Linee guida per le procedure legali

Autorità governative e forze dell'ordine al di fuori degli Stati Uniti

Queste linee guida sono destinate ad autorità governative e forze dell'ordine al di fuori degli Stati Uniti nei casi in cui vi sia l'esigenza di richiedere informazioni sui clienti e sulle clienti di servizi, prodotti e dispositivi Apple alle entità Apple nell'area geografica o nel Paese di pertinenza. Apple aggiornerà le presenti Linee guida laddove necessario.

Nelle presenti Linee guida, per Apple si intende l'entità competente responsabile delle informazioni sui clienti e sulle clienti in una determinata area geografica o in un determinato Paese. In qualità di azienda globale, Apple è articolata in svariate entità legali in diverse giurisdizioni e tali entità legali sono responsabili dei dati personali che raccolgono e che vengono elaborati per loro conto da Apple Inc. Ad esempio, le informazioni sui punti vendita negli enti di vendita al dettaglio di Apple al di fuori degli Stati Uniti sono controllate dai singoli enti in ogni Paese. I dati personali correlati a Apple.com e ai Servizi multimediali di Apple possono essere controllati anche da entità legali al di fuori degli Stati Uniti, come illustrato nei termini di ciascun servizio nell'ambito di una specifica giurisdizione. Solitamente le entità legali di Apple al di fuori degli Stati Uniti in Australia, Canada, Irlanda e Giappone sono responsabili dei dati dei clienti e delle clienti correlati ai servizi Apple nell'ambito delle rispettive aree geografiche.

Tutte le altre richieste di informazioni riguardanti i clienti e le clienti Apple, incluse le domande di tali clienti relative alla divulgazione delle informazioni, devono essere inviate attraverso la pagina www.apple.com/it/privacy/contact/. Le presenti Linee guida non si applicano alle richieste da parte di autorità governative e forze dell'ordine degli Stati Uniti nei confronti di Apple Inc.

Per le richieste di informazioni da parte di autorità governative e forze dell'ordine, Apple si attiene alle leggi applicabili alle entità globali che controllano i dati aziendali e fornisce eventuali dettagli secondo i requisiti di legge. Fatta eccezione per le situazioni di emergenza (definite di seguito nella sezione Richieste di emergenza), tutte le richieste di contenuti da parte di autorità governative e forze dell'ordine al di fuori degli Stati Uniti devono essere conformi alle leggi applicabili, inclusa la legge ECPA (Electronic Communications Privacy Act) statunitense. Una richiesta nell'ambito di un trattato bilaterale di assistenza giudiziaria o di un accordo esecutivo secondo il Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") è conforme alla legge ECPA. Apple fornirà i contenuti presenti negli account dei clienti e delle clienti solo a fronte di un atto giudiziario legalmente valido.

Per le richieste provenienti da soggetti privati, Apple si attiene alle leggi applicabili alle entità che controllano i dati dei clienti e delle clienti e fornisce tali dati secondo i requisiti di legge.

Apple ha centralizzato il processo di ricezione, tracciamento, elaborazione e risposta per le richieste legalmente legittime ricevute da autorità governative, forze dell'ordine e soggetti privati, dal momento della ricezione fino all'invio della risposta. Un team qualificato dell'ufficio Affari legali di Apple esamina e valuta tutte le richieste ricevute. Vengono contestate o rifiutate tutte le richieste che, secondo quanto stabilito da Apple, risultano prive di una valida base legale oppure ambigue, inappropriate

o eccessivamente generiche.

Apple fornisce le risposte alle forze dell'ordine all'indirizzo email ufficiale del funzionario o della funzionaria richiedente. La conservazione di tutte le prove in base alle risposte fornite da Apple è responsabilità delle forze dell'ordine che ne fanno richiesta.

INDICE

I. Informazioni generali

Apple progetta, realizza e commercializza dispositivi mobili multimediali e di comunicazione, computer e lettori musicali digitali portatili, oltre a vendere una vasta gamma di articoli correlati a tali prodotti: software, servizi, periferiche, soluzioni di networking, contenuti e applicazioni digitali di terze parti. I prodotti e i servizi Apple includono Mac, iPhone, iPad, iPod touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, una gamma di applicazioni software per uso domestico e professionale, i sistemi operativi iOS e macOS X, iCloud e svariati accessori, servizi e opzioni di assistenza. Inoltre Apple vende e fornisce applicazioni e contenuti digitali attraverso Apple Music, App Store, Apple Books e Mac App Store. Le informazioni sui clienti e sulle clienti vengono conservate da Apple in conformità alla politica sulla privacy di Apple e ai termini di servizio applicabili per ciascun servizio offerto. Apple si impegna a salvaguardare la privacy dei clienti e delle clienti dei prodotti e servizi Apple ("Clienti Apple"). Di conseguenza, salvo quanto previsto dalla legge per le situazioni di emergenza, le informazioni sui clienti e sulle clienti Apple non saranno divulgate senza un atto giudiziario legalmente valido.

Le informazioni contenute in queste Linee guida sono destinate alle autorità governative e alle forze dell'ordine al di fuori degli Stati Uniti per definire la procedura legale richiesta da Apple per poter divulgare informazioni in formato elettronico alle autorità governative e alle forze dell'ordine al di fuori degli Stati Uniti. Le Linee guida non hanno lo scopo di fornire consulenza legale. La sezione delle domande frequenti ("Domande frequenti") delle presenti Linee guida contiene le risposte ad alcune delle domande che Apple riceve più spesso. Né le Linee guida né le Domande frequenti coprono tutte le possibili circostanze che potrebbero verificarsi.

In caso di ulteriori domande, inviare un'email all'indirizzo lawenforcement@apple.com.

L'indirizzo email di cui sopra è destinato esclusivamente all'uso da parte del personale delle autorità governative e delle forze dell'ordine. Qualsiasi email inviata al suddetto indirizzo deve provenire da un indirizzo email valido e ufficiale delle forze dell'ordine o di autorità governative.

Le richieste legali di informazioni che Apple riceve devono riguardare un particolare dispositivo oppure un particolare cliente o una particolare cliente Apple e i servizi specifici che Apple ha fornito a tale cliente. Apple può fornire informazioni su un dispositivo o su un cliente o una cliente dell'azienda finché è ancora in possesso di tali informazioni, nel rispetto delle proprie politiche sulla conservazione dei dati. Apple conserva i dati come definito di seguito in alcune parti della sezione "Informazioni rese disponibili". Tutti gli altri dati sono conservati solo per il periodo necessario agli scopi indicati nella nostra politica sulla privacy. Al fine di evitare errori di interpretazione e casi di obiezione, contestazione e/o rifiuto, si chiede alle autorità governative e alle forze dell'ordine di non inviare richieste ambigue, inappropriate oppure eccessivamente vaghe o generiche. Fatta eccezione per le situazioni di emergenza (definite di seguito nella sezione Richieste di emergenza), tutte le richieste di contenuti da parte di autorità governative e forze dell'ordine al di fuori degli Stati Uniti devono essere conformi alle leggi applicabili, inclusa la legge ECPA (Electronic Communications Privacy Act) statunitense. Una richiesta nell'ambito di un trattato bilaterale di assistenza giudiziaria o di un accordo esecutivo secondo il Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") è conforme alla legge ECPA. Apple fornirà i contenuti presenti negli account dei clienti e delle clienti solo a fronte di un atto giudiziario legalmente valido.

