Diretrizes de Processos Jurídicos

Autoridades Governamentais e Policiais fora dos Estados Unidos

Estas Diretrizes são fornecidas para serem usadas por órgãos governamentais e policiais fora dos Estados Unidos durante a busca por informações sobre clientes de aparelhos, produtos e serviços da Apple, e são provenientes de entidades da Apple na região ou país pertinente. A Apple atualizará estas Diretrizes conforme necessário.

Nestas Diretrizes, o termo Apple designa a entidade relevante responsável pelas informações dos clientes de uma região ou um país específico. A Apple, na qualidade de empresa global, conta com diversas pessoas jurídicas em jurisdições diferentes, as quais são responsáveis pelas informações pessoais que coletam e que são processadas em nome delas pela Apple Inc. Por exemplo, as informações de pontos de venda nas entidades de varejo da Apple fora dos Estados Unidos são controladas por entidades de varejo individuais da Apple em cada país. As informações pessoais relacionadas ao site Apple.com e aos Serviços de Mídia da Apple também poderão ser controladas por pessoas jurídicas fora dos Estados Unidos, conforme indicado nos termos de cada serviço em uma jurisdição específica. Normalmente, as pessoas jurídicas da Apple fora dos Estados Unidos na Austrália, no Canadá, na Irlanda e no Japão são responsáveis pelos dados de clientes relacionados aos serviços da Apple nas respectivas regiões.

Todas as outras solicitações de informações referentes aos clientes da Apple, inclusive dúvidas dos clientes sobre a divulgação de informações, deverão ser direcionadas para www.apple.com/br/privacy/contact/. Estas Diretrizes não se aplicam às solicitações de autoridades governamentais e policiais dos Estados Unidos feitas à Apple Inc.

No caso de solicitações por informações feitas por autoridades governamentais e policiais, a Apple cumpre as leis relacionadas às entidades globais que controlam nossos dados, e fornecemos informações conforme exigido pela lei. Todas as solicitações de órgãos governamentais e policiais fora dos Estados Unidos em busca de conteúdo, com exceção de circunstâncias emergenciais (definidas abaixo em Solicitações Emergenciais), devem estar em conformidade com as leis aplicáveis, inclusive a lei dos Estados Unidos relativa à privacidade nas comunicações (ECPA — Electronic Communications Privacy Act). Uma solicitação feita sob um Tratado de Assistência Jurídica Mútua ou Acordo Executivo de acordo com a Lei para Esclarecer o Uso Legal de Dados no Exterior ("CLOUD Act") estará em conformidade com a ECPA. A Apple somente fornecerá conteúdo do cliente, na forma como existe na conta do cliente, mediante o processo judicialmente válido.

No caso de solicitações de entidades privadas, a Apple cumpre as leis relacionadas às entidades locais que controlam os dados de cliente e fornecerá os dados conforme exigido pela lei.

A Apple dispõe de um processo centralizado para receber, rastrear, processar e responder a solicitações judiciais legítimas provenientes de autoridades governamentais, autoridades policiais e entidades privadas, desde o momento em que são recebidas até quando uma resposta é enviada. Uma equipe treinada em nosso departamento jurídico examina e avalia todas as solicitações recebidas. As solicitações que, segundo determinação da Apple, carecem de base legal válida ou são

consideradas inapropriadas, confusas ou muito abrangentes são contestadas, questionadas ou rejeitadas.

A Apple fornece respostas para autoridade governamental ou policial solicitante no endereço de e-mail oficial da autoridade solicitante. Toda a preservação de evidências de acordo com as respostas fornecidas pela Apple é de responsabilidade da autoridade governamental ou policial solicitante.

ÍNDICE

I. Informações Gerais

II. Solicitações Judiciais à Apple

A. Solicitações de Informações por Autoridades Governamentais ou Policiais
B. Como Gerenciar e Responder a Solicitações de Informações por Autoridades Governamentais ou Policiais
C. Solicitações de Conservação
D. Solicitações Emergenciais
E. Solicitações de Restrição de Acesso/Exclusão de Conta
F. Notificação ao Cliente

