien stellen keine Rechtsberatung dar. Der Abschnitt „Fragen und Antworten“ („FAQ“) dieser Richtlinien soll Antworten auf Fragen liefern, die Apple häufig gestellt werden. Weder diese Richtlinien noch die FAQ decken alle Umstände ab, die sich ergeben können. Weitere Fragen können an law.enf.emeia@apple.com gestellt werden. Diese E-Mail Adresse ist nur zur Verwendung durch Ermittlungs- und Regierungsbeamte gedacht. Alle an diese Adresse gerichteten E-Mails müssen von einem gültigen E-Mail Konto einer Ermittlungs-/Regierungsbehörde gesendet werden. 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 Ermittlungsbehörden darüber informiert werden.

Bei dem gemäss 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 unseren [Datenschutzrichtlinien](#) aufgeführten Zwecke erforderlich ist. Ermittlungsbehörden sind angehalten, ihre Anfragen so knapp und spezifisch wie möglich zu formulieren, um Fehlinterpretationen und/oder Einwände aufgrund einer zu breit gefassten Anfrage zu vermeiden.

II. Richtlinien zur Zustellung

A. Informationsanfragen durch Ermittlungsbehörden

Apple akzeptiert rechtsgültige Informationsanfragen durch Ermittlungsbehörden per E-Mail, sofern die Absenderadresse die offizielle E-Mail Adresse der betreffenden Ermittlungsbehörde ist. Ermittlungsbeamte in der EMEIA-Region, die eine Informationsanfrage an Apple stellen, müssen das „Law Enforcement Information Request“-Formular aus Anhang A ausfüllen und es von der offiziellen E-Mail Adresse ihrer Ermittlungsbehörde an law.enf.emeia@apple.com senden. Diese E-Mail Adresse ist nur zur Entgegennahme von Ermittlungsanfragen von Ermittlungs- und Regierungsbeamten gedacht.

Apple betrachtet eine Informationsanfrage durch Ermittlungsbehörden dann als rechtsgültig, wenn sie nach Treu und Glauben die Prävention, Aufdeckung oder Ermittlung von strafbaren Handlungen zum Zweck hat. Wir reagieren angemessen auf Anfragen, die wir in diesem Sinne als rechtsgültig betrachten.

B. Anfragen zur Datensicherstellung

Alle von Apple gespeicherten iCloud Inhaltsdaten werden am Serverstandort verschlüsselt. Wenn andere Anbieter zur Speicherung von Daten genutzt werden, erhalten diese von Apple niemals die Schlüssel. Apple speichert die Schlüssel in eigenen Rechenzentren in den USA. Daher müssen Ermittlungsbehörden ausserhalb der USA, die diese Inhalte einsehen möchten, um Rechtshilfe durch die Justizbehörden der USA ersuchen. Besteht zwischen einem Land und den USA ein Rechtshilfeabkommen (Mutual Legal Assistance Treaty, MLAT), so kann ein Rechtsverfahren gemäss diesem Abkommen oder durch andere Kooperationen mit den Justizbehörden der USA eingeleitet werden. Wird im Vorfeld eines bevorstehenden MLAT-Verfahrens um Datensicherstellung ersucht, ist der Antrag per E-Mail (subpoenas@apple.com) an Apple Inc. zu richten. 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 Ablauf der 90 Tage werden die sichergestellten Daten 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.

C. Notfall-Anfragen

Apple versteht unter einer Notfall-Anfrage eine Anfrage, die sich auf Umstände bezieht, die nach Treu und Glauben eine unmittelbare und ernsthafte Bedrohung

- 1) des Lebens/der Sicherheit von Einzelpersonen oder
- 2) der Sicherheit eines Staates darstellen oder
- 3) zu erheblichen Schäden an wichtiger Infrastruktur oder wichtigen Einrichtungen führen können.

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

Um eine Notfall-Anfrage an Apple zu stellen, muss der Ermittlungsbeamte die „EMERGENCY Law Enforcement Information Request“-Vorlage in Anhang B ausfüllen und direkt vom offiziellen E-Mail Konto der Ermittlungsbehörde aus mit Betreff „Emergency Law Enforcement Information Request“ an folgende Adresse senden: exigent@apple.com.