Nessuna informazione contenuta in queste Linee guida intende definire diritti esigibili nei confronti di Apple; inoltre, le politiche di Apple possono essere soggette ad aggiornamenti e modifiche senza previa comunicazione alle autorità governative o alle forze dell'ordine.

II. Richieste legali nei confronti di Apple

A. Richieste di informazioni da parte di autorità governative e forze dell'ordine

Apple accetta la notifica di richieste di informazioni legalmente valide inviate tramite email da autorità governative o forze dell'ordine, purché tali richieste siano state trasmesse da un indirizzo email ufficiale dell'autorità che le inoltra. Il personale delle autorità governative e delle forze dell'ordine al di fuori degli Stati Uniti che inoltra a Apple una richiesta di informazioni deve compilare il modulo Government & Law Enforcement Information Request (Richiesta di informazioni da parte di autorità governative e forze dell'ordine) da trasmettere direttamente dall'indirizzo email ufficiale dell'autorità in questione all'indirizzo lawenforcement@apple.com.

L'indirizzo email di cui sopra è destinato esclusivamente all'uso da parte del personale delle autorità governative e delle forze dell'ordine. Laddove le richieste contengano cinque o più identificativi, come numeri di serie/IMEI di dispositivi, ID Apple, indirizzi email o numeri di ordini/fatture, dovranno essere trasmesse in formato modificabile (ad esempio Numbers, Excel, Pages o documento Word). Gli identificativi come quelli riportati sopra sono solitamente richiesti per cercare informazioni riguardanti dispositivi, account o transazioni finanziarie.

Nota: nel rispetto degli standard di sicurezza di sistema, Apple non scarica le richieste legali o la relativa documentazione da link inviati tramite email.

Affinché Apple possa divulgare le informazioni sui clienti e sulle clienti a fronte di una richiesta da parte delle forze dell'ordine, è necessario che il funzionario o la funzionaria che inoltra la richiesta indichi la base legale che autorizza l'autorità in questione a raccogliere i dati probativi sotto forma di dati personali da un soggetto titolare del trattamento come Apple. Esempi di richieste che Apple considera legalmente valide sono: Production Order (Australia, Canada, Nuova Zelanda), lettres de réquisition ou commissions rogatoires (Francia), Solicitud Datos (Spagna), Ordem Judicial (Brasile), Auskunftsersuchen (Germania), Obligation de dépôt (Svizzera), 個人情報の開示依頼 (Giappone), Personal Data Request, Order, Warrant e Communications Data Authorisation (Regno Unito), oltre alle richieste e/o alle ordinanze di tribunali equivalenti provenienti da altri Paesi.

B. Gestione delle richieste di informazioni da parte di autorità governative e forze dell'ordine e invio della risposta

Apple esamina attentamente tutte le richieste legali per verificare che abbiano una valida base legale e ottempera alle richieste legalmente valide. Vengono contestate o rifiutate tutte le richieste che, secondo quanto stabilito da Apple, risultano prive di una valida base legale oppure ambigue, inappropriate o eccessivamente generiche.

Per finalità di trattamento e in virtù delle limitazioni dei sistemi, Apple non può accettare richieste legali contenenti più di 25 identificativi di account. Se l'autorità inoltra una richiesta legale con più di 25 identificativi di account, Apple risponderà ai primi 25 e l'autorità dovrà inoltrare una nuova richiesta legale per gli identificativi aggiuntivi.

C. Richieste di conservazione

Fatta eccezione per le situazioni di emergenza (definite di seguito nella sezione Richieste di

emergenza), tutte le richieste di contenuti da parte di autorità governative e forze dell'ordine al di fuori degli Stati Uniti devono essere conformi alle leggi applicabili, inclusa la legge ECPA (Electronic Communications Privacy Act) statunitense. Una richiesta nell'ambito di un trattato bilaterale di assistenza giudiziaria o di un accordo esecutivo secondo il Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") è conforme alla legge ECPA. Eventuali richieste di conservazione dei dati in vista di imminenti richieste ai sensi della legge ECPA devono essere trasmesse tramite email all'indirizzo lawenforcement@apple.com.

Tali richieste devono includere ID Apple/indirizzo email dell'account pertinente oppure nome completo **e** numero di telefono e/o nome completo **e** indirizzo fisico del cliente o della cliente titolare dell'account Apple in questione. Una volta ricevuta una richiesta di conservazione, Apple effettua un'estrazione una tantum dei dati del cliente o della cliente richiesti, disponibili al momento della richiesta, e li conserva per 90 giorni. Trascorsi 90 giorni, i dati conservati saranno automaticamente rimossi dal server di archiviazione. Tuttavia, è possibile prorogare tale periodo di ulteriori 90 giorni inoltrando una nuova richiesta. Il tentativo di sottoporre più di due richieste di conservazione per lo stesso account comporterà il trattamento della seconda richiesta come una richiesta di proroga della richiesta di conservazione originale e non come una richiesta di conservazione distinta relativa a nuovi dati.

D. Richieste di emergenza

Apple considera richieste di emergenza quelle legate a circostanze che implicano una seria e imminente minaccia per la vita/sicurezza di persone, la sicurezza di uno stato o la sicurezza di infrastrutture/ impianti di importanza critica.

Se il funzionario o la funzionaria dell'autorità governativa o delle forze dell'ordine che invia la richiesta è in grado di confermare in modo soddisfacente che tale richiesta è legata a una o più delle circostanze di emergenza sopra indicate, Apple la esaminerà con la massima priorità.

Per richiedere a Apple di divulgare volontariamente le informazioni sulla base di una circostanza di emergenza, il funzionario o la funzionaria dell'autorità governativa o delle forze dell'ordine richiedente deve compilare il modulo Emergency Government & Law Enforcement Information Request (Richiesta di emergenza da parte di autorità governative e forze dell'ordine) da trasmettere direttamente dall'indirizzo email ufficiale dell'autorità in questione all'indirizzo exigent@apple.com inserendo la dicitura "Emergency Request" (Richiesta di emergenza) nell'oggetto dell'email.

Qualora autorità governative o forze dell'ordine desiderino ricevere dati su un cliente o una cliente a fronte di un'apposita richiesta di informazioni d'emergenza, è possibile che venga contattato/a un superiore o una superiore del funzionario o della funzionaria che ha inoltrato la richiesta a Apple per avere la conferma che si tratti di una richiesta legittima. Il funzionario o la funzionaria dell'autorità governativa o delle forze dell'ordine che invia la richiesta di informazioni di emergenza deve fornire nella richiesta stessa anche le informazioni di contatto di un superiore o una superiore.

Qualora le autorità governative o le forze dell'ordine abbiano la necessità di contattare Apple per una richiesta di informazioni di emergenza, possono rivolgersi al Global Security Operations Center (GSOC) di Apple al numero 001 408 974-2095. Questo numero di telefono offre un servizio di risposta in più lingue.

E. Richieste di limitazione/cancellazione di account

Qualora autorità governative o forze dell'ordine richiedano che l'ID Apple di un cliente o una cliente venga limitato/cancellato, Apple dovrà richiedere un'ordinanza del tribunale, o altro atto giudiziario equivalente nel Paese in questione (solitamente una sentenza di condanna, un mandato o un'ingiunzione), a dimostrazione del fatto che l'account da limitare/cancellare è stato utilizzato in modo illecito.

Apple esamina attentamente tutte le richieste provenienti da autorità governative e forze dell'ordine per verificare che abbiano una valida base legale. Qualora Apple stabilisca che non vi è alcuna valida base legale oppure l'ordinanza del tribunale non dimostri che l'account da limitare/cancellare è stato utilizzato in modo illecito, la richiesta verrà rifiutata/contestata.

Qualora Apple riceva dall'autorità governativa o dalle forze dell'ordine un'ordinanza del tribunale accettabile, o altro atto giudiziario equivalente nel Paese in questione (solitamente una sentenza di condanna, un mandato o un'ingiunzione), a dimostrazione del fatto che l'account da limitare/cancellare è stato utilizzato in modo illecito, Apple provvederà ad agire come richiesto per limitare/cancellare l'account in osservanza dell'ordinanza del tribunale, dandone quindi comunicazione al funzionario o alla funzionaria richiedente.

F. Notifica ai clienti e alle clienti

Quando Apple riceve, da autorità governative o forze dell'ordine, una richiesta legalmente valida di fornire informazioni su un account Apple, provvede a informare il cliente o la cliente in questione, eccetto nei casi in cui: a) tale azione sia esplicitamente vietata dalla richiesta legalmente valida, da un'ordinanza del tribunale ricevuta da Apple o dalla legge vigente in materia; b) Apple, a sua propria discrezione, ritenga che da ciò deriverebbe un rischio di lesioni o morte per una persona identificabile; c) sussista una situazione di potenziale rischio per un minore o una minore; d) tale azione non sia richiesta dalle circostanze del caso.

Dopo 90 giorni, Apple invierà una notifica differita per le richieste di informazioni di emergenza eccetto nei casi in cui: a) tale azione sia esplicitamente vietata da un'ordinanza del tribunale o dalla legge vigente in materia; b) Apple, a sua propria discrezione, ritenga che da ciò deriverebbe un rischio di lesioni o morte per una persona o gruppo di persone identificabile; c) sussista una situazione di potenziale rischio per un minore o una minore. Apple invierà una notifica differita dopo il termine del periodo di riservatezza specificato in un'ordinanza del tribunale eccetto nei casi in cui: a) Apple, a sua propria discrezione, ritenga ragionevolmente che da ciò deriverebbe un rischio di lesioni o morte per una persona o gruppo di persone identificabile; b) sussista una situazione di potenziale rischio per un minore o una minore; c) tale azione non sia richiesta dalle circostanze del caso.

Apple comunicherà ai propri clienti e alle proprie clienti la limitazione/cancellazione del rispettivo account Apple a seguito di ricezione da parte di Apple di un'ordinanza del tribunale (solitamente una sentenza di condanna, un mandato o un'ingiunzione) a dimostrazione del fatto che l'account da limitare/cancellare è stato utilizzato in modo illecito o in violazione dei Termini di servizio di Apple, eccetto nei casi in cui: a) tale azione sia vietata dall'atto giudiziario stesso, da un'ordinanza del tribunale ricevuta da Apple o dalla legge vigente in materia; b) sussista una situazione di potenziale rischio per un minore o una minore; c) Apple, a sua propria discrezione, ritenga ragionevolmente che da ciò deriverebbe un rischio di lesioni o morte per una persona o gruppo di persone identificabile; d) tale azione non sia richiesta dalle circostanze del caso.

III. Informazioni rese disponibili da Apple

In questa sezione sono descritti, in generale, i tipi di informazioni che possono essere rese disponibili da Apple al momento della pubblicazione delle presenti Linee guida.

A. Registrazione di dispositivi

Quando un cliente o una cliente registra un dispositivo Apple con sistema operativo precedente ad iOS 8 e macOS Sierra 10.12, Apple riceve alcune informazioni di base sul cliente stesso o sulla cliente stessa e sulla registrazione, tra cui nome, indirizzo fisico, indirizzo email e numero di telefono. Poiché Apple non provvede a verificarle, tali informazioni potrebbero essere inesatte e non corrispondere all'effettivo proprietario o all'effettiva proprietaria del dispositivo. Per i dispositivi con iOS 8 e versioni successive e per i Mac con macOS Sierra 10.12 e versioni successive, le informazioni sulla registrazione vengono raccolte quando il cliente o la cliente associa un dispositivo a un ID Apple di iCloud. Tali informazioni potrebbero essere inesatte e non corrispondere all'effettivo proprietario o all'effettiva proprietaria del dispositivo. È possibile ottenere le informazioni sulla registrazione, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Per i numeri di serie dei dispositivi, Apple utilizza le cifre 0 (zero) e 1 (uno) anziché le lettere "O" e "I".
Le richieste relative a numeri di serie contenenti le lettere "O" e "I" non daranno alcun risultato. Qualora una richiesta legale includa cinque o più numeri di serie, Apple richiede che tali numeri di serie siano inviati anche in formato elettronico modificabile (ad esempio Numbers, Excel, Pages o documento Word).

B. Archivi del servizio clienti

Apple può fornire informazioni sui contatti avuti dagli utenti e dalle utenti con il servizio clienti Apple in merito a un dispositivo o servizio. Queste informazioni possono contenere anche i dati sulle interazioni con i clienti e le clienti riguardanti l'assistenza offerta per un particolare dispositivo o servizio Apple. Inoltre, possono essere rese disponibili anche le informazioni relative a dispositivo, garanzia e riparazione. È possibile ottenere tali informazioni, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

C. Servizi multimediali di Apple

App Store, Apple Music, l'app Apple TV, Apple Podcasts e Apple Books ("Servizi multimediali di Apple") sono applicazioni software che i clienti e le clienti usano per organizzare ed eseguire le app, riprodurre contenuti audio/video digitali e trasmettere contenuti in streaming. I Servizi multimediali di Apple offrono inoltre contenuti che i clienti e le clienti possono scaricare sui loro computer e dispositivi iOS. Al momento della creazione di un account Apple, il cliente o la cliente può fornire alcune informazioni di base, tra cui nome, indirizzo fisico, indirizzo email e numero di telefono. Inoltre, possono essere disponibili anche informazioni relative a connessioni e transazioni di acquisto/download e connessioni per aggiornamenti/download ripetuti dei Servizi multimediali di Apple. Le informazioni relative agli indirizzi IP possono essere limitate agli ultimi 18 mesi. È possibile ottenere le informazioni sui clienti e sulle clienti dei Servizi multimediali di Apple e i registri delle connessioni con gli indirizzi IP, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Le richieste di dati riguardanti i Servizi multimediali di Apple devono includere l'identificativo del dispositivo Apple (numero di serie, IMEI, MEID o GUID) oppure l'indirizzo email dell'account/ID Apple pertinente. Se non si conosce l'indirizzo email dell'account/ID Apple, è necessario fornire a Apple le informazioni sul cliente o sulla cliente dei Servizi multimediali di Apple sotto forma di nome completo **e** numero di telefono (e/o nome completo **e** indirizzo fisico) per consentire l'identificazione dell'account del cliente o della cliente dei Servizi multimediali di Apple. I funzionari e le funzionarie delle autorità governative o delle forze dell'ordine possono fornire anche un numero d'ordine valido dei Servizi multimediali di Apple oppure il numero completo di una carta di credito o debito associata agli acquisti di Servizi multimediali di Apple. Oltre a questi parametri può essere fornito anche il nome del cliente o della cliente; tuttavia quest'ultimo dato, da solo, non è sufficiente per ottenere le informazioni.