III. Informações Disponíveis na Apple

A. Registro de Aparelhos
B. Registros do Atendimento ao Cliente
C. Serviços de Mídia da Apple
D. Transações em Apple Stores
E. Pedidos em Apple.com
F. Cartões-presente
G. Apple Pay
H. iCloud
I. Buscar
J. AirTag e Programa de Acessórios da Rede do App Buscar
K. Extração de Dados de Aparelhos com iOS Bloqueados pelo Código de Acesso
L. Solicitação de Endereço IP
M. Outras Informações Disponíveis sobre os Aparelhos
N. Solicitações por Dados de CFTV de Apple Stores
O. Game Center
P. Ativação de Aparelhos com iOS
Q. Registros de Conexão
R. Registros do Meu ID Apple e do iForgot
S. FaceTime
T. iMessage
U. App Apple TV
V. Iniciar Sessão com a Apple

IV. Perguntas frequentes

I. Informações Gerais

A Apple cria, fabrica e comercializa aparelhos de mídia e comunicações móveis, computadores pessoais e aparelhos portáteis para reprodução de música digital. Também vende diversos itens relacionados, como softwares, serviços, periféricos e soluções de rede, além de aplicativos e conteúdo digital de terceiros. Os produtos e serviços da Apple incluem Mac, iPhone, iPad, iPod touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, um portfólio de aplicativos de software profissionais e de consumo, os sistemas operacionais iOS e macOS X, iCloud e diversas ofertas de acessórios, serviços e suporte. Além disso, a Apple vende e fornece aplicativos e conteúdo digital por meio dos serviços Apple Music, App Store, Apple Books e Mac App Store. As informações de clientes são mantidas pela Apple de acordo com a política de privacidade da Apple e os termos de serviço que se aplicam à oferta de serviço específica. A Apple tem o compromisso de manter a privacidade dos clientes dos produtos e serviços da Apple ("clientes da Apple"). Consequentemente, exceto em situações emergenciais conforme previsto por lei, as informações sobre os clientes da Apple não serão divulgadas sem um processo legal válido.

As informações contidas nestas Diretrizes visam esclarecer os órgãos governamentais e policiais fora dos Estados Unidos sobre o processo judicial exigido pela Apple para divulgar informações eletrônicas a autoridades governamentais e policiais fora dos Estados Unidos. A finalidade destas Diretrizes não é oferecer orientação jurídica. A seção de perguntas frequentes destas Diretrizes visa fornecer respostas para algumas das perguntas mais comuns recebidas pela Apple. Nem estas Diretrizes nem as perguntas frequentes abordarão todas as circunstâncias concebíveis que possam surgir.

Em caso de outras dúvidas, entre em contato com lawenforcement@apple.com.

O endereço de e-mail indicado acima destina-se exclusivamente ao uso por funcionários de agências governamentais e policiais. Se você optar por enviar um e-mail para esse endereço, deverá usar um endereço de e-mail válido e oficial de uma agência governamental ou policial.

As solicitações judiciais enviadas para a Apple devem buscar informações referentes a um determinado aparelho ou cliente da Apple e ao(s) serviço(s) específico(s) fornecido(s) pela Apple a esse cliente. A Apple poderá fornecer informações sobre aparelhos ou clientes da Apple, contanto que ainda mantenha a posse das informações solicitadas de acordo com as políticas de retenção de dados da empresa. A Apple retém os dados conforme descrito abaixo, em seções específicas de "Informações Disponíveis". Todos os outros dados serão retidos pelo período necessário ao cumprimento das finalidades descritas em nossa política de privacidade. Os órgãos governamentais e policiais devem ser o mais restritos e específicos possível ao elaborar solicitações para evitar interpretação errônea, contestação, questionamento e/ou rejeição em resposta a uma solicitação inapropriada, confusa ou muito abrangente. Todas as solicitações de órgãos governamentais e policiais fora dos Estados Unidos em busca de conteúdo, com exceção de circunstâncias emergenciais (definidas abaixo em Solicitações Emergenciais), devem estar em conformidade com as leis aplicáveis, inclusive a lei dos Estados Unidos relativa à privacidade nas comunicações (ECPA — Electronic Communications Privacy Act). Uma solicitação feita sob um Tratado de Assistência Jurídica Mútua ou Acordo Executivo de acordo com a Lei para Esclarecer o Uso Legal de Dados no Exterior ("CLOUD Act") estará em conformidade com a ECPA. A Apple somente fornecerá conteúdo do cliente, na forma como existe na conta do cliente, mediante o processo judicialmente válido.

Nada nestas Diretrizes se destina a criar direitos exequíveis contra a Apple, e as políticas da Apple poderão ser atualizadas ou modificadas no futuro sem aviso prévio à autoridade governamental

ou policial.