Sollte Apple in seiner Antwort auf die Notfall-Informationsanfrage der Ermittlungsbehörde Kundendaten vorlegen, muss ein Dienstvorgesetzter des Ermittlungsbeamten, der die Notfall-Anfrage eingereicht hat, gegenüber Apple bestätigen, dass es sich um eine berechnigte Notfall-Anfrage handelt. Deswegen verlangt Apple, dass der Ermittlungsbeamte in seiner Notfall-Anfrage Kontaktinformationen eines Dienstvorgesetzten angibt.

Zudem sollte sich der Ermittlungsbeamte, der die Notfall-Anfrage einreicht, unter +1 408 974 2095 an das Global Security Operations Centre (GSOC) von Apple wenden, dieses über das Vorliegen einer Notfall-Anfrage einer Ermittlungsbehörde sowie die wichtigsten Details daraus in Kenntnis setzen und darum bitten, sie dem zuständigen Team als Notfall-Anfrage vorzulegen. Unter dieser Telefonnummer wird Unterstützung für alle Sprachen bereitgestellt.

D. Anfragen zur Accountlöschung

Wenn eine Ermittlungsbehörde um Löschung der Apple ID eines Kunden ersucht, muss sie Apple einen Gerichtsbeschluss oder eine richterliche Anordnung vorlegen, in der der zu löschende Account und die Grundlage für die Anfrage angegeben sind.

E. Benachrichtigung betroffener Nutzer

Apple benachrichtigt seine Kunden, wenn eine Ermittlungsbehörde eine berechtigte Informationsanfrage nach persönlichen Daten stellt, es sei denn, die Benachrichtigung des Kunden würde nach Ermessen von Apple wahrscheinlich die Arbeit der Justiz behindern oder die Rechtspflege beeinträchtigen.

Apple benachrichtigt Nutzer zeitverzögert über Notfall-Anfragen, es sei denn, dass dies nach Ermessen von Apple wahrscheinlich die Arbeit der Justiz behindern oder die Rechtspflege beeinträchtigen würde. Apple benachrichtigt Nutzer nach Verstreichen einer gerichtlich verfügbaren Geheimhaltungsperiode zeitverzögert über Anfragen, es sei denn, dass dies nach Ermessen von Apple wahrscheinlich die Arbeit der Justiz behindern oder die Rechtspflege beeinträchtigen würde.

III. Bei Apple verfügbare Informationen

A. Geräteregistrierung

Bei der Registrierung von Apple Geräten mit Betriebssystemversionen vor iOS 8 und OS Yosemite 10.10 stellen Kunden Apple grundlegende Registrierungs- oder Kundeninformationen wie Name, Adresse, E-Mail Adresse und Telefonnummer bereit. Diese Informationen werden von Apple nicht überprüft, 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 OS Yosemite 10.10 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. Die Registrierungsinformationen können im Rahmen einer rechtsgültigen Anfrage angefordert 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. Daher liefern Anfragen nach Seriennummern mit den Buchstaben „O“ und „I“ keine Ergebnisse.

B. Kundendienstaufzeichnungen

Apple kann Informationen zu Kontaktaufnahmen zwischen Kunden und dem Kundendienst von Apple in Bezug auf ein Gerät oder einen Service zur Verfügung stellen. Zu diesen Informationen zählen ggf. Aufzeichnungen von Supportinteraktionen mit dem Kunden in Bezug auf ein konkretes Gerät oder einen Dienst von Apple. Zudem sind ggf. auch Informationen zu Gerät, Garantie und Reparaturen verfügbar. Diese Informationen können mit einer rechtsgültigen Anfrage angefordert 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. iTunes Abonnenteninformationen und Verbindungsprotokolle mit IP Adressen können mit einer rechtsgültigen Anfrage angefordert werden.

Aufzeichnungen zu iTunes Kauf-/Downloadtransaktionen werden vom luxemburgischen Unternehmen iTunes S.à.r.l. verwaltet. Aufgrund rechtlicher Bestimmungen kann iTunes nur dann auf solche Anfragen reagieren, wenn sie von der Luxemburger Staatsanwaltschaft für rechtmässig erklärt und an iTunes weitergeleitet wurden. Anfragen nach diesen Aufzeichnungen sind unter folgender Adresse an die Luxemburger Staatsanwaltschaft zu richten: Parquet Général, Procureur Général d'Etat, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, Fax-Nr.: +352 470 550, E-Mail: parquet.general@justice.etat.lu.