Nota: per le richieste legali contenenti dati completi riguardanti carte di credito/debito, è necessario (per motivi di sicurezza) che tali dati siano trasmessi in un documento protetto da password/codificato (.PDF e formato modificabile, ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e che la password venga fornita in un'email separata. Inoltre, nel rispetto degli standard di sicurezza di sistema, Apple non scarica le richieste legali o la relativa documentazione da link inviati tramite email.

D. Transazioni presso gli Apple Store

Le transazioni del punto vendita sono quelle effettuate presso gli Apple Store con pagamento in contanti oppure tramite carta di credito/debito o carta regalo. Le richieste relative ai registri di un punto vendita devono includere il numero completo della carta di credito/debito utilizzata e possono includere anche informazioni aggiuntive come ora e data della transazione, importo e articoli acquistati. È possibile ottenere le informazioni riguardanti il tipo di carta associata a un determinato acquisto, il nome dell'acquirente, l'indirizzo email, l'ora/la data della transazione, l'importo della transazione e la sede dello store, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Le richieste di duplicati delle ricevute devono includere il numero della transazione Retail associata agli acquisti ed è possibile ottenere i duplicati, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Nota: per le richieste legali contenenti dati completi riguardanti carte di credito/debito, è necessario (per motivi di sicurezza) che tali dati siano trasmessi in un documento protetto da password/codificato (.PDF e formato modificabile, ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e che la password venga fornita in un'email separata. Inoltre, nel rispetto degli standard di sicurezza di sistema, Apple non scarica la documentazione relativa a richieste legali da link inviati tramite email.

E. Ordini su Apple.com

Per gli acquisti effettuati online su Apple.com, Apple conserva informazioni che possono includere: nome dell'acquirente, indirizzo di spedizione, numero di telefono, indirizzo email, prodotti acquistati, importo e indirizzo IP degli acquisti. Le richieste di informazioni sugli ordini effettuati online su Apple.com devono includere un numero completo di carta di credito/debito oppure un numero d'ordine o il numero di serie dell'articolo acquistato. Oltre a questi parametri può essere fornito anche il nome del cliente o della cliente; tuttavia quest'ultimo dato, da solo, non è sufficiente per ottenere le informazioni. In alternativa, le richieste di informazioni sugli ordini effettuati online su Apple.com possono includere l'indirizzo email dell'account/ID Apple pertinente. Se non si conosce l'indirizzo email dell'account/ID Apple, Apple richiede le informazioni sul cliente o sulla cliente sotto forma di

nome completo **e** numero di telefono (e/o nome completo **e** indirizzo fisico) per identificare l'account Apple oggetto della richiesta. È possibile ottenere le informazioni sugli acquisti per gli ordini effettuati online su Apple.com, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Nota: per le richieste legali contenenti dati completi riguardanti carte di credito/debito, è necessario (per motivi di sicurezza) che tali dati siano trasmessi in un documento protetto da password/codificato (.PDF e formato modificabile, ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e che la password venga fornita in un'email separata. Inoltre, nel rispetto degli standard di sicurezza di sistema, Apple non scarica la documentazione relativa a richieste legali da link inviati tramite email.

F. Carte regalo

Le carte regalo Apple Store e le carte regalo App Store & iTunes hanno un numero di serie. Il formato del numero di serie varia in funzione di fattori quali design e/o data di emissione. Apple può fornire le informazioni disponibili relativamente alle carte regalo Apple Store e alle carte regalo App Store & iTunes a fronte di apposita richiesta legalmente valida nel Paese del richiedente o della richiedente. Per le richieste legali contenenti cinque o più numeri di serie delle carte regalo, Apple richiede che tali numeri di serie siano trasmessi in un documento protetto da password/codificato (ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e che la password venga fornita in un'email separata.

i. Carte regalo Apple Store

Le carte regalo Apple Store possono essere utilizzate per acquisti su Apple.com o in un Apple Store. Le informazioni disponibili possono includere informazioni sull'acquirente della carta regalo (se acquistata da Apple anziché da un rivenditore di terze parti), le transazioni di acquisto associate e gli articoli acquistati. In alcuni casi, Apple può essere in grado di annullare o sospendere una carta regalo Apple Store, a seconda dello stato della carta in questione. È possibile ottenere le informazioni sulle carte regalo Apple Store, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Nota: per le richieste legali contenenti dati completi riguardanti carte regalo Apple Store, è necessario (per motivi di sicurezza) che i dati della carta regalo Apple Store siano trasmessi in un documento protetto da password/codificato (.PDF e formato modificabile, ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e la password venga fornita in un'email separata. Inoltre, nel rispetto degli standard di sicurezza di sistema, Apple non scarica la documentazione relativa a richieste legali da link inviati tramite email.

ii. Carte regalo App Store & iTunes

Le carte regalo App Store & iTunes possono essere utilizzate in Apple Music, App Store, Apple Books e Mac App Store. Attraverso il numero di serie, Apple è in grado di stabilire se una carta regalo App Store & iTunes è stata attivata (acquistata presso un punto vendita) o utilizzata (aggiunta al saldo del credito presso lo store di un account Apple).
Dopo che una carta regalo App Store & iTunes è stata attivata, le informazioni disponibili possono includere il nome del punto vendita, la sede, la data e l'ora. Dopo che una carta

regalo App Store & iTunes è stata utilizzata, le informazioni disponibili possono includere i dati della persona titolare dell'account Apple correlato, la data e l'ora di attivazione e/o utilizzo e l'indirizzo IP di utilizzo. In alcuni casi, Apple può essere in grado di disattivare una carta regalo App Store & iTunes, a seconda dello stato della carta in questione. È possibile ottenere le informazioni sulle carte regalo App Store & iTunes, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Nota: per le richieste legali contenenti dati completi riguardanti carte regalo App Store & iTunes, è necessario (per motivi di sicurezza) che tali dati siano trasmessi in un documento protetto da password/codificato (.PDF e formato modificabile, ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e che la password venga fornita in un'email separata. Inoltre, nel rispetto degli standard di sicurezza di sistema, Apple non scarica la documentazione relativa a richieste legali da link inviati tramite email.

G. Apple Pay

Le transazioni effettuate con Apple Pay presso un punto vendita fisico (ad esempio per comunicazioni NFC/contactless) e nelle app o presso un punto vendita online vengono autenticate in modo sicuro sul dispositivo del cliente o della cliente e inviate in forma codificata al rivenditore o al gestore di servizi di pagamento del rivenditore. Benché la sicurezza delle transazioni venga verificata da un server Apple, Apple non elabora i pagamenti e non memorizza tali transazioni né i numeri completi delle carte di credito/debito associate agli acquisti effettuati con Apple Pay. Tali informazioni possono essere disponibili tramite le banche di emissione, la rete di pagamento o il rivenditore in questione.

Per ulteriori informazioni sui Paesi e sulle aree geografiche in cui è supportato Apple Pay, visitare la pagina support.apple.com/it-it/HT207957.

Per richiedere i dati delle transazioni per gli acquisti effettuati presso gli Apple Store o su Apple.com, Apple richiede il codice DPAN (Device Primary Account Number) utilizzato per la transazione. Il codice DPAN è composto da 16 cifre e può essere richiesto alla banca di emissione. Nota: il codice DPAN è usato nelle transazioni di pagamento contactless con il rivenditore al posto del numero effettivo della carta di credito/debito (FPAN/Funding PAN). Il codice DPAN è convertito nel FPAN corrispondente dal gestore di servizi di pagamento. Con le informazioni sul codice DPAN rilevante, Apple può effettuare una ricerca ragionevole per individuare le informazioni richieste tramite il sistema del punto vendita. È possibile ottenere le informazioni, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Apple può fornire le informazioni su Apple Pay relative al tipo o ai tipi di carta di credito/debito che un cliente o una cliente ha aggiunto a Apple Pay insieme alle informazioni sul cliente o sulla cliente. È possibile ottenere tali informazioni, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente. Per richiedere tali informazioni, occorre fornire a Apple un identificativo del dispositivo (numero di serie Apple, SEID, IMEI o MEID) oppure un indirizzo email dell'account/ID Apple.

Nota: per le richieste legali contenenti il codice DPAN, è necessario (per motivi di sicurezza) che tali dati siano trasmessi in un documento protetto da password/codificato (.PDF e formato modificabile, ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e che la password venga fornita in un'email separata. Inoltre, nel rispetto degli standard di sicurezza di sistema, Apple non scarica la documentazione relativa a richieste legali da link inviati tramite email.

H. iCloud

iCloud è il servizio cloud di Apple con cui i clienti e le clienti possono accedere ai loro contenuti (ad esempio, foto, documenti e molto altro) da tutti i loro dispositivi. I clienti e le clienti possono utilizzare iCloud anche per effettuare il backup dei loro dispositivi iOS e iPadOS. Con il servizio iCloud, i clienti e le clienti possono configurare un account email iCloud.com. I domini di posta elettronica di iCloud possono essere @icloud.com, @me.com e @mac.com. Tutti i dati memorizzati da Apple su iCloud sono codificati e archiviati presso la sede del server. Per i dati che Apple può decodificare, Apple conserva le chiavi di codifica nei propri data center negli Stati Uniti. Apple non riceve né conserva le chiavi di codifica per i dati crittografati end-to-end del cliente o della cliente.

iCloud è un servizio customer-based. Le richieste relative ai dati di iCloud devono includere l'indirizzo email dell'account/ID Apple pertinente. Se non si conosce l'indirizzo email dell'account/ID Apple, Apple richiede le informazioni sul cliente o sulla cliente sotto forma di nome completo **e** numero di telefono (e/o nome completo **e** indirizzo fisico) per identificare l'account Apple oggetto della richiesta. Laddove venga fornito solamente un numero di telefono o un indirizzo email dell'account/ID Apple, possono essere fornite le informazioni disponibili per gli account verificati associati a tali criteri.

I. Possono essere rese disponibili le seguenti informazioni di iCloud:

I. Informazioni sul cliente o sulla cliente

Per configurare un account iCloud, l'utente può fornire a Apple alcune informazioni di base, come nome, indirizzo fisico, indirizzo email e numero di telefono. Possono essere rese disponibili anche le informazioni relative alle connessioni con il servizio iCloud.

È possibile ottenere le informazioni sui clienti e sulle clienti di iCloud e i registri delle connessioni con gli indirizzi IP, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente. I registri delle connessioni vengono conservati per un massimo di 25 giorni.

II. Registri di posta

I registri di posta contengono alcuni dati sulle comunicazioni in entrata e in uscita: ora, data, indirizzi di posta elettronica di mittente e persona a cui è destinata l'email. I registri di posta di iCloud vengono conservati per un massimo di 25 giorni e, se disponibili, possono essere ottenuti con l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

III. Contenuti della posta elettronica e altri contenuti di iCloud, Il mio streaming foto, Libreria foto di iCloud, iCloud Drive, Contatti, Calendari, Preferiti, cronologia di navigazione di Safari, cronologia delle ricerche di Mappe, Messaggi, backup dei dispositivi iOS

iCloud archivia i contenuti relativi ai servizi che il cliente o il cliente ha scelto di conservare su tale account per tutto il tempo in cui quest'ultimo rimane attivo. Apple non conserva i contenuti eliminati una volta che sono stati cancellati dai server Apple. I contenuti di iCloud possono includere email, foto, documenti, contatti, calendari, segnalibri, cronologia di navigazione di Safari, cronologia delle ricerche di Mappe, Messaggi e backup dei dispositivi

iOS che sono stati archiviati. Tali backup i possono includere foto e video del rullino foto, impostazioni del dispositivo, dati delle app, iMessage, Business Chat, SMS, MMS e messaggi della segreteria telefonica. Tutti i dati memorizzati da Apple su iCloud sono codificati e archiviati presso la sede del server. Per i dati che Apple può decodificare, Apple conserva le chiavi di codifica nei propri data center negli Stati Uniti. Apple non riceve né conserva le chiavi di codifica per i dati crittografati end-to-end del cliente o della cliente.

Fatta eccezione per le situazioni di emergenza (definite in precedenza nella sezione Richieste di emergenza), tutte le richieste di contenuti da parte di autorità governative e forze dell'ordine al di fuori degli Stati Uniti devono essere conformi alle leggi applicabili, inclusa la legge ECPA (Electronic Communications Privacy Act) statunitense. Una richiesta nell'ambito di un trattato bilaterale di assistenza giudiziaria o di un accordo esecutivo secondo il Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") è conforme alla legge ECPA. Apple fornirà i contenuti presenti negli account dei clienti e delle clienti solo a fronte di una richiesta legalmente valida.

II. Protezione avanzata dei dati

La protezione avanzata dei dati per iCloud è una funzione che utilizza la crittografia end-to-end per proteggere i dati di iCloud con il massimo livello di sicurezza dei dati offerto da Apple. Per coloro che abilitano la protezione avanzata dei dati per iCloud, potrebbero essere disponibili dati limitati di iCloud. Maggiori informazioni sulla protezione avanzata dei dati sono disponibili su support.apple.com/it-it/guide/security/sec973254c5f/web e support.apple.com/it-it/HT212520.

Le seguenti informazioni possono essere rese disponibili da iCloud se l'utente ha abilitato la protezione avanzata dei dati per iCloud:

a. Informazioni sul cliente o sulla cliente
Per configurare un account iCloud, l'utente può fornire a Apple alcune informazioni di base, come nome, indirizzo fisico, indirizzo email e numero di telefono. Possono essere rese disponibili anche le informazioni relative alle connessioni con il servizio iCloud. È possibile ottenere le informazioni sui clienti e sulle clienti di iCloud e i registri delle connessioni con gli indirizzi IP, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente. I registri delle connessioni vengono conservati per un massimo di 25 giorni.

b. Registri di posta
I registri di posta contengono alcuni dati sulle comunicazioni in entrata e in uscita: ora, data, indirizzi di posta elettronica di mittente e persona a cui è destinata l'email. I registri di posta di iCloud vengono conservati per un massimo di 25 giorni e, se disponibili, possono essere ottenuti con l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

c. Contenuti della posta elettronica e altri contenuti di iCloud
Se l'utente abilita la protezione avanzata dei dati, iCloud archivia i contenuti relativi a email, contatti e calendari che l'utente ha scelto di conservare nell'account fintanto che l'account stesso rimane attivo. Questi dati possono essere forniti così come sono nell'account del cliente o della cliente, a seguito di un'apposita richiesta legalmente valida per il Paese di chi ha presentato tale richiesta. Tali dati vengono archiviati da Apple e, inoltre, vengono codificati presso la sede in cui si trova il server. Per i dati che Apple può decodificare, Apple conserva le chiavi di codifica nei propri data center negli Stati Uniti. Apple non riceve né conserva le chiavi di codifica per i dati crittografati end-to-end del cliente o della cliente.

La protezione avanzata dei dati utilizza la crittografia end-to-end e Apple non può decodificare alcuni contenuti di iCloud, tra cui Foto, iCloud Drive, Backup, Note e segnalibri di Safari. In alcune circostanze, Apple può conservare informazioni limitate relative a questi servizi iCloud, che possono essere ottenute, se disponibili, con apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

III. Relay privato iCloud

Relay privato iCloud è un servizio per la privacy su internet compreso nell'abbonamento iCloud+. Relay privato protegge la navigazione web dell'utente in Safari, le query di risoluzione DNS (Domain Name Space) e il traffico http delle app non codificato. Per utilizzare Relay privato iCloud, l'utente deve avere un abbonamento iCloud+ e un dispositivo con iOS 15, iPadOS 15 o macOS Monterey (macOS 12) o versioni successive. Maggiori informazioni su Relay privato sono disponibili su support.apple.com/it-it/HT212614 e www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.

Quando Relay privato è abilitato, le richieste di navigazione web di ogni utente vengono inviate tramite due relay internet separati e protetti. L'indirizzo IP dell'utente è visibile al provider di rete dell'utente e al primo relay, gestito da Apple. I dati DNS di ogni utente sono codificati, quindi nessuna delle parti può vedere l'indirizzo del sito web che l'utente sta cercando di visitare. Il secondo relay, gestito da un fornitore di contenuti di terze parti, genera un indirizzo IP temporaneo, decodifica il nome del sito web che l'utente ha richiesto e connette tale utente al sito. Relay privato verifica che il client che si connette sia un iPhone, iPad o Mac. Relay privato sostituisce l'indirizzo IP originale dell'utente con uno assegnato dall'intervallo di indirizzi IP utilizzati dal servizio. L'indirizzo IP assegnato può essere condiviso tra più utenti di Relay privato nella stessa area.

Nel caso in cui le richieste di navigazione web utilizzino Relay privato, Apple non è in grado di determinare l'indirizzo IP del client dell'utente o l'account dell'utente corrispondente sulla base degli indirizzi IP di Relay privato. Apple non ha informazioni da fornire in merito all'ID Apple associato all'indirizzo IP di Relay privato.

Nota: Relay privato iCloud non è disponibile in tutti i Paesi o le aree geografiche. Se l'utente ha abilitato Relay privato e si reca in un luogo in cui questa funzione non è disponibile, Relay privato verrà disattivato automaticamente e si riattiverà al rientro dell'utente in un Paese o in un'area geografica che lo supporta.

I. Dov'è

Dov'è è una funzione attivabile dall'utente, che consente ai clienti e alle clienti di iCloud di individuare i propri iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac o AirTag smarriti o rubati e/o di compiere alcune azioni sul dispositivo (ad esempio, impostarlo sulla modalità smarrito, bloccarlo o inizializzarlo). Per ulteriori informazioni su questo servizio, visitare la pagina www.apple.com/it/icloud/find-my/.

Affinché Dov'è funzioni nel caso in cui un cliente o una cliente abbia smarrito il proprio dispositivo, è necessario che sia stata attivata sul dispositivo in questione prima dello smarrimento. Non è possibile attivare la funzione Dov'è su un dispositivo dopo che quest'ultimo è stato smarrito, da remoto oppure su richiesta di autorità governative o forze dell'ordine. Le informazioni sui servizi di localizzazione di un dispositivo sono memorizzate su ogni singolo dispositivo; Apple non può recuperare tali informazioni da uno specifico dispositivo. Le informazioni sui servizi di localizzazione di un dispositivo individuato tramite la funzione Dov'è sono destinate alla visualizzazione da parte del cliente o della cliente; Apple non dispone dei contenuti delle mappe né degli avvisi inviati attraverso il servizio. Attraverso il

seguente link di supporto, è possibile accedere a informazioni utili e alle procedure che un cliente o una cliente può eseguire in caso di smarrimento o furto di un dispositivo iOS: support.apple.com/it-it/HT201472.

I registri delle connessioni relative alla funzione Dov'è sono disponibili per un periodo massimo di 25 giorni e, se disponibili, possono essere ottenuti attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente. Per ottenere informazioni sulle attività transazionali della funzione Dov'è in relazione a richieste di blocco o inizializzazione da remoto di un dispositivo, se disponibili, è necessario presentare una richiesta legalmente valida nel Paese del richiedente o della richiedente.

J. AirTag e Find My Network Accessory Program

L'app Dov'è su iPhone, iPad, iPod touch e Mac permette ai clienti e alle clienti di localizzare oggetti personali agganciandovi un AirTag o utilizzando un prodotto del Find My Network Accessory Program.

Con AirTag, iOS 14.5 e macOS 11.3 o versioni successive, i clienti e le clienti possono ricevere assistenza nella ricerca di oggetti personali smarriti (chiavi, zaini, valigie ecc.) usando l'app Dov'è. Per emettere un suono o per utilizzare Posizione precisa con i modelli iPhone compatibili, l'AirTag deve trovarsi nel raggio di azione del Bluetooth dell'iPhone, iPad o iPod touch associato. Se non si trova nelle vicinanze del proprietario o della proprietaria, è possibile ottenere la posizione approssimativa dell'AirTag se questo si trova nel raggio di azione di un dispositivo della rete di Dov'è, costituita da centinaia di milioni di dispositivi Apple nel mondo. Ulteriori informazioni sono disponibili su: support.apple.com/it-it/HT212227 e support.apple.com/it-it/HT210967.

Il Find My Network Accessory Program consente l'utilizzo della rete Dov'è ai prodotti di produttori di terze parti (biciclette, cuffie ecc.), in modo che i clienti e le clienti possano localizzare i prodotti di terze parti supportati tramite l'app Dov'è con iOS 14.3 e macOS 11.1 o versioni successive.

Per aggiungere un AirTag o prodotti di terze parti supportati al pannello Oggetti nell'app Dov'è, i clienti e le clienti devono avere un ID Apple, accedere al loro account iCloud con la funzione Dov'è attivata e registrare l'AirTag o i prodotti di terze parti supportati sul proprio ID Apple. L'interazione è protetta da crittografia end-to-end e Apple non può visualizzare la posizione di un AirTag o di un prodotto di terze parti supportato. Per ulteriori informazioni, visitare la pagina support.apple.com/it-it/HT211331.

Attraverso un numero di serie, Apple può fornire i dettagli dell'account associato a fronte di un'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente. La cronologia di associazione di AirTag è disponibile per un periodo massimo di 25 giorni. Il seguente link di supporto fornisce informazioni su come individuare il numero di serie di un AirTag: support.apple.com/it-it/HT211658.

Per i numeri di serie dei dispositivi, Apple utilizza le cifre 0 (zero) e 1 (uno) anziché le lettere "O" e "I". Le richieste relative a numeri di serie contenenti le lettere "O" e "I" non daranno alcun risultato. Qualora una richiesta legale includa cinque o più numeri di serie, Apple richiede che tali numeri di serie siano inviati anche in formato elettronico modificabile (ad esempio Numbers, Excel, Pages o documento Word).

K. Estrazione di dati da dispositivi iOS bloccati mediante codice

Per tutti i dispositivi con iOS 8.0 e versioni successive, Apple non è in grado di estrarre i dati dai dispositivi poiché solitamente le informazioni richieste dalle forze dell'ordine sono codificate e Apple

non possiede la chiave di codifica. Tutti gli iPhone 6 e i modelli successivi sono dotati di serie di iOS 8.0 o una versione successiva di iOS.

Per i dispositivi con sistema operativo da iOS 4 ad iOS 7, Apple potrebbe, a seconda dello stato del dispositivo, eseguire estrazioni di dati dai dispositivi stessi in conformità alla legge CalECPA (California's Electronic Communications Privacy Act, codice penale della California, §§1546-1546.4). Affinché Apple possa eseguire un'estrazione di dati da un dispositivo iOS che soddisfa questi criteri, le forze dell'ordine devono ottenere un mandato di perquisizione per esigenze probatorie ai sensi della legge CalECPA. Oltre a quanto previsto dalla legge CalECPA, Apple non ha identificato altre autorità legali riconosciute che possono richiedere all'azienda di estrarre i dati in qualità di terza parte nell'ambito di attività investigative ufficiali.

L. Richiesta di indirizzo IP

Prima di inoltrare un procedimento legale con un indirizzo IP come identificatore, Apple chiede alle forze dell'ordine di verificare che l'indirizzo IP in oggetto non sia un indirizzo IP pubblico o del router e non utilizzi la Carrier-Grade Network Address Translation (CGNAT), nonché di confermare a Apple durante la notifica del procedimento legale che si tratta di un indirizzo IP non pubblico. Inoltre, tali richieste devono includere un limite temporale non superiore a tre giorni. In risposta a tale richiesta, Apple potrebbe essere in grado di produrre registri di connessione (fare riferimento alla sezione III.Q di seguito), da cui le forze dell'ordine possono tentare di identificare un particolare account Apple/ID Apple da usare come identificatore in una richiesta di follow-up di un procedimento legale. I dati dei clienti e delle clienti Apple basati su un indirizzo IP, se disponibili, possono essere ottenuti mediante apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

M. Altre informazioni disponibili relative ai dispositivi

Indirizzo MAC: un indirizzo MAC (Media Access Control) è un codice identificativo univoco assegnato alle interfacce di rete per le comunicazioni che viaggiano su un determinato segmento di rete. Tutti i prodotti Apple con interfacce di rete come Bluetooth, Ethernet, Wi-Fi o FireWire avranno uno o più indirizzi MAC. Per ottenere le informazioni relative all'indirizzo MAC è necessario presentare un'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente fornendo a Apple un numero di serie (oppure, nel caso di un dispositivo iOS, un numero IMEI, MEID o UDID).

N. Richieste di dati dei sistemi di videosorveglianza degli Apple Store

I dati dei sistemi di videosorveglianza variano in base alla sede dello store. Tali dati vengono conservati presso gli Apple Store per un massimo di 30 giorni. In molte giurisdizioni, le leggi locali stabiliscono di conservarli soltanto per ventiquattro (24) ore. Una volta trascorso questo periodo, i dati dei sistemi di videosorveglianza potrebbero non essere più disponibili. Le richieste riguardanti esclusivamente i dati dei sistemi di videosorveglianza possono essere inviate all'indirizzo lawenforcement@apple.com. Le autorità governative o le forze dell'ordine devono specificare la data, l'ora ed eventuali altre informazioni correlate alla transazione in questione.

O. Game Center

Game Center è il social network di Apple per i giochi. Le informazioni sulle connessioni a Game Center di un cliente o una cliente oppure di un dispositivo possono essere rese disponibili. È possibile ottenere le informazioni sui registri delle connessioni, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

P. Attivazione di dispositivi iOS

Quando un cliente o una cliente attiva un dispositivo iOS con un operatore di telefonia mobile o esegue un upgrade del software, Apple riceve alcune informazioni dall'operatore o dal dispositivo stesso, a seconda dei casi. Possono essere resi disponibili gli indirizzi IP associati all'operazione eseguita, i numeri ICCID e altri identificativi del dispositivo. È possibile ottenere tali informazioni, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

Dual SIM: per i dispositivi dotati di dual SIM, è possibile ottenere le informazioni sull'operatore di telefonia per la scheda nano-SIM e/o eSIM, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente. Una eSIM è una scheda SIM digitale che permette ai clienti e alle clienti di attivare un piano telefonico di un operatore senza dover usare una nano-SIM fisica. Per ulteriori informazioni, visitare la pagina support.apple.com/it-it/HT209044. In Cina continentale, a Hong Kong e Macao, iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone XS Max e iPhone XR hanno la tecnologia dual SIM con due schede nano-SIM.

Q. Registri delle connessioni

È possibile richiedere a Apple l'attività di connessione ai servizi Apple di un cliente o una cliente oppure di un dispositivo (ad esempio, a Apple Music, app Apple TV, Apple Podcasts, Apple Books, iCloud, Il mio ID Apple e forum di discussione Apple), laddove disponibile. È possibile ottenere i registri di queste connessioni con gli indirizzi IP, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

R. Registri di iForgot e Il mio ID Apple

È possibile richiedere a Apple i registri di iForgot e Il mio ID Apple di un cliente o una cliente. Tali registri possono contenere informazioni sulle operazioni di reimpostazione delle password. È possibile ottenere i registri di connessione con gli indirizzi IP, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

S. FaceTime

Le comunicazioni via FaceTime sono interamente codificate e Apple non può decodificare in alcun modo i dati in transito da un dispositivo all'altro. Apple non può intercettare le comunicazioni che avvengono via FaceTime. Quando viene inoltrata una chiamata FaceTime, Apple riceve i registri della chiamata FaceTime in entrata. Questi registri non indicano se ha effettivamente avuto luogo una conversazione tra clienti. I registri delle chiamate FaceTime in entrata vengono conservati per un massimo di 25 giorni. È possibile ottenere i registri delle chiamate FaceTime, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

T. iMessage

Le comunicazioni via iMessage sono interamente codificate e Apple non può decodificare in alcun modo i dati in transito da un dispositivo all'altro. Apple non può intercettare le comunicazioni che avvengono via iMessage e non dispone dei registri delle comunicazioni iMessage. Apple dispone invece dei registri relativi alle query sulla compatibilità con iMessage. Questi registri indicano che una

query è stata avviata da un'applicazione del dispositivo (ad esempio, Messaggi, Contatti, Telefono ecc.) e indirizzata ai server di Apple per trovare un handle di ricerca (che può essere un numero di telefono, un indirizzo email o un ID Apple) e stabilire se tale handle di ricerca è "compatibile" con iMessage. I registri relativi alle query sulla compatibilità con iMessage non indicano se ha effettivamente avuto luogo una conversazione tra clienti. Apple non è in grado di stabilire se una comunicazione iMessage ha effettivamente avuto luogo sulla base dei suddetti registri. Inoltre, Apple non è in grado di identificare l'applicazione che ha avviato la query. I registri relativi alle query sulla compatibilità con iMessage non confermano l'effettivo tentativo di esecuzione di un'operazione con iMessage. Questi registri vengono conservati per un massimo di 25 giorni. È possibile ottenere i registri relativi alle query sulla compatibilità con iMessage, se disponibili, attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

U. App Apple TV

Con l'app Apple TV i clienti e le clienti possono cercare/acquistare/riprodurre e sottoscrivere abbonamenti a film e serie TV forniti da Apple TV+, canali Apple TV e app/servizi di altre aziende. Potrebbe essere disponibile la cronologia degli acquisti e dei download.

Le richieste di informazioni sui clienti e sulle clienti dell'app Apple TV devono includere l'identificativo del dispositivo Apple (numero di serie, IMEI, MEID o GUID) oppure l'indirizzo email dell'account/ID Apple pertinente. Se non si conosce l'indirizzo email dell'account/ID Apple, è necessario fornire a Apple le informazioni sul cliente o sulla cliente sotto forma di nome completo e numero di telefono (e/o nome completo e indirizzo fisico) per consentire l'identificazione dell'account del cliente o della cliente. I funzionari e le funzionarie delle autorità governative o delle forze dell'ordine possono fornire anche un numero d'ordine Apple valido oppure il numero completo di una carta di credito o debito associata agli acquisti nell'app Apple TV. Oltre a questi parametri può essere fornito anche il nome del cliente o della cliente; tuttavia quest'ultimo dato, da solo, non è sufficiente per ottenere le informazioni.

Nota: per le richieste legali contenenti dati completi riguardanti carte di credito/debito, è necessario (per motivi di sicurezza) che tali dati siano trasmessi in un documento protetto da password/codificato (.PDF e formato modificabile, ad esempio Numbers, Excel, Pages o documento Word) all'indirizzo lawenforcement@apple.com e che la password venga fornita in un'email separata. Inoltre, nel rispetto degli standard di sicurezza di sistema, Apple non scarica la documentazione relativa a richieste legali da link inviati tramite email.

V. Accedi con Apple

La funzione Accedi con Apple consente ai clienti e alle clienti di accedere in modo più riservato a siti web e app di terze parti utilizzando l'ID Apple. Tramite il pulsante Accedi con Apple nei siti e nelle app aderenti, i clienti e le clienti possono configurare un account e accedere con il loro ID Apple. Anziché utilizzare un account dei social media o compilare moduli e scegliere una nuova password, i clienti e le clienti possono semplicemente toccare il pulsante Accedi con Apple, controllare le informazioni e accedere in modo rapido e sicuro con Face ID, Touch ID o il codice del dispositivo. Per ulteriori informazioni, visitare la pagina support.apple.com/it-it/HT210318.

Nascondi la mia email è una funzione di Accedi con Apple. Utilizza un servizio di inoltro email privato di Apple per creare e condividere un indirizzo email univoco e casuale che inoltra i messaggi all'indirizzo email personale del cliente o della cliente. È possibile ottenere le informazioni di base sul cliente o sulla cliente attraverso l'apposita richiesta legalmente valida nel Paese del richiedente o della richiedente.

IV.Domande frequenti

D: Posso contattare Apple tramite email per eventuali domande riguardanti una richiesta di informazioni da parte delle forze dell'ordine?
R: Sì, le domande o le richieste relative a un procedimento giudiziario di autorità governative possono essere inviate all'indirizzo lawenforcement@apple.com.

D: Per far funzionare o utilizzare un dispositivo è necessario registrarlo presso Apple?
R: No, per far funzionare o utilizzare i dispositivi non è necessario registrarli presso Apple.

D: Apple può fornirmi il codice di un dispositivo iOS attualmente bloccato?
R: No, Apple non ha accesso ai codici dei clienti e delle clienti.

D: Come posso restituire un dispositivo rubato o smarrito al legittimo proprietario o alla legittima proprietaria?
R: In questi casi, occorre contattare lawenforcement@apple.com. Nel messaggio, indicare il numero di serie del dispositivo (o il numero IMEI, se disponibile) e qualsiasi altra informazione rilevante. Per informazioni su come trovare il numero di serie, visitare la pagina: support.apple.com/it-it/HT204308.

Se le informazioni sul cliente o sulla cliente sono disponibili, Apple provvederà a contattare la persona in questione e fornirle informazioni per rivolgersi alle forze dell'ordine e recuperare il dispositivo. Tuttavia, qualora non sia possibile identificare l'utente sulla base delle informazioni disponibili, potrebbe essere richiesto di inviare una richiesta legalmente valida.

D: Apple conserva un elenco dei dispositivi smarriti o rubati?
R: No, Apple non conserva un elenco dei dispositivi smarriti o rubati.

D: Dopo che le forze dell'ordine hanno concluso un'indagine o una causa, come occorre procedere con le informazioni fornite?
R: Al termine di un'indagine o di una causa, e una volta esauriti tutti i gradi di appello, i contenuti e i dati forniti alle autorità governative o alle forze dell'ordine contenenti informazioni di identificazione personale (incluse eventuali copie) devono essere distrutti.

D: In caso di ricezione di una richiesta di informazioni da parte delle forze dell'ordine, i clienti interessati o le clienti interessate ricevono una comunicazione?
R: Sì, la politica di Apple in materia si applica alle richieste di accesso agli account da parte di forze dell'ordine, autorità governative e soggetti privati. Apple provvede a informare i clienti e le clienti e le persone titolari degli account eccetto nei casi in cui: a) tale azione sia vietata da un'ordinanza di non divulgazione o dalla legge vigente in materia; b) Apple, a sua propria discrezione, ritenga ragionevolmente che da ciò deriverebbe un rischio di lesioni gravi o morte per una persona; c) sussista una situazione di potenziale rischio per un minore o una minore; d) tale azione non sia richiesta dalle circostanze del caso.