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 Kunden von Geräten, Produkten und Dienstleistungen von Apple gegenüber Apple-Entitäten, 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 Kundendaten 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 Apple.com und Apple-Mediendiensten 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 betreffenden Gebiete die Verantwortung für Kundendaten im Zusammenhang mit Apple-Services.

Alle anderen Auskunftsersuchen in Bezug auf Apple Kund:innen, einschließlich Fragen von Kund:innen hinsichtlich der Offenlegung von Informationen, sind an www.apple.com/de/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 oder eines Executive Agreement unter dem Clarifying Lawful Overseas Use of Data Act („CLOUD Act Agreement“) erfolgt in Übereinstimmung mit dem ECPA. Apple stellt Inhalte von Kunden ausschließlich infolge eines derartigen rechtsgültigen Verfahrens und nur in der im Account des Kunden vorliegenden Form zur Verfügung.

Bei Auskunftsersuchen von privaten Parteien hält sich Apple an die Gesetzgebung in Bezug auf lokale Entitäten, die mit Kundendaten 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 beanstandet, angefochten oder abgelehnt.

Apple stellt der anfragenden Strafverfolgungsbehörde Antworten an die offizielle E-Mail-Adresse der anfragenden Behörde zur Verfügung. Für die gesamte Beweissicherung gemäß den Antworten von Apple ist die anfragende Strafverfolgungsbehörde verantwortlich.

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 touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, eine Reihe von Softwareprogrammen für Privat- und Geschäftskunden, die Betriebssysteme iOS und macOS X, iCloud und verschiedene Zubehör-, Dienstleistungs- und Supportangebote. Apple verkauft und vertreibt außerdem über Apple Music, App Store, Apple Books und den Mac App Store digitale Inhalte und Programme. Apple speichert Kundendaten gemäß der Datenschutzrichtlinie von Apple und den gültigen Nutzungsbedingungen für den jeweils angebotenen Service. Apple nimmt den Schutz der Privatsphäre der Kunden von Apple-Produkten und -Diensten („Apple-Kunden“) ernst. Dementsprechend werden Informationen über Apple-Kunden, außer in gesetzlich geregelten Notfallsituationen, nicht ohne korrektes Rechtsverfahren veröffentlicht.

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“ deckt 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 Mailbox senden, muss dies von einer gültigen und offiziellen E-Mail-Adresse einer Regierungs- oder Strafverfolgungsbehörde aus geschehen.

Bei Auskunftsersuchen von Ermittlungsbehörden, die bei Apple eingehen, 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 Fehlinterpretation, Einspruch, Anfechtung und/oder 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 oder eines Executive Agreement unter dem Clarifying Lawful Overseas Use of Data Act („CLOUD Act Agreement“) erfolgt in Übereinstimmung mit dem ECPA. Apple stellt Inhalte von Kunden ausschließlich infolge eines derartigen rechtsgültigen Verfahrens und nur in der im Account des Kunden vorliegenden Form zur Verfügung.

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 anfragenden 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 aus 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 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 (z. B. Numbers, Excel, Pages oder Word). Solche identifizierenden Angaben sind in der Regel erforderlich, um Informationssuchen im Zusammenhang mit Geräten, Accounts oder Finanztransaktionen durchführen zu können.

Hinweis: Aufgrund von System-Sicherheitsstandards lädt Apple keine rechtlichen Anfragen oder zugehörigen Dokumente über Links herunter, die per E-Mail gesendet wurden.

Damit Apple Kundendaten auf eine Anfrage von Strafverfolgungsbehörden offenlegen kann, muss der anfragende Beamte die Rechtsgrundlage angeben, die die Erfassung von beweiskräftigen Informationen in Form von personenbezogenen Daten durch eine Strafverfolgungsbehörde von einem Datenverantwortlichen wie Apple zulässt. Beispiele für Anfragen, die Apple für rechtsgültig hält: Production Orders (Australien, Kanada, Neuseeland), lettres de réquisition ou commissions rogatoires (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, Orders, Warrants und Communications Data Authorisations (Vereinigtes Königreich) sowie die entsprechenden Gerichtsbeschlüsse und/oder Anfragen anderer Länder.

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

Apple prüft alle rechtlichen Auskunftsersuchen sorgfältig, um sicherzustellen, dass jede Anfrage eine gültige Rechtsgrundlage besitzt. Gültigen Anfragen wird entsprochen. Wenn Apple feststellt, dass keine gültige Rechtsgrundlage vorliegt, oder eine Anfrage unklar, unangemessen oder zu weit gefasst ist, wird Apple die entsprechende Anfrage ablehnen, anfechten oder zurückweisen.

Zu Verarbeitungszwecken und aufgrund von Systembeschränkungen kann Apple keine rechtlichen Anfragen akzeptieren, die mehr als 25 Account-IDs enthalten. Wenn Strafverfolgungsbehörden rechtliche Anfragen mit mehr als 25 Account-IDs einreichen, antwortet Apple auf die ersten 25. Die Strafverfolgungsbehörden müssen neue rechtliche Anfragen für weitere IDs neu einreichen.