D. Transaktionen im Apple Store

Bargeld-, Kredit-/Bankkarten- oder Geschenkkartentransaktionen, die im Apple Store stattfinden, sind sogenannte Verkaufsstellentransaktionen. Für die Herausgabe von Informationen über die Art der Karte, die für einen bestimmten Kauf verwendet wurde, den Namen des Käufers, dessen E-Mail Adresse, Datum und Uhrzeit der Transaktion sowie Transaktionsbetrag und Standort des Store ist eine rechtsgültigen Anfrage erforderlich. Eine rechtsgültige Anfrage nach Aufzeichnungen von Verkaufsstellen muss die vollständige Nummer der verwendeten Kredit-/Bankkarte sowie ggf. alle zusätzlichen Informationen wie Datum und Uhrzeit der Transaktion sowie Kaufbetrag und gekaufte Produkte enthalten. Zudem können Ermittlungsbehörden Apple die Belegnummer des Kaufs bzw. der Käufe übermitteln, um als Antwort auf eine rechtsgültige Anfrage Kopien von Belegen zu erhalten.

E. Einkäufe im Apple Online Store

Apple hält Informationen zu Onlinekäufen vor, u. a. Käufername, Versandadresse, Telefonnummer, E-Mail Adresse, Bezeichnung des gekauften Produkts, Kaufbetrag und IP Adresse. Um diese Informationen zu erhalten, muss eine rechtsgültige Anfrage gestellt werden. Zur Anforderung von Informationen über Onlinekäufe (ausgenommen iTunes Käufe) sind eine vollständige Kredit-/Bankkartennummer, eine Bestellnummer, Referenznummer oder Seriennummer des gekauften Artikels erforderlich. In Verbindung mit diesen Parametern kann auch ein Kundenname angegeben werden. Der Kundenname allein reicht zur Offenlegung der Informationen jedoch nicht aus.

F. iTunes Geschenkkarten

iTunes Geschenkkarten tragen einen sechzehnstelligen alphanumerischen Einlösecode unter dem grauen Rubbelbereich auf der Kartenrückseite sowie einen neunzehnstelligen Code unten auf der Karte. Auf Grundlage dieser Codes kann Apple bestimmen, ob die Karte aktiviert¹ oder eingelöst wurde und ob über den der Karte zugeordneten Account Käufe erfolgten. Beim Aktivieren von iTunes Geschenkkarten speichert Apple den Namen des Store, den Standort, das Datum und die Uhrzeit. Wenn iTunes Geschenkkarten durch Käufe in iTunes eingelöst werden, wird die

¹ „Aktiviert“ bedeutet, dass die Karte in einem Geschäft gekauft, aber noch nicht verwendet oder eingelöst wurde.

Geschenkkarte mit einem Benutzerkonto verknüpft. Im Apple Online Store gekaufte iTunes Geschenkkarten können in den Systemen von Apple anhand ihrer Apple Online Store Bestellnummern ausfindig gemacht werden (Hinweis: Dies gilt nur für bei Apple und nicht bei anderen Anbietern gekaufte iTunes Geschenkkarten). Informationen zum Kunden, der die Karte(n) eingelöst hat, müssen im Rahmen einer rechtsgültigen Anfrage angefordert werden. Informationen zu iTunes Onlinekäufen sind über eine Anfrage an die Luxemburger Staatsanwaltschaft unter folgender Adresse einzuholen: Parquet Général, Procureur Général d'Etat, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, Fax-Nr.: +352 470 550, E-Mail: parquet.general@justice.etat.lu.

Apple kann iTunes Geschenkkarten als Reaktion auf eine rechtsgültige Anfrage von Ermittlungsbehörden/staatlichen Stellen nicht deaktivieren.

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. Mögliche iCloud E-Mail Domains sind @icloud.com, @me.com² und @mac.com. Alle iCloud Inhaltsdaten, die von Apple gespeichert werden, sind am Serverstandort verschlüsselt. Wenn andere Anbieter zur Speicherung von Daten genutzt werden, erhalten diese von Apple niemals die Schlüssel. Apple speichert die Schlüssel in eigenen Rechenzentren in den USA.

iCloud ist ein Abonnenten-basierter Service. Anfragen nach iCloud Daten müssen die entsprechende Apple ID/Account E-Mail Adresse beinhalten. Sind Apple ID/Account E-Mail Adresse 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. iCloud Abonnenteninformationen und Verbindungsprotokolle mit IP Adressen können mit einer rechtsgültigen Anfrage angefordert werden. Die Verbindungsprotokolle werden bis zu 30 Tage gespeichert.

ii. Mailprotokolle

iCloud Mailprotokolle umfassen Aufzeichnungen zu ein- und ausgehender Kommunikation wie Uhrzeit, Datum sowie E-Mail Adresse von Absender und Empfänger. Mailprotokolle können mit einer rechtsgültigen Anfrage angefordert werden. iCloud Mailprotokolle werden bis zu 60 Tage gespeichert.

² Der MobileMe Dienst wurde durch iCloud ersetzt. Deshalb verfügt Apple über keine separaten Inhalte, die ehemaligen MobileMe Accounts zugeordnet sind. Befinden sich die Inhalte nicht in iCloud, sind sie nicht mehr gespeichert.

iii. E-Mail Inhalte und andere iCloud Inhalte. Fotostream, Dokumente, Kontakte, Kalender, Lesezeichen, Backups von iOS Geräten

In iCloud werden Inhalte, die der Abonnent zur Verwaltung in seinem Account ausgewählt hat, nur gespeichert, solange der Account aktiv ist. iCloud Inhalte sind beispielsweise E-Mails, gespeicherte Fotos, Dokumente, Kontakte, Kalender, Lesezeichen oder Backups von iOS Geräten. Backups von iOS Geräten können Fotos und Videos aus den Aufnahmen des Nutzers, Geräteeinstellungen, App-Daten, iMessage Nachrichten, SMS und MMS Nachrichten sowie Voicemails enthalten. Alle Inhalte und Daten von iCloud, die von Apple gespeichert werden, sind am Serverstandort verschlüsselt. Wenn andere Anbieter zur Speicherung von Daten genutzt werden, erhalten diese von Apple niemals die Schlüssel. Apple speichert die Schlüssel in eigenen Rechenzentren in den USA. Ermittlungsbehörden ausserhalb der USA, die diese Inhalte einsehen möchten, müssen um Rechtshilfe durch die Justizbehörden der USA ersuchen. Besteht zwischen einem Land und den USA ein Rechtshilfeabkommen (Mutual Legal Assistance Treaty, MLAT), so kann ein Rechtsverfahren gemäss diesem Abkommen oder durch anderweitige Kooperationen mit den Justizbehörden der USA eingeleitet werden. Apple Inc. stellt Inhalte von Abonnenten, wie sie in dem Account des Abonnenten vorliegen, nur dann zur Verfügung, wenn ein Durchsuchungsbeschluss gemäss dem MLAT-Verfahren vorliegt.

Apple speichert keine Inhalte, nachdem diese von den Apple Servern gelöscht wurden.

H. Mein iPhone suchen

„Mein iPhone suchen“ ist eine Funktion für Nutzer, mit der iCloud Abonnenten verlorene oder verlegte iPhone, iPad, iPod touch oder Mac Geräte suchen und/oder bestimmte Massnahmen ergreifen können wie können z. B. den Modus „Verloren“ für ein Gerät aktivieren, ein Gerät sperren oder alle Einstellungen und Inhalte löschen. Weitere Informationen zu diesem Dienst sind unter <http://www.apple.com/chde/icloud/find-my-iphone.html> verfügbar. Die Standortinformationen eines Geräts, das mit der App „Mein iPhone suchen“ aufgefunden wurde, werden den Nutzern angezeigt. Apple speichert keine Datensätze mit Karten oder E-Mail Benachrichtigungen im Rahmen des Service. Gegebenenfalls sind Verbindungsprotokolle für „Mein iPhone suchen“ verfügbar. Diese können mit einer rechtsgültigen Anfrage angefordert werden. Die Verbindungsprotokolle für „Mein iPhone suchen“ sind für einen Zeitraum von etwa 30 Tagen verfügbar. Transaktionsaktivitäten für „Mein iPhone suchen“ mit Anfragen nach ferngesteuerter Sperrung oder Löschung der Inhalte eines Geräts können nur nach Eingang einer rechtsgültigen Anfrage offengelegt werden.