II. Solicitações Judiciais à Apple

A. Solicitações de Informações por Autoridades Governamentais ou Policiais

A Apple aceita atender a solicitações de informações judicialmente válidas por parte de autoridades governamentais ou policiais, enviadas por e-mail por órgãos governamentais e policiais, contanto que o envio seja feito pelo endereço de e-mail oficial do órgão em questão. As autoridades governamentais e policiais fora dos Estados Unidos que enviarem uma solicitação de informações à Apple deverão preencher um modelo da Solicitação de Informações por Autoridade Governamental ou Policial e enviá-lo diretamente pelo respectivo endereço de e-mail oficial para o endereço lawenforcement@apple.com.

O endereço de e-mail indicado acima destina-se exclusivamente ao uso por funcionários de agências governamentais e policiais. Nos casos em que as solicitações contiverem cinco ou mais identificadores, como número de série ou IMEI do aparelho, IDs Apple, endereços de e-mail ou números de nota fiscal ou pedido, tais dados deverão ser enviados em formato editável (por exemplo, documento do Numbers, Excel, Pages ou Word). Em geral, identificadores como esses são necessários para conduzir buscas por informações relacionadas a aparelhos, contas ou transações financeiras.

Nota: A Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

Para que a Apple divulgue informações do cliente em resposta a um pedido de um órgão policial, a autoridade solicitante deve indicar a base legal que autoriza a obtenção de informações probatórias na forma de dados pessoais por uma autoridade policial de um Controlador de Dados como a Apple. Exemplos de solicitações que a Apple considera legalmente válidas são: Production Orders (Austrália, Canadá, Nova Zelândia), lettres de réquisition ou commissions rogatoires (França), Solicitud Datos (Espanha), Ordem Judicial (Brasil), Auskunftsersuchen (Alemanha), Obligation de dépôt (Suíça), 個人情報の開示依頼 (Japão), Personal Data Request, Orders, Warrants and Communications Data Authorizations (UK), bem como ordens judiciais equivalentes e/ou solicitações de outros países.

B. Como Gerenciar e Responder a Solicitações de Informações por Autoridades Governamentais ou Policiais

A Apple analisa atentamente todas as solicitações judiciais para assegurar que há uma base legal válida para cada solicitação e atende às solicitações judicialmente válidas. Nos casos em que a Apple determinar que não há base legal válida ou em que uma solicitação for inapropriada, confusa ou muito abrangente, a Apple contestará, questionará ou rejeitará a solicitação.

Para fins de processamento e devido a limitações do sistema, a Apple não aceita solicitações judiciais que contenham mais de 25 identificadores de conta. Se a autoridade policial enviar solicitações judiciais com mais de 25 identificadores de conta, a Apple responderá aos primeiros 25, e essas autoridades precisarão reenviar outras solicitações judiciais no caso de identificadores adicionais.

C. Solicitações de Conservação

Todas as solicitações de órgãos governamentais e policiais fora dos Estados Unidos em busca de conteúdo, com exceção de circunstâncias emergenciais (definidas abaixo em Solicitações Emergenciais), devem estar em conformidade com as leis aplicáveis, inclusive a lei dos Estados Unidos relativa à privacidade nas comunicações (ECPA — Electronic Communications Privacy Act). A Uma solicitação feita sob um Tratado de Assistência Jurídica Mútua ou Acordo Executivo de acordo com Lei para Esclarecer o Uso Legal de Dados no Exterior ("CLOUD Act") estará em conformidade com a ECPA. Uma solicitação para conservar dados em antecipação a uma solicitação iminente em conformidade com a ECPA deverá ser enviada por e-mail para o endereço lawenforcement@apple.com.

As solicitações de conservação devem incluir os seguintes dados relevantes: ID Apple/endereço de e-mail da conta, ou nome completo **e** número de telefone, e/ou nome completo **e** endereço físico do cliente da conta Apple em questão. Após receber uma solicitação de conservação, a Apple manterá, por 90 dias, um extrato único dos dados de cliente existentes solicitados que estiverem disponíveis na ocasião da solicitação. Após o período de 90 dias, a conservação será removida automaticamente do servidor de armazenamento. Contudo, é possível estender esse período por mais 90 dias mediante a renovação da solicitação. Se houver uma tentativa de atender a mais de duas solicitações de conservação para a mesma conta, a segunda solicitação será tratada como uma solicitação de extensão da conservação original, e não uma conservação separada de novos dados.