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). A Anfrage im Rahmen eines gegenseitigen Rechtshilfeabkommens oder eines Executive Agreement unter dem Clarifying Lawful Overseas Use of Data Act („CLOUD Act Agreement“) erfolgt in Übereinstimmung mit dem ECPA. Eine Anfrage zur Sicherstellung von Daten im Vorgriff auf eine folgende ECPA-konforme Anfrage ist per E-Mail zu richten an: 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 Kunden des betreffenden Apple-Accounts enthalten. Bei Eingang einer Anfrage zur Datensicherstellung erstellt Apple einen einmaligen Auszug der zum Anfragezeitpunkt vorhandenen angefragten Kundendaten 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. Der Versuch, mehr als zwei Anträge auf Datensicherstellung desselben Accounts zu bedienen, führt dazu, dass der zweite Antrag als Antrag auf Erweiterung der ursprünglichen Datensicherstellung und nicht als separate Sicherstellung neuer Daten behandelt wird.

D. Notfallanfragen

Apple betrachtet eine Anfrage als Notfallanfrage, wenn sie sich auf Umstände bezieht, die eine unmittelbare und ernsthafte Bedrohung für das Leben/die Sicherheit von Personen, die Sicherheit eines Staates oder die Sicherheit wichtiger Infrastrukturen/Installationen darstellen.

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 in einer Notfallanfrage die Freigabe von Informationen von Apple anzufordern, muss der:die die Anfrage stellende Regierungs- oder Ermittlungsbeamte das Formular Emergency Government & Law Enforcement Information Request ausfüllen und es direkt von der offiziellen E-Mail-Adresse der Regierungs- bzw. Strafverfolgungsbehörde aus mit Betreff „Notfallanfrage“ an die E-Mail-Adresse exigent@apple.com richten.

Wenn ein solches Notfall-Auskunftsersuchen der Regierungs- oder Strafverfolgungsbehörde (Emergency Government & Law Enforcement Information Request) zu Kundendaten gestellt wird, kann der Dienstvorgesetzte des Ermittlungsbeamten, der die Notfallanfrage eingereicht hat, kontaktiert werden, um gegenüber Apple zu 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 für eine Notfallanfrage erreichen muss, kann sich der entsprechende Mitarbeiter an das Global Security Operations Center (GSOC) von Apple unter 001 408 974-2095 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 (häufig eine Verurteilung oder ein Haftbefehl), der belegt, dass der einzuschränkende bzw. zu löschende Account rechtswidrig verwendet wurde.

Apple prüft sämtliche Anfragen von Regierungs- und Strafverfolgungsbehörden sorgfältig, um sicherzustellen, dass jede Anfrage eine gültige Rechtsgrundlage besitzt. Wenn Apple feststellt, dass keine gültige Rechtsgrundlage vorliegt, oder wenn aus dem Gerichtsbeschluss nicht hervorgeht, dass der einzuschränkende bzw. zu löschende Account rechtswidrig betrieben wurde, wird Apple den Antrag ablehnen/anfechten.

Wenn Apple einen zufriedenstellenden Gerichtsbeschluss oder einen gleichwertigen inländischen Rechtsvorgang (häufig eine Verurteilung oder ein Haftbefehl) von der Regierungs- oder Strafverfolgungsbehörde erhält, der belegt, dass der einzuschränkende bzw. zu löschende Account rechtswidrig 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 Kunden

Apple informiert betroffene Kunden, wenn deren Apple-Accountinformationen 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 eine solche Benachrichtigung 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 solche Benachrichtigung nicht den zugrundeliegenden Tatsachen des Falls entspricht.

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 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.

Apple informiert seine Kunden, wenn deren Apple-Account infolge eines Apple zugestellten Gerichtsbeschlusses (häufig 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.

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

Grundlegende Registrierungs- oder Kundendaten, einschließlich Name, Adresse, E-Mail-Adresse und Telefonnummer, werden Kund:innen von Apple bei der Registrierung eines Apple Geräts vor iOS 8 und macOS Sierra 10.12 zur Verfügung gestellt. Apple überprüft diese Informationen nicht, und sie sind möglicherweise nicht korrekt oder spiegeln den Eigentümer des Geräts nicht wider. 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. Aufnahme können Registrierungsinformationen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers 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. Wenn eine rechtliche Anfrage fünf oder mehr Seriennummern enthält, benötigt Apple diese Seriennummern außerdem in einem editierbaren elektronischen Format (z. B. Numbers, Excel, Pages oder Word).

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 Antragstellers abgefragt werden.

C. Apple-Mediendienste

App Store, Apple Music, Apple TV App, Apple Podcasts und Apple Books („Apple-Mediendienste“) sind Softwareanwendungen, die Kunden zum Organisieren und Abspielen von Apps, digitaler Musik und Videos sowie zum Streamen von Inhalten verwenden. Apple-Mediendienste stellen auch Inhalte für Kunden zum Download für ihre Computer und iOS-Geräte bereit. Beim Eröffnen eines Apple-Accounts kann der Kunde grundlegende Kundeninformationen wie Name, Wohnanschrift, E-Mail-Adresse und Telefonnummer angeben. Zudem sind ggf. Informationen zu Kauf-/Downloadtransaktionen und -verbindungen, Verbindungen zum Zweck von Aktualisierung/erneutem

Download über Apple-Mediendienste verfügbar. Angaben zu IP-Adressen können auf die letzten 18 Monate beschränkt sein. Sofern verfügbar, können Apple-Mediendienst-Kundeninformationen und Verbindungsprotokolle mit IP-Adressen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

Anfragen nach Apple-Mediendienst-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 die entsprechenden Apple-Mediendienst-Kundeninformationen in Form des vollständigen Namens **und** der Telefonnummer und/oder des vollständigen Namens **und** der Wohnanschrift, um den entsprechenden Account des Apple-Mediendienst-Kunden identifizieren zu können. Regierungs- oder Ermittlungsbeamte können auch eine gültige Apple-Mediendienst-Auftragsnummer oder eine vollständige Debit- oder Kreditkartennummer, mit der Apple-Mediendienst-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.

Hinweis: Insoweit Ihre rechtliche Anfrage vollständige Kredit- bzw. Debitkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument (PDF und editierbares Format, z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen. Darüber hinaus lädt Apple aufgrund von System-Sicherheitsstandards keine Dokumente zu rechtlichen Anfragen über Links herunter, die per E-Mail gesendet wurden.

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 Antragstellers 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 Antragstellers abgefragt werden.

Hinweis: Insoweit Ihre rechtliche Anfrage vollständige Kredit- bzw. Debitkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument (PDF und editierbares Format, z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen. Darüber hinaus lädt Apple aufgrund von System-Sicherheitsstandards keine Dokumente zu rechtlichen Anfragen über Links herunter, die per E-Mail gesendet wurden.

E. Bestellungen bei Apple.com

Apple pflegt Informationen über Online-Bestellungen bei apple.com. Diese können unter anderem den Namen des Käufers, die Versandadresse, die Telefonnummer, die E-Mail-Adresse, gekaufte Produkte,

den Kaufbetrag und die beim Kauf verwendete IP-Adresse umfassen. Auskunftsersuchen hinsichtlich Online-Bestellungen bei apple.com im müssen eine vollständige Kredit- bzw. Debitkartennummer oder eine Auftragsnummer 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 Online-Bestellungen bei apple.com 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 Kundeninformationen 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 Kaufinformationen zu Online-Bestellungen bei apple.com über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

Hinweis: Insoweit Ihre rechtliche Anfrage vollständige Kredit- bzw. Debitkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument (PDF und editierbares Format, z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen. Darüber hinaus lädt Apple aufgrund von System-Sicherheitsstandards keine Dokumente zu rechtlichen Anfragen über Links herunter, die per E-Mail gesendet wurden.

F. Geschenkkarten

Apple Store-Karten und App Store & iTunes-Karten haben eine Seriennummer. Diese Seriennummern haben verschiedene Formate, die unter anderem vom Design und/oder dem Ausstellungsdatum abhängen. Apple kann verfügbare Informationen zu Apple Store-Karten sowie App Store & iTunes-Karten als Antwort auf die entsprechende rechtsgültige Anfrage für das Land des Antragstellers bereitstellen. Wenn eine rechtliche Anfrage 5 oder mehr Seriennummern von Geschenkkarten enthält, müssen diese Seriennummern in einem passwortgeschützten/verschlüsselten Dokument (z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen.

i. Apple Store-Geschenkkarten

Apple Store-Karten können für Einkäufe bei Apple.com oder in einem Apple Store verwendet werden. 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-Karte möglicherweise stornieren oder sperren. Dies hängt vom Status der betroffenen Karte ab. Sofern verfügbar, können Informationen über Apple Store-Karten über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

Hinweis: Insoweit Ihre rechtliche Anfrage Apple Store-Geschenkkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument (PDF und editierbares Format, z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen. Darüber hinaus lädt Apple aufgrund von System-Sicherheitsstandards keine Dokumente zu rechtlichen Anfragen über Links herunter, die per E-Mail gesendet wurden.

ii. App Store & iTunes-Karten

App Store & iTunes-Karten können in Apple Music, App Store, Apple Books und im Mac App Store verwendet werden. Anhand der Seriennummer kann Apple bestimmen, ob die App Store & iTunes-Karte aktiviert (d. h. an einer Einzelhandels-Verkaufsstelle gekauft) oder eingelöst wurde (d. h. auf das Guthaben eines Apple-Accounts aufgebucht).

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

Hinweis: Insoweit Ihre rechtliche Anfrage vollständige App Store & iTunes-Geschenkkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument (PDF und editierbares Format, z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen. Darüber hinaus lädt Apple aufgrund von System-Sicherheitsstandards keine Dokumente zu rechtlichen Anfragen über Links herunter, die per E-Mail gesendet wurden.

G. Apple Pay

Apple Pay-Transaktionen, die bei Einzelhändlern (z. B. für NFC/kontaktlose Kommunikation) und in Apps oder Online-Verkaufsstellen erfolgen, werden auf dem Gerät des Kunden sicher authentifiziert und in verschlüsselter Form an den Händler oder den Zahlungsabwickler des Händlers gesendet. Während die Transaktionssicherheit von einem Apple Server verifiziert wird, verarbeitet Apple weder Zahlungen noch werden diese Transaktionen oder die vollständigen Kredit-/Debitkartennummern für Einkäufe mit Apple Pay gespeichert. Diese Informationen können über die jeweilige Ausgabebank, das Zahlungsnetzwerk oder den Händler erhältlich sein.

Weitere Informationen über Länder und Regionen, die Apple Pay unterstützen, finden sich in support.apple.com/de-de/HT207957.

Zur Anforderung von Transaktionsdaten für Einkäufe, die an Apple Store-Standorten oder bei Apple.com getätigt wurden, benötigt Apple die primäre Kontonummer des Geräts (DPAN), die für die Transaktion verwendet wurde. Die DPAN hat 16 Stellen und kann von der ausstellenden Bank bezogen werden. Hinweis: Die DPAN wird für Kontaktloszahlungen an den Händler anstelle der tatsächlichen Kredit-/Debitkartennummer verwendet (FPAN/Funding PAN). Die DPAN wird vom Zahlungsabwickler in die jeweilige FPAN umgewandelt. Mit den relevanten DPAN-Informationen kann Apple möglicherweise eine angemessene Suche durchführen, um entsprechende Informationen über sein POS-System zu finden. Sofern verfügbar, können diese Informationen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

Apple kann möglicherweise Apple Pay-Informationen über die Art(en) der Kredit-/Debitkarte(n), die ein Kunde zu Apple Pay hinzugefügt hat, zusammen mit Kundendaten zur Verfügung stellen. Sofern verfügbar, können diese Informationen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden. Um solche Informationen

anzufordern, benötigt Apple eine Gerätekennung (Apple-Seriennummer, SEID, IMEI oder MEID) oder eine Apple-ID/-Account-E-Mail-Adresse.

Hinweis: Insoweit Ihre rechtliche Anfrage die DPAN enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument (PDF und editierbares Format, z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen. Darüber hinaus lädt Apple aufgrund von System-Sicherheitsstandards keine Dokumente zu rechtlichen Anfragen über Links herunter, die per E-Mail gesendet wurden.

H. iCloud

iCloud ist der Cloud-Service von Apple, mit dem Kund:innen von all ihren Geräten aus auf Fotos, Dokumente und mehr zugreifen können. Mit iCloud haben Kund:innen außerdem die Möglichkeit, ihre iOS und iPadOS Geräte in iCloud zu sichern. Mit dem iCloud Service können Kund:innen einen iCloud.com-E-Mail-Account einrichten. iCloud E-Mail-Domains können @icloud.com, @me.com und @mac.com lauten. Alle iCloud-Inhaltsdaten, die von Apple gespeichert werden, sind am Serverstandort verschlüsselt. Für Daten, die Apple entschlüsseln kann, verwahrt Apple die Verschlüsselungsschlüssel in den Rechenzentren in den USA. Apple erhält und speichert keine Verschlüsselungsschlüssel für die End-to-End-verschlüsselten Daten der Kund:innen.

iCloud ist ein kundenbasierter 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 Kundeninformationen in Form des vollständigen Namens **und** der Telefonnummer und/oder des vollständigen Namens **und** der Wohnanschrift, um den entsprechenden Apple-Account identifizieren zu können. Wenn nur eine Telefonnummer oder Apple-ID/-Account-E-Mail-Adresse angegeben ist, können verfügbare Informationen für verifizierte Accounts, die mit diesen Kriterien verknüpft sind, bereitgestellt werden.

I. Folgende Informationen sind ggf. in iCloud verfügbar:

I. Kundendaten

Wenn ein:e Kund:in einen iCloud Account einrichtet, kann er Apple grundlegende Kundendaten wie Name, Wohnanschrift, E-Mail-Adresse und Telefonnummer angeben. Zudem sind ggf. Verbindungsinformationen zu iCloud Funktionen verfügbar. iCloud Kundendaten und Verbindungsprotokolle mit IP-Adressen können ggf. über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden. Verbindungsprotokolle werden bis zu 25 Tage lang gespeichert.

II. Mailprotokolle

Mailprotokolle enthalten Aufzeichnungen eingehender und ausgehender Mitteilungen wie Uhrzeit, Datum, E-Mail-Adressen des Absenders und Empfänger-E-Mail-Adressen. iCloud Mailprotokolle werden bis zu 25 Tage aufbewahrt und können ggf. über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers 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 Kunde für die Pflege im Account ausgewählt hat, während der Account des Kunden aktiv bleibt. Apple behält gelöschte Inhalte nicht bei, nachdem sie von den Servern von Apple gelöscht wurden. iCloud Inhalte können E-Mails, gespeicherte Fotos, Dokumente, Kontakte, Kalender, Lesezeichen, den Safari Browserverlauf, den Karten-Suchverlauf, Nachrichten und Backups von iOS Geräten umfassen. Backups von iOS Geräten können Fotos und Videos in den Aufnahmen, Geräteeinstellungen, App-Daten, iMessage, Business Chat, SMS und MMS sowie Voicemail enthalten. Alle iCloud-Inhaltsdaten, die von Apple gespeichert werden, sind am Serverstandort verschlüsselt. Für Daten, die Apple entschlüsseln kann, verwahrt Apple die Verschlüsselungsschlüssel in den Rechenzentren in den USA. Apple erhält und speichert keine Verschlüsselungsschlüssel für die End-to-End-verschlüsselten Daten der Kund:innen.

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 oder eines Executive Agreement unter dem Clarifying Lawful Overseas Use of Data Act („CLOUD Act Agreement“) erfolgt in Übereinstimmung mit dem ECPA. Apple stellt Inhalte von Kunden ausschließlich infolge eines solchen rechtsgültigen Auskunftsersuchens und nur in der im Account des Kunden vorliegenden Form zur Verfügung.

II. Erweiterter Datenschutz

Erweiterter Datenschutz für iCloud ist eine Funktion, die End-to-End-Verschlüsselung verwendet, um iCloud Daten mit Apples höchster Datensicherheit zu schützen. Für Nutzer:innen, die den erweiterten Datenschutz für iCloud aktivieren, sind möglicherweise eingeschränkte iCloud Daten verfügbar. Weitere Informationen zum erweiterten Datenschutz finden Sie im Web unter support.apple.com/de-de/guide/security/advanced-data-protection-for-icloud-sec973254c5f/ und unter support.apple.com/de-de/HT212520.

Die folgenden Informationen sind möglicherweise in iCloud verfügbar, wenn Nutzer:innen den erweiterten Datenschutz für iCloud aktiviert haben:

a. Kundendaten
Wenn ein:e Kund:in einen iCloud Account einrichtet, kann er Apple grundlegende Kundendaten wie Name, Wohnanschrift, E-Mail-Adresse und Telefonnummer angeben. Zudem sind ggf. Verbindungsinformationen zu iCloud Funktionen verfügbar. Sofern verfügbar, können iCloud Kundendaten und Verbindungsprotokolle mit IP-Adressen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden. Verbindungsprotokolle werden bis zu 25 Tage lang gespeichert.

b. Mailprotokolle
Mailprotokolle enthalten Aufzeichnungen eingehender und ausgehender Mitteilungen wie Uhrzeit, Datum, E-Mail-Adressen des Absenders und Empfänger-E-Mail-Adressen. iCloud Mailprotokolle werden bis zu 25 Tage aufbewahrt und können ggf. über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

C. E-Mail-Inhalte und andere iCloud Inhalte

Für Nutzer:innen, die den erweiterten Datenschutz aktiviert haben, speichert iCloud Inhalte für E-Mails, Kontakte und Kalender, die der:die Kund:in für die Pflege im Account ausgewählt hat, während der Account des:der Kund:in aktiv bleibt. Diese Daten können, sofern sie im Kundenaccount vorhanden sind, mit der entsprechenden rechtsgültigen Anfrage für das Land des Antragstellers bereitgestellt werden. Diese eingeschränkten Daten werden von Apple gespeichert und zusätzlich am Serverstandort verschlüsselt. Für Daten, die Apple entschlüsseln kann, verwahrt Apple die Verschlüsselungsschlüssel in den Rechenzentren in den USA. Apple erhält und speichert keine Verschlüsselungsschlüssel für die End-to-End-verschlüsselten Daten der Kund:innen.

Für den erweitertem Datenschutz wird eine End-to-End-Verschlüsselung verwendet, und Apple kann bestimmte iCloud Inhalte nicht entschlüsseln, einschließlich Fotos, iCloud Drive, Backup, Notizen und Safari Lesezeichen. Unter bestimmten Umständen verwahrt Apple möglicherweise eingeschränkte Informationen zu diesen iCloud Services, die ggf. über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden können.

III. iCloud Privat-Relay

iCloud Privat-Relay ist ein Datenschutzservice im Internet, der im Rahmen eines iCloud + Abonnements angeboten wird. Privat-Relay schützt das Surfen im Internet in Safari, DNS-Abfragen (Domain Name Space) und unverschlüsseltem HTTP-App-Datenverkehr. Nutzer:innen müssen über ein iCloud + Abonnement und ein Gerät mit iOS 15, iPadOS 15 oder macOS Monterey (macOS 12) oder neuer verfügen, um iCloud Privat-Relay nutzen zu können. Weitere Informationen zu Privat-Relay finden Sie unter support.apple.com/de-de/HT212614 und www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.

Wenn Privat-Relay aktiviert ist, werden Webbrowsing-Anfragen von Nutzer:innen über zwei separate, sichere Internetrelays versendet. Die Nutzer-IP-Adresse ist für den Netzwerkanbieter der Nutzer:innen und für das erste Relay, das von Apple betrieben wird, sichtbar. Die DNS-Einträge der Nutzer:innen sind verschlüsselt, sodass keine Partei die Adresse der Website sehen kann, die der:die Nutzer:in aufrufen möchte. Das zweite Relay, das von einem externen Inhaltsanbieter betrieben wird, generiert eine temporäre IP-Adresse, entschlüsselt den Namen des:der angeforderten Websitenutzer:in und verbindet den:die Nutzer:in mit der Website. Privat-Relay überprüft, ob der Client, der sich verbindet, ein iPhone, iPad oder Mac ist. Privat-Relay ersetzt die ursprüngliche IP-Adresse der Nutzer:innen durch eine Adresse, die aus dem vom Service verwendeten IP-Adressbereich zugewiesen wurde. Die zugewiesene Relay-IP-Adresse kann von mehreren Privat-Relay-Nutzer:innen im selben Bereich gemeinsam genutzt werden.

Wenn Privat-Relay für private Webbrowsing-Anfragen verwendet wird, ist Apple nicht in der Lage, die Client-IP-Adresse oder den entsprechenden Nutzeraccount anhand der Privat-Relay IP-Adressen zu ermitteln. Apple hat keine Informationen bezüglich der Apple ID, die der Privat-Relay IP-Adresse zugeordnet ist.

Hinweis: iCloud Privat-Relay ist nicht in allen Ländern oder Regionen verfügbar. Wenn Privat-Relay aktiviert ist und Nutzer:innen an einen Ort reisen, an dem Privat-Relay nicht verfügbar ist, wird es automatisch deaktiviert und wieder aktiviert, wenn sich die Nutzer:innen wieder in einem Land oder einer Region befinden, in dem bzw. der es unterstützt wird.

I. Wo ist?

„Wo ist?“ ist eine Funktion für Nutzer, mit der iCloud-Kunden verlorene oder verlegte iPhone-, iPad-, iPod touch-, Apple Watch-, Mac-Geräte, AirPods oder AirTags 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 Service finden Sie unter www.apple.com/de/icloud/find-my/.

Damit ein Kunde, der sein Gerät verloren hat, die Funktion „Wo ist?“ verwenden kann, muss diese bereits vor dem Verlust auf dem betroffenen Gerät aktiviert gewesen sein. Ein Aktivieren der Funktion „Wo ist?“ ist nach dem Verlust des Geräts nicht mehr per Fernsteuerung oder auf Anfrage von Regierungs- oder Strafverfolgungsbehörden möglich. 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 „Wo ist?“ aufgefunden wurde, werden den Kunden angezeigt. Apple speichert keine Inhalte mit Karten oder Benachrichtigungen im Rahmen des Dienstes. Der folgende Supportlink liefert Informationen und Maßnahmen, die Kund:innen bei Verlust oder Diebstahl eines iOS Geräts ergreifen können: support.apple.com/kb/ HT201472.

Verbindungsprotokolle zu „Wo ist?“ stehen für einen Zeitraum von bis zu 25 Tagen zur Verfügung. Sind sie verfügbar, können sie über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden. Sofern verfügbar, können Transaktionsaktivitäten zu „Wo ist?“ zum Zwecke von Anfragen zum ferngesteuerten Sperren oder Löschen eines Geräts über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

J. AirTag und „Wo ist?“-Netzwerk-Zubehörprogramm

Mit der App „Wo ist?“ auf dem iPhone, iPad, iPod touch und Mac können Kunden einfach persönliche Gegenstände finden, indem sie einen AirTag daran befestigen oder ein Produkt verwenden, das Teil des „Wo ist?“-Netzwerk-Zubehörprogramms ist.

Mit AirTag und iOS 14.5 bzw. macOS 11.3 oder höher erhalten Kund:innen mithilfe der App „Wo ist? “ Unterstützung bei der Suche nach verloren gegangenen persönlichen Gegenständen (Schlüssel, Rucksäcke, Gepäck usw.). AirTag muss sich in Bluetooth-Reichweite des gekoppelten iPhone-, iPad- oder iPod touch-Geräts befinden, um einen Ton abspielen oder die Genaue Suche mit kompatiblen iPhone-Modellen verwenden zu können. Wenn sich das AirTag nicht in der Nähe seines Besitzers befindet, kann der ungefähre Standort des AirTag angegeben werden, sofern sich das AirTag in Reichweite eines Geräts im „Wo ist?“-Netzwerk befindet, das aus mehreren hundert Millionen Apple-Geräten auf der ganzen Welt besteht. Weitere Informationen finden Sie unter: support.apple.com/de-de/HT212227 und support.apple.com/de-de/HT210967.
Das „Wo ist?“-Netzwerk-Zubehörprogramm öffnet das Programm „Wo ist?“ für Produkte von Drittanbietern (Fahrräder, Kopfhörer usw.), damit Kund:innen die Möglichkeit haben, ihre unterstützten Produkte von Drittanbietern mit der App „Wo ist?“ mit iOS 14.3 und macOS 11.1 oder neuer zu suchen.

Um AirTag oder unterstützte Produkte von Drittanbietern zum Tab „Objekte“ in der App „Wo ist? “ hinzuzufügen, müssen Kunden über eine Apple-ID verfügen, in ihrem iCloud-Account mit aktivierter Funktion „Wo ist?“ angemeldet sein und ihr AirTag oder ihre unterstützten Produkte von Drittanbietern mit ihrer Apple-ID registrieren. Die Interaktion ist Ende-zu-Ende-verschlüsselt und Apple kann den Standort eines AirTag oder von unterstützten Produkten von Drittanbietern nicht einsehen. Weitere Informationen finden Sie unter support.apple.com/de-de/HT211331.

Mit einer Seriennummer kann Apple möglicherweise die Daten des gekoppelten Accounts als Antwort auf das ordnungsgemäße und rechtsgültige Auskunftsersuchen für das Land des Antragstellers

bereitstellen. Der AirTag-Kopplungsverlauf ist für einen Zeitraum von bis zu 25 Tagen verfügbar. Der folgende Supportlink liefert Informationen zur Ermittlung einer AirTag-Seriennummer: support.apple.com/de-de/HT211658.

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. Wenn eine rechtliche Anfrage fünf oder mehr Seriennummern enthält, benötigt Apple diese Seriennummern außerdem in einem editierbaren elektronischen Format (z. B. Numbers, Excel, Pages oder Word).

K. 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 werkseitig 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.

L. IP-Adressanfrage

Vor der Aufnahme eines Rechtsverfahrens mit einer IP-Adresse als Bezeichner fordert Apple die Strafverfolgungsbehörden auf, sich zu vergewissern, dass es sich bei der betreffenden IP-Adresse nicht um eine öffentliche oder eine Router-IP-Adresse handelt und dafür keine Carrier-Grade Network Address Translation (CGNAT) verwendet wird, und Apple gegenüber im Rahmen des Rechtsverfahrens zu bestätigen, dass es sich um eine nicht öffentliche IP-Adresse handelt. Darüber hinaus müssen derartige Anfragen eine Datumsbeschränkung von maximal drei Tagen umfassen. Als Reaktion auf eine derartige Anfrage ist Apple möglicherweise in der Lage, Verbindungsprotokolle (siehe unten, Abschnitt III.Q) zu erstellen, in denen Strafverfolgungsbehörden möglicherweise einen bestimmen Apple Account/eine bestimmte Apple ID identifizieren und diese in einem anschließenden Gerichtsverfahren als Bezeichner verwenden können. Sofern verfügbar, können Apple Kundendaten auf Basis einer IP-Adresse über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

M. 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 MAC-Adressinformationen abrufen. Sofern verfügbar, können diese über ein ordnungsgemäßes und rechtsgültiges

Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

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

O. Game Center

Game Center ist das soziale Spielenetzwerk von Apple. Ggf. sind für Kund:innen oder ein Gerät Informationen zu Game Center-Verbindungen verfügbar. Sofern verfügbar, können Verbindungsprotokolle über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

P. iOS-Geräteaktivierung

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

Dual SIM: Für Geräte mit Dual SIM können Informationen des Mobilfunkanbieters für die Nano-SIM und/oder eSIM, falls verfügbar, mit dem entsprechenden rechtsgültigen Antrag für das Land des Antragstellers bezogen werden. Eine eSIM ist eine digitale SIM, die Kunden ermöglicht, einen Mobilfunktarif von ihrem Mobilfunkanbieter zu aktivieren, ohne auf eine physische Nano-SIM-Karte angewiesen zu sein. Weitere Informationen finden Sie unter support.apple.com/de-de/HT209044. In Festlandchina, Hongkong und Macao verfügen iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone XS Max und iPhone XR über Dual SIM mit zwei Nano-SIM-Karten.

Q. Verbindungsprotokolle

Verbindungsaktivitäten für einen Kunden oder ein Gerät mit Apple Services wie Apple Music, Apple TV App, Apple Podcasts, Apple Books, iCloud, „Meine Apple ID“ und Apple Diskussionen können, sofern verfügbar von Apple bezogen werden. Sofern verfügbar, können diese Verbindungsprotokolle mit IP-Adressen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

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

Protokolle für „Meine Apple-ID“ und iForgot für einen Kunden 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 Antragstellers abgefragt werden.

S. FaceTime

Die FaceTime-Kommunikation ist durchgehend verschlüsselt. Apple verfügt über keine Möglichkeit FaceTime-Daten zu entschlüsseln, die zwischen Geräten gesendet werden. Apple kann die FaceTime-Kommunikation nicht abfangen. Apple verfügt über Protokolle, die Daten über die Einleitung von FaceTime-Anrufeinladungen enthalten. Diese Protokolle geben keinen Aufschluss darüber, ob zwischen Kunden tatsächlich eine Kommunikation stattfand. Protokolle zu FaceTime-Anrufeinladungen werden bis zu 25 Tage lang gespeichert. Sofern verfügbar, können Protokolle zu FaceTime-Anrufeinladungen über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

T. iMessage

Die Kommunikation über iMessage ist durchgehend verschlüsselt. Apple verfügt über keine Möglichkeit, iMessage-Daten zu entschlüsseln, die zwischen Geräten gesendet werden. Apple kann die iMessage-Kommunikation nicht 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 gesucht wird (z. B. Telefonnummer, E-Mail-Adresse oder Apple ID), um festzustellen, ob dieses nachgeschlagene Element für iMessage geeignet ist. Die Abfrageprotokolle zur iMessage Fähigkeit geben keinen Aufschluss darüber, ob zwischen Kund:innen tatsächlich eine Kommunikation stattfand. Anhand der Abfrageprotokolle zur iMessage-Fähigkeit kann Apple nicht bestimmen, ob eine tatsächliche iMessage-Kommunikation erfolgte. Apple kann außerdem nicht nachvollziehen, welche Anwendung die Abfrage tatsächlich initiiert hat. Die Abfrageprotokolle zur iMessage Fähigkeit sind keine Bestätigung dafür, dass ein iMessage Ereignis tatsächlich versucht wurde. Die Abfrageprotokolle zur iMessage Fähigkeit werden bis zu 25 Tage aufbewahrt. Sofern verfügbar, können Abfrageprotokolle zur iMessage Fähigkeit über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

U. iMessage

Mit der Apple TV App können Kunden TV-Sendungen und Filme von Apple TV+, Apple TV Channels sowie Apps und Dienste von anderen Anbietern durchsuchen, kaufen, abonnieren und wiedergeben. Der Kauf- und Download-Verlauf kann verfügbar sein.

Anfragen nach Apple TV App-Kundendaten 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 Kundeninformationen in Form des vollständigen Namens und der Telefonnummer und/oder des vollständigen Namens und der Wohnanschrift, um den entsprechenden Kundenaccount identifizieren zu können. Regierungs- oder Ermittlungsbeamte können auch eine gültige Apple-Auftragsnummer oder eine vollständige Debit- oder Kreditkartennummer vorlegen, mit der Apple TV App-Käufe getätigt wurden. In Verbindung mit diesen Parametern kann auch ein Kundenname angegeben werden. Der Kundenname allein reicht zur Offenlegung der Informationen jedoch nicht aus.

Hinweis: Insoweit Ihre rechtliche Anfrage vollständige Kredit- bzw. Debitkartendaten enthält, sollten diese Angaben aus Datenschutzgründen in einem passwortgeschützten/verschlüsselten Dokument (PDF und editierbares Format, z. B. Numbers, Excel, Pages oder Word) an lawenforcement@apple.com

übermittelt werden. Das Passwort ist in einer separaten E-Mail mitzuteilen. Darüber hinaus lädt Apple aufgrund von System-Sicherheitsstandards keine Dokumente zu rechtlichen Anfragen über Links herunter, die per E-Mail gesendet wurden.

V. Mit Apple anmelden

„Mit Apple anmelden" ist eine privatere Möglichkeit für Kunden, sich bei Apps und Websites von Drittanbietern mit ihrer vorhandenen Apple-ID anzumelden. Über die Taste „Mit Apple anmelden" auf einer teilnehmenden App oder Website kann ein Kunde einen Account einrichten und sich mit seiner Apple-ID anmelden. Anstatt einen Social Media-Account zu verwenden oder Formulare auszufüllen und ein neues Passwort zu wählen, kann ein Kunde einfach auf die Taste „Mit Apple anmelden" tippen, seine Informationen überprüfen und sich schnell und sicher mit Face ID, Touch ID oder seinem Gerätepasswort anmelden. Weitere Informationen finden Sie unter support.apple.com/de-de/HT210318.

„E-Mail-Adresse verbergen" ist ein Feature von „Mit Apple anmelden". Es verwendet den privaten E-Mail-Relay-Dienst von Apple, um eine eindeutige, zufällige E-Mail-Adresse zu erstellen, die E-Mails an die private E-Mail-Adresse eines Kunden weiterleitet. Grundlegende Kundendaten können über ein ordnungsgemäßes und rechtsgültiges Auskunftsersuchen für das Land des Antragstellers abgefragt werden.

IV.Häufig gestellte Fragen

Q: Kann ich Fragen zu meinem Auskunftsersuchen im Zuge eines Ermittlungsverfahrens per E-Mail an Apple richten?
A: Ja, Fragen oder Anfragen zu behördlichen Rechtsvorgängen können per E-Mail an folgende Adresse geschickt werden: lawenforcement@apple.com.

Q: 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.

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

Q: Kann Apple mir helfen, ein verloren gegangenes oder gestohlenes Gerät dem:der rechtmäßigen Eigentümer:in zurückzugeben?
A: Wenden Sie sich in einem solchen Fall an lawenforcement@apple.com. Bitte geben Sie in Ihrer E-Mail die Seriennummer des Geräts (oder ggf. die IMEI) sowie weitere relevante Informationen an. Informationen zum Finden der Seriennummer finden Sie hier: support.apple.com/de-de/HT204308.

Wenn die entsprechenden Kundeninformationen verfügbar sind, nimmt Apple Kontakt mit dem Kunden auf und nennt Kontaktdaten der entsprechenden Dienststelle, um das Gerät zurückzuerhalten. Wenn sich der Kunde jedoch nicht anhand der verfügbaren Daten ermitteln lässt, werden Sie angewiesen, eine rechtsgültige Anfrage zu stellen.

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

Q: 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.

Q: Werden die entsprechenden Kund:innen 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.