Apple kann diese Funktion auch auf Anfrage von Ermittlungsbehörden nicht auf den Geräten von Benutzern aktivieren. Die Funktion „Mein iPhone suchen“ muss im Voraus vom Nutzer für das relevante Gerät aktiviert worden sein. Apple speichert keine GPS Informationen konkreter Geräte oder Nutzer.

I. Extrahieren von Daten aus mit Code gesperrten iOS Geräten

Anfragen nach technischer Unterstützung beim Zugriff auf bestimmte Inhalte konkreter Geräte müssen gemäss dem MLAT-Verfahren an Apple Inc. gerichtet werden. Ermittlungsbehörden ausserhalb der USA, die diese Inhalte einsehen möchten, müssen um Rechtshilfe durch die Justizbehörden der USA ersuchen. Besteht zwischen einem Land und den USA ein Rechtshilfeabkommen („MLAT“), so kann gemäss diesem Abkommen oder durch anderweitige Kooperationen mit den Justizbehörden der USA ein rechtsgültiges Verfahren eingeleitet werden. Bei Geräten mit iOS 8.0 und neueren Betriebssystemversionen führt Apple keine iOS Datenextraktionen durch, da hier die entsprechenden Extraktionstools nicht mehr funktionieren. Die zu extrahierenden Dateien sind verschlüsselt und der Schlüssel ist an den Code des Nutzers

gebunden. Apple kennt diesen Code nicht. Bei iOS Geräten mit iOS Versionen vor iOS 8.0 kann Apple Inc. bestimmte Arten von aktiven Daten von gesperrten iOS Geräten extrahieren, sofern ein Durchsuchungsbeschluss gemäss MLAT-Verfahren vorgelegt wird. Das heisst, die vom Nutzer erstellten aktiven Dateien auf einem iOS Gerät, die in den nativen Apps von Apple enthalten sind und deren Daten nicht per Code verschlüsselt sind („nutzergenerierte aktive Dateien“), können extrahiert, auf externe Medien kopiert und den Ermittlungsbehörden ausgehändigt werden. Apple Inc. kann diesen Datenextraktionsvorgang auf iOS Geräten mit Betriebssystemversionen von iOS 4 bis iOS 7 durchführen. Hinweis: Nachdem Apple Inc. ein Durchsuchungsbeschluss gemäss dem MLAT-Verfahren vorgelegt wurde, können Ermittlungsbehörden ausschliesslich die folgenden Arten von nutzergenerierten aktiven Dateien ausgehändigt werden: SMS, iMessage, MMS, Fotos, Videos, Kontakte, Audioaufnahmen und Anruflisten. Apple Inc. kann keine Mails, Kalendereinträge oder Daten von Apps anderer Anbieter bereitstellen.

Die Datenextraktion kann ausschliesslich am Hauptsitz von Apple Inc. in Cupertino (Kalifornien, USA) und nur bei Geräten durchgeführt werden, die sich in funktionsfähigem Zustand befinden. Damit Apple Inc. bei diesem Vorgang mitwirken kann, muss der Durchsuchungsbeschluss die nachstehend benannten Formulierungen sowie die Seriennummer oder IMEI Nummer des Geräts enthalten. Weitere Informationen zum Auffinden der Seriennummer oder IMEI Nummer von iOS Geräten gibt es hier: <http://support.apple.com/kb/ht4061>.

Der Name des zuständigen Richters muss deutlich und lesbar auf dem Durchsuchungsbeschluss vermerkt sein.

Liegt den Ermittlungsbehörden ein entsprechend formulierter Durchsuchungsbeschluss vor, kann er Apple Inc. per E-Mail an subpoenas@apple.com vorgelegt werden. Das iOS Gerät für die Datenextraktion kann Apple Inc. entweder im Rahmen eines persönlichen Termins bereitgestellt oder an Apple eingeschendet werden. Das Gerät darf erst eingeschendet werden, wenn der zuständige Ermittlungsbeamte per E-Mail eine entsprechende Aufforderung von Apple erhalten hat.

Im Falle eines persönlichen Termins muss der zuständige Ermittlungsbeamte eine FireWire Festplatte mit einer Speicherkapazität von mindestens der doppelten Speicherkapazität des iOS Geräts mitbringen. Wird das Gerät eingeschendet, muss die Ermittlungsbehörde Apple eine externe Festplatte oder einen USB Speicherstick mit einer Speicherkapazität von mindestens der doppelten Speicherkapazität des iOS Geräts bereitstellen. Das Gerät darf erst eingeschendet werden, wenn die Ermittlungsbehörde eine Aufforderung hierzu per E-Mail erhalten hat.

Nach Abschluss der Datenextraktion stellen wir eine Kopie des nutzergenerierten Inhalts des Geräts bereit. Apple Inc. speichert keine Kopien der Nutzerdaten, die bei dem Vorgang extrahiert wurden. Die Beweissicherung obliegt den Ermittlungsbehörden.

Erforderliche Formulierung des Durchsuchungsbeschlusses:

„Es wird hiermit angeordnet, dass Apple Inc. [ERMITTLUNGSBEHÖRDE] bei der Durchsuchung eines Apple iOS Geräts mit Modellnr. _____, im _____ -Netz mit Zugangsnummer (Telefonnummer) _____, Seriennummer³ oder IMEI⁴ Nummer _____ und FCC ID-Nr. _____ (im Folgenden das „Gerät“) unterstützt und hierfür in angemessenem Rahmen technische Unterstützung leistet, wenn sich das Gerät in funktionsfähigem Zustand befindet und mit der Code-Schutzfunktion gesperrt wurde. Diese technische Unterstützung in angemessenem Rahmen umfasst – soweit möglich – die Extraktion von Daten auf dem Gerät, das Kopieren der Daten vom Gerät auf eine externe Festplatte oder ein anderes Speichermedium und die Rückgabe dieses Speichermediums an die Ermittlungsbehörde. Die Ermittlungsbehörde kann anschliessend die Gerätedaten auf dem bereitgestellten Speichermedium durchsuchen.

Zudem wird angeordnet, dass im Falle des Vorliegens verschlüsselter Daten auf dem Gerät Apple den Ermittlungsbehörden eine Kopie der verschlüsselten Daten aushändigen darf. Apple ist jedoch nicht verpflichtet, die Daten zu entschlüsseln oder die Ermittlungsbehörden anderweitig beim Zugriff auf die verschlüsselten Daten zu unterstützen.

Obwohl Apple angemessene Anstrengungen unternehmen muss, die Integrität der Daten auf dem Gerät zu wahren, ist Apple nicht dazu verpflichtet, im Rahmen der hiermit angeordneten Unterstützung Kopien von Nutzerdaten zu speichern. Die Beweissicherung obliegt den Ermittlungsbeamten.“

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. Diese Informationen können im Rahmen einer rechtsgültigen Anfrage und nach Vorlage einer Seriennummer (oder im Fall von iOS Geräten IMEI, MEID oder UDID) von Apple angefordert werden.

UDID: Der eindeutige Gerätebezeichner (UDID) ist eine Folge von 40 Buchstaben und Zahlen, die einem bestimmten iOS Gerät zugeordnet ist. Ein UDID kann beispielsweise wie folgt aussehen: 2j6f0ec908d137be2e1730235f5664094b831186.

Sind die Ermittlungsbehörden in Besitz des Geräts, kann eine Verbindung zwischen dem Gerät und iTunes hergestellt werden, um die UDID abzurufen. Die UDID kann in iTunes unter „Übersicht“ durch Klicken auf die Seriennummer angezeigt werden.

³ 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. Daher können bei Seriennummern, die die Buchstaben „O“ oder „I“ enthalten, keine iOS Extraktionen durchgeführt werden.

⁴ Die IMEI Nummer ist auf der Rückseite des iPad (Wi-Fi + Cellular Modell), des ursprünglichen iPhone sowie der iPhone Modelle 5, 5c, 5s, 6 und 6 Plus eingraviert. Weitere Infos unter <http://support.apple.com/kb/ht4061>. Hinweis: Bei Modellen, bei denen IMEI Nummern im Fach für die SIM Karte eingraviert sind, ist das Fach für die SIM Karte des Geräts möglicherweise nicht das passende Original, das mit dem Gerät ausgeliefert wurde.

K. Anfragen nach Überwachungsvideos aus dem Apple Store

Aufzeichnungen von Überwachungsvideos können je nach Standort des Stores variieren. Aufzeichnungen von Überwachungsvideos werden höchstens 30 Tage lang im Apple Store aufbewahrt. In vielen europäischen Ländern beträgt die Aufbewahrungsdauer je nach einschlägiger Rechtslage lediglich 24 Stunden. Nach diesem Zeitraum sind die Überwachungsvideos möglicherweise nicht mehr verfügbar. Ermittlungsbehörden können Überwachungsvideos bei jedem Apple Store anfragen. Dabei sollten die Ermittlungsbehörden Datum, Uhrzeit und die zugehörigen Transaktionsinformationen in Bezug auf das angeforderte Video 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. Verbindungsprotokolle mit IP Adressen und Transaktionsaufzeichnungen können ausschliesslich auf Grundlage einer rechtsgültigen Anfrage verfügbar gemacht 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. Diese Informationen können ausschliesslich auf Grundlage einer rechtsgültigen Anfrage verfügbar gemacht werden.

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. Verbindungsprotokolle mit IP Adressen und Transaktionsaufzeichnungen können ausschliesslich auf Grundlage einer rechtsgültigen Anfrage verfügbar gemacht werden.

O. Protokolle für Meine Apple ID und iForgot

Protokolle für Meine Apple ID and iForgot für einen Nutzer können bei Apple angefragt werden. Die Protokolle für Meine Apple ID und iForgot können Informationen über Kennworrücksetzungen enthalten. Verbindungsprotokolle mit IP Adressen und Transaktionsaufzeichnungen können ausschliesslich auf Grundlage einer rechtsgültigen Anfrage verfügbar gemacht 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 den Nutzern tatsächlich eine Kommunikation stattfand. Apple verfügt weder über Informationen darüber, ob der FaceTime Anruf erfolgreich aufgebaut wurde, noch über die Dauer eines FaceTime Anrufs. Protokolle zu FaceTime Anrufeinladungen werden bis zu 30 Tage lang gespeichert. Protokolle zu FaceTime Anrufeinladungen können ausschliesslich auf Grundlage einer rechtsgültigen Anfrage verfügbar gemacht werden.

IV. Fragen und Antworten

F: Kann ich Apple bei Fragen in Bezug auf meine Ermittlungsanfrage oder mein Rechtsverfahren kontaktieren?

A: Ja, Fragen zu anhängigen Ermittlungsanfragen können per E-Mail an law.enf.emeia@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. Je nach iOS Version des Geräts können jedoch nach Vorlage eines rechtsgültigen Durchsuchungsbeschlusses gemäss dem geltenden MLAT-Verfahren bestimmte Daten von einem gesperrten Gerät extrahiert werden. Dies ist in den vorliegenden Richtlinien beschrieben.

F: Speichert Apple GPS-Informationen, die bei Vorlage einer rechtsgültigen Anfrage bereitgestellt werden können?

A: Nein, Apple speichert den Standort von Geräten nicht.

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 Ermittlungsbehörden 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, Apple benachrichtigt betroffene Nutzer, wenn eine Ermittlungsbehörde eine rechtsgültige Informationsanfrage nach persönlichen Account-Informationen stellt, es sei denn, dass eine solche Benachrichtigung nach Ermessen von Apple wahrscheinlich die Arbeit der Justiz beeinträchtigen oder die Rechtspflege behindern würde.

F: Kann Apple mir helfen, ein gestohlenes oder verlorenes Gerät dem rechtmässigen Eigentümer zurückzugeben?

A: Finden Ermittlungsbehörden innerhalb der EMEA-Region ein potenziell gestohlenes oder verlorenes Gerät und soll es an den rechtmässigen Eigentümer zurückgegeben werden, kann eine Anfrage an uns gesendet werden: law.enf.emeia@apple.com. Dabei müssen die Seriennummer oder die IMEI Nummer des Geräts sowie alle zusätzlichen relevanten Informationen angegeben werden. Wenn Registrierungsinformationen vorhanden sind, kontaktieren wir die registrierte Person und weisen sie an, sich mit den Ermittlungsbehörden in Verbindung zu setzen.

V. Anhang A

Das „Law Enforcement Information Request“ Formular für Anfragen durch Ermittlungsbehörden in der EMEA-Region ist als bearbeitbare PDF Datei unter folgender Adresse verfügbar:

<http://www.apple.com/legal/privacy/emea-le-infrequest.pdf>

VI. Anhang B

Das „EMERGENCY Law Enforcement Information Request“ Formular für Notfall-Anfragen durch Ermittlungsbehörden ist als bearbeitbare PDF Datei unter folgender Adresse verfügbar:

<http://www.apple.com/legal/privacy/le-emergencyrequest.pdf>