D. Solicitações Emergenciais

A Apple considera que uma solicitação é emergencial quando está relacionada a circunstâncias que envolvam ameaças graves e iminentes à vida ou segurança de pessoas, à segurança de um Estado ou à segurança de infraestruturas ou instalações críticas.

Caso a autoridade governamental ou policial solicitante ofereça confirmação satisfatória de que a solicitação está relacionada a circunstâncias emergenciais que envolvam um ou mais dos critérios acima, a Apple examinará tal solicitação em caráter de emergência.

A fim de fazer uma solicitação para que a Apple divulgue informações de forma voluntária em caráter de emergência, a autoridade governamental ou policial solicitante deve preencher o formulário Solicitação Emergencial de Informações por Autoridade Governamental ou Policia e enviá-lo diretamente pelo respectivo endereço de e-mail oficial para o endereço exigent@apple.com com as palavras "Pedido de emergência" na linha do assunto.

Caso uma autoridade governamental ou policial busque dados de cliente em resposta a uma Solicitação Emergencial de Informações por Autoridade Governamental ou Policial, um supervisor do órgão governamental ou policial que enviou a Solicitação Emergencial de Informações por Autoridade Governamental ou Policial poderá ser contatado e solicitado a confirmar para a Apple que a solicitação emergencial era legítima. A autoridade governamental ou policial que enviar a Solicitação Emergencial de Informações por Autoridade Governamental ou Policial deverá indicar as informações de contato do supervisor na solicitação.

Caso a autoridade governamental ou policial precise entrar em contato com a Apple devido a uma investigação emergencial, entre em contato com o Global Security Operations Center (GSOC, Centro Global de Operações de Segurança) da Apple pelo telefone 001 408 974-2095. Esse número de telefone oferece suporte em vários idiomas.

E. Solicitações de Restrição de Acesso/Exclusão de Conta

Caso uma autoridade governamental ou policial solicite que a Apple restrinja ou apague o ID Apple de um cliente, a Apple exigirá uma ordem judicial ou outro processo judicial local equivalente (geralmente condenação ou mandado) demonstrando que a conta a ser restringida ou apagada foi usada de forma ilícita.

A Apple analisa atentamente todas as solicitações de autoridades governamentais e policiais para assegurar que há uma base legal válida para cada solicitação. Nos casos em que a Apple determina que não há base jurídica válida ou quando a ordem judicial não demonstrar que a conta a ser restrita/excluída foi usada ilegalmente, a Apple rejeitará/contestará a solicitação.

Nas situações em que a Apple receber uma ordem judicial satisfatória ou outro processo judicial local equivalente (geralmente condenação ou mandado), enviado por uma autoridade governamental ou policial, demonstrando que a conta a ser restringida ou apagada foi usada de forma ilícita, a Apple promoverá a ação exigida de restringir ou apagar a conta em cumprimento à ordem judicial e orientará o órgão solicitante conforme necessário.

F. Notificação ao Cliente

A Apple notificará os clientes quando as informações da respectiva conta Apple estiverem sendo requisitadas em resposta a uma solicitação judicial válida de uma autoridade governamental ou policial, exceto quando tal notificação for expressamente proibida pela solicitação judicial válida, por uma ordem judicial recebida pela Apple, pela legislação aplicável ou quando a Apple, a seu critério exclusivo, acreditar que tal notificação acarretará risco de lesão ou morte para um indivíduo identificável, quando o caso envolver exposição infantil a situações de risco, ou quando a notificação não for aplicável aos fatos pertinentes do caso.

Passados 90 dias, a Apple apresentará uma notificação diferida relacionada a divulgações emergenciais, exceto quando a notificação for proibida por uma ordem judicial ou pela legislação aplicável ou quando a Apple, a critério exclusivo dela, acreditar que tal notificação poderia acarretar risco de lesão ou morte para um indivíduo ou um grupo de indivíduos identificáveis, ou quando o caso envolver exposição infantil a situações de risco. A Apple fornecerá uma notificação diferida após o término do período de não divulgação especificado em uma ordem judicial, salvo se a Apple, a critério exclusivo dela, tiver motivos razoáveis para acreditar que fornecer tal notificação poderia acarretar risco de lesão ou morte para um indivíduo ou um grupo de indivíduos identificáveis, quando o caso envolver exposição infantil a situações de risco, ou quando a notificação não for aplicável aos fatos pertinentes do caso.

A Apple notificará seus clientes quando a respectiva conta Apple tiver sido restringida ou apagada por ter a Apple recebido uma ordem judicial (geralmente condenação ou mandado) demonstrando que a conta a ser restringida ou apagada foi usada de forma ilícita ou em violação dos termos de serviço da Apple; exceto quando fornecer tal notificação for proibida pelo processo judicial em si, por uma ordem judicial recebida pela Apple, pela legislação aplicável, quando o caso envolver exposição infantil a situações de risco, ou quando a Apple, a critério exclusivo dela, tiver motivos razoáveis para acreditar que fornecer tal notificação poderia acarretar risco de lesão ou morte para um indivíduo ou um grupo de indivíduos identificáveis, ou quando a notificação não for aplicável aos fatos pertinentes do caso.

III. Informações Disponíveis na Apple

Esta seção abrange os tipos gerais de informação que a Apple poderá disponibilizar na ocasião da publicação destas Diretrizes.

A. Registro de Aparelhos

Informações básicas sobre clientes ou cadastros, inclusive nome, endereço, endereço de e-mail e número de telefone, são fornecidas à Apple pelos clientes ao fazer o registro em um aparelho Apple com versão anterior ao iOS 8 e ao macOS Sierra 10.12. A Apple não verifica essas informações, as quais podem não ser precisas ou podem não refletir o proprietário do aparelho. As informações de registro correspondentes a aparelhos que executam o iOS 8 e versões posteriores, assim como computadores Mac que executam o macOS Sierra 10.12 e versões posteriores, são recebidas quando um cliente associa um aparelho a um ID Apple do iCloud. Essas informações podem não ser precisas ou podem não refletir o proprietário do aparelho. Registro as informações, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

Deve-se observar que os números de série dos aparelhos Apple não contêm as letras "O" ou "I"; em vez disso, a Apple utiliza os algarismos 0 (zero) e 1 (um) nos números de série. As solicitações por números de série com a letra "O" ou "I" não produzirão resultados. Nos casos em que uma solicitação judicial tiver cinco ou mais números de série, a Apple solicitará que esses números também sejam enviados em formato eletrônico editável (por exemplo, documento do Numbers, Excel, Pages ou Word).

B. Registros do Atendimento ao Cliente

Os contatos que os clientes mantiveram com o atendimento ao cliente da Apple a respeito de um aparelho ou serviço podem ser obtidos na Apple. Essas informações podem incluir registros de interações de suporte com clientes referentes a um aparelho ou serviço específico da Apple. Também podem estar disponíveis informações sobre o aparelho, a garantia e o reparo. Essas informações, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

C. Serviços de Mídia da Apple

App Store, Apple Music, o app Apple TV, Apple Podcasts e Apple Books ("Serviços de Mídia da Apple") são aplicativos de software usados pelos clientes para organizar e reproduzir apps, música e vídeo digital e streaming de conteúdo. Os Serviços de Mídia da Apple também fornecem conteúdo para os clientes baixarem nos respectivos computadores e aparelhos com iOS. Quando um cliente abre uma conta Apple, informações básicas do cliente, como nome, endereço físico, endereço de e-mail e número de telefone, podem ser fornecidas pelo cliente. Além disso, também podem estar disponíveis informações sobre conexões e transações de compra/download nos Serviços de Mídia da Apple e conexões de atualização/novo download. As informações de endereços IP podem estar limitadas aos 18 meses mais recentes. Os registros de conexões e informações de cliente dos Serviços de Mídia da Apple com endereços IP, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante.

As solicitações de dados dos Serviços de Mídia da Apple devem incluir o identificador do aparelho Apple (número de série, IMEI, MEID ou GUID) ou ID Apple/endereço de e-mail da conta pertinente. Se o ID Apple/endereço de e-mail da conta forem desconhecidos, será necessário fornecer à Apple as informações do cliente dos Serviços de Mídia da Apple na forma de nome completo **e** número de telefone e/ou nome completo **e** endereço físico para identificar a conta de cliente dos Serviços de Mídia da Apple em questão. As autoridades governamentais ou policiais também podem fornecer um número de pedido válido dos Serviços de Mídia da Apple ou um número completo de cartão de débito ou crédito associado à(s) compra(s) nos Serviços de Mídia da Apple. Um nome de cliente em combinação com esses parâmetros também poderá ser fornecido, mas apenas o nome do cliente não é suficiente para obter informações.

Nota: nos casos em que a solicitação judicial tiver dados completos de cartão de crédito/débito, para fins de segurança dos dados, tais dados deverão ser enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. O documento pode ser .PDF e formato editável, por exemplo, documento do Numbers, Excel, Pages ou o Word. Além disso, a Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

D. Transações em Apple Stores

Transações de Ponto de Venda são transações em espécie, cartão de crédito/débito ou cartão-presente realizadas em uma Apple Store. As solicitações de registros de Pontos de Venda devem incluir o número completo do cartão de crédito/débito usado e podem incluir outras informações, por exemplo, data e hora da transação, valor e itens adquiridos. Informações sobre o tipo de cartão associado a determinada compra, nome do comprador, endereço de e-mail, data e hora da transação, valor da transação e localização da loja, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

As solicitações de cópias duplicadas de recibos devem incluir o número da transação de varejo associado à(s) compra(s) e, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

Nota: nos casos em que a solicitação judicial tiver dados completos de cartão de crédito/débito, para fins de segurança dos dados, tais dados deverão ser enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. O documento pode ser .PDF e formato editável, por exemplo, documento do Numbers, Excel, Pages ou o Word. Além disso, a Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

E. Pedidos em Apple.com

A Apple mantém informações sobre pedidos online no site Apple.com, que podem incluir nome do comprador, endereço de envio, número de telefone, endereço de e-mail, produto(s) adquirido(s), valor da compra e endereço IP da compra. As solicitações por informações relacionadas a pedidos online no site Apple.com devem incluir um número completo de cartão de crédito/débito ou um número de pedido ou número de série do item adquirido. Um nome de cliente em combinação com esses parâmetros também poderá ser fornecido, mas apenas o nome do cliente não é suficiente para obter informações. Como alternativa, as solicitações por informações relacionadas a pedidos online no site Apple.com podem incluir o ID Apple/endereço de e-mail da conta pertinente. Se o ID Apple/endereço de e-mail da conta forem desconhecidos, será necessário fornecer à Apple as informações do cliente na forma de nome completo **e** número de telefone e/ou nome completo **e** endereço físico para

identificar a conta Apple em questão. Informações sobre compras de pedidos online no site Apple.com, se disponíveis, podem ser obtidas com uma solicitação válida legalmente do país do solicitante.

Nota: nos casos em que a solicitação judicial tiver dados completos de cartão de crédito/débito, para fins de segurança dos dados, tais dados deverão ser enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. O documento pode ser .PDF e formato editável, por exemplo, documento do Numbers, Excel, Pages ou o Word. Além disso, a Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

F. Cartões-presente

Os Cartões-presente da Apple Store e os Cartões-presente da App Store e iTunes contam com um número de série. O formato do número de série varia dependendo de elementos como design e/ou data de emissão. A Apple pode fornecer informações disponíveis sobre Cartões-presente da Apple Store e Cartões-presente da App Store e iTunes mediante a solicitação judicialmente válida pertinente para o país do solicitante. Nos casos em que uma solicitação judicial tiver cinco ou mais números de série de vales-presente, a Apple solicitará que esses números sejam enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. O documento pode ser do Numbers, Excel, Pages ou o Word.

i. Cartões-presente da Apple Store

Os Cartões-presente da Apple Store podem ser usados em compras no site Apple.com ou em uma Apple Store. Os registros disponíveis podem incluir informações sobre o comprador do cartão-presente (caso tenha sido adquirido na Apple, e não em um estabelecimento de terceiros), as transações de compras associadas e os itens adquiridos. Em alguns casos, a Apple poderá cancelar ou suspender um Cartão-presente da Apple Store, dependendo do status do cartão específico. As informações de Cartões-presente da Apple Store, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

Nota: nos casos em que a solicitação judicial tiver dados completos do Cartão-presente da Apple Store, para fins de segurança dos dados, tais dados deverão ser enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. O documento pode ser .PDF e formato editável, por exemplo, documento do Numbers, Excel, Pages ou o Word. Além disso, a Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

ii. Cartões-presente da App Store e iTunes

Os Cartões-presente da App Store e iTunes podem ser usados no Apple Music, na App Store, no Apple Books e na Mac App Store. Com o número de série, a Apple pode determinar se o Cartão-presente da App Store e iTunes foi ativado (adquirido em um ponto de venda de varejo) ou resgatado (adicionado ao saldo de crédito na loja de uma conta Apple).

Quando um Cartão-presente da App Store e iTunes é ativado, os registros disponíveis podem

incluir nome da loja, localização, data e hora. Quando um Cartão-presente da App Store e iTunes é resgatado, os registros disponíveis podem incluir informações do cliente da conta Apple relacionada, data e hora da ativação e/ou do resgate e endereço IP do resgate. Em alguns casos, a Apple poderá desativar um Cartão-presente da App Store e iTunes, dependendo do status do cartão específico. As informações de Cartões-presente da App Store e iTunes, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

Nota: nos casos em que a solicitação judicial tiver dados completos do Cartão-presente da App Store e iTunes, para fins de segurança dos dados, tais dados deverão ser enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. O documento pode ser .PDF e formato editável, por exemplo, documento do Numbers, Excel, Pages ou o Word. Além disso, a Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

G. Apple Pay

As transações do Apple Pay feitas em lojas (por exemplo, no caso de comunicações com a tecnologia contactless/NFC) e em apps ou pontos de venda online são autenticadas de forma segura no aparelho do cliente e enviadas de forma criptografada para o estabelecimento ou processador de pagamentos do estabelecimento. Embora a segurança da transação seja verificada por um servidor da Apple, a Apple não processa os pagamentos, além de não armazenar tais transações nem os números completos de cartão de crédito/débito associados às compras feitas usando o Apple Pay. Essas informações podem estar disponíveis no banco emissor, na rede de pagamentos ou no estabelecimento relevantes.

Mais informações sobre os países e regiões que aceitam o Apple Pay estão disponíveis no artigo support.apple.com/pt-br/HT207957.

Para solicitar os dados de transação das compras feitas em Apple Stores ou no site Apple.com, a Apple exige o Número da Conta Principal do Aparelho (DPAN) usado na transação. O DPAN tem 16 dígitos e pode ser obtido no banco emissor. Nota: o DPAN é usado em transações de pagamentos sem contato com o comerciante em vez do número do cartão de crédito/débito (FPAN/PAN de financiamento). O DPAN é convertido no FPAN correspondente pelo processador do pagamento. Com as informações de DPAN relevantes, a Apple poderá fazer uma busca razoável para localizar informações responsivas por meio do sistema do seu ponto de venda. Os registros, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante.

A Apple pode fornecer informações ao Apple Pay sobre os tipos de cartões de crédito/débito que um cliente adicionou ao Apple Pay com as informações do cliente. Essas informações, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante. Para solicitar tais informações, a Apple exige um identificador do aparelho (número de série da Apple, SEID, IMEI ou MEID) ou um ID Apple/endereço de e-mail da conta.

Nota: nos casos em que a solicitação judicial tiver o DPAN, para fins de segurança dos dados, tais dados deverão ser enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. O documento pode ser .PDF e formato editável, por exemplo, documento do Numbers, Excel, Pages ou o Word. Além disso, a Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

H. iCloud

iCloud é o serviço de nuvem da Apple por meio do qual os clientes podem acessar músicas, fotos, documentos e outros itens em todos os seus aparelhos. Os clientes também podem fazer backup de aparelhos com iOS e iPadOS no iCloud. Com o serviço iCloud, os clientes podem configurar uma conta de e-mail no iCloud.com. Os domínios de e-mail do iCloud podem ser @icloud.com, @me.com e @mac.com. Todos os dados de conteúdo do iCloud armazenados pela Apple são criptografados no local do servidor. Para os dados que a Apple pode descriptografar, a Apple mantém as chaves de criptografia em seus data centers nos EUA. A Apple não recebe nem retém chaves de criptografia para os dados criptografados de ponta a ponta do cliente.

O iCloud é um serviço voltado a clientes. As solicitações por dados do iCloud devem incluir o ID Apple/endereço de e-mail da conta pertinente. Se o ID Apple/endereço de e-mail da conta forem desconhecidos, será necessário fornecer à Apple as informações do cliente na forma de nome completo **e** número de telefone e/ou nome completo **e** endereço físico para identificar a conta Apple em questão. Quando apenas um número de telefone ou ID Apple/endereço de e-mail da conta são fornecidos, informações disponíveis das contas verificadas associadas a esses critérios podem ser geradas.

I. As seguintes informações podem estar disponíveis no iCloud:

I. Informações do Cliente

Quando um cliente configura uma conta do iCloud, informações básicas dele, como nome, endereço físico, endereço de e-mail e número de telefone, podem ser fornecidas à Apple. Também podem estar disponíveis informações sobre conexões com recursos do iCloud.

Os registros de conexões e informações de cliente do iCloud com endereços IP, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante. Os registros de conexões são retidos por até 25 dias.

II. Registros do Mail

Os registros do Mail incluem dados de comunicações de entrada e de saída, por exemplo, hora, data, endereços de e-mail dos remetentes e endereços de e-mail dos destinatários. Os registros de e-mail do iCloud são retidos por até 25 dias e, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante.

III. Conteúdo de E-mail e Outros Tipos de Conteúdo do iCloud, Meu Compartilhamento de Fotos, Fototeca do iCloud, iCloud Drive, Contatos, Calendários, Favoritos, Histórico de Navegação do Safari, Histórico de Busca do Mapas, Mensagens, Backups de Aparelhos com iOS

O iCloud armazenará o conteúdo dos serviços que o cliente optou por manter na conta enquanto a conta do cliente permanecer ativa. A Apple não retém conteúdo apagado depois que ele é removido dos servidores da Apple. O conteúdo do iCloud pode incluir e-mails, fotos armazenadas, documentos, contatos, calendários, favoritos, histórico de navegação do Safari, histórico de busca do Mapas, mensagens e backups de aparelhos com iOS. Os backups de aparelhos com iOS podem incluir fotos e vídeos do Rolo da Câmera, ajustes do aparelho, dados de apps, iMessage, Chat de Negócios, mensagens SMS e MMS e voicemail. Todos os dados de conteúdo do iCloud armazenados pela Apple são criptografados no local do servidor. Para os dados que a Apple pode descriptografar, a Apple mantém as chaves de criptografia em seus data centers nos EUA. A Apple não recebe nem retém chaves de criptografia para os dados criptografados de ponta a ponta do cliente.

Todas as solicitações de órgãos governamentais e policiais fora dos Estados Unidos em busca de conteúdo, com exceção de circunstâncias emergenciais (definidas acima em Solicitações Emergenciais), devem estar em conformidade com as leis aplicáveis, inclusive a lei dos Estados Unidos relativa à privacidade nas comunicações (ECPA — Electronic Communications Privacy Act). Uma solicitação feita sob um Tratado de Assistência Jurídica Mútua ou Acordo Executivo de acordo com a Lei para Esclarecer o Uso Legal de Dados no Exterior ("CLOUD Act") estará em conformidade com a ECPA. A Apple somente fornecerá conteúdo do cliente, na forma como existe na conta do cliente, mediante a solicitação judicialmente válida.

II. Proteção Avançada de Dados

A Proteção Avançada de Dados do iCloud é um recurso que usa criptografia de ponta a ponta para proteger os dados do iCloud com o mais alto nível de segurança de dados da Apple. Para usuários que ativam a Proteção Avançada de Dados para iCloud, podem estar disponíveis dados limitados do iCloud. Mais informações sobre a Proteção Avançada de Dados podem ser encontradas em support.apple.com/pt-br/guide/security/advanced-data-protection-for-icloud-sec973254c5f/ e support.apple.com/pt-br/HT212520.

As seguintes informações podem estar disponíveis no iCloud se um usuário tiver ativado a Proteção Avançada de Dados para iCloud:

a. Informações do Cliente
Quando um cliente configura uma conta do iCloud, informações básicas dele, como nome, endereço físico, endereço de e-mail e número de telefone, podem ser fornecidas à Apple. Além disso, também podem estar disponíveis informações sobre conexões de recursos do iCloud. As informações do cliente do iCloud e os registros de conexão com endereços IP, caso estejam disponíveis, podem ser obtidos com a solicitação legalmente válida apropriada para o país do solicitante. Os registros de conexões são retidos por até 25 dias.

b. Registros do Mail
Os registros do Mail incluem dados de comunicações de entrada e de saída, por exemplo, hora, data, endereços de e-mail dos remetentes e endereços de e-mail dos destinatários. Os registros de e-mail do iCloud são retidos por até 25 dias e, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida

pertinente para o país do solicitante.

c. Conteúdo de E-mail e Outros Tipos de Conteúdo do iCloud
Quando a Proteção Avançada de Dados está ativada, o iCloud armazena o conteúdo de e-mail, contatos e calendários que o cliente decidiu manter na conta enquanto a conta do cliente permanece ativa. Esses dados podem ser fornecidos, conforme existam na conta do cliente, com a solicitação legalmente válida apropriada para o país do solicitante. Esses dados limitados são armazenados pela Apple e, além disso, criptografados no local do servidor. Para os dados que a Apple pode descriptografar, a Apple mantém as chaves de criptografia em seus data centers nos EUA. A Apple não recebe nem retém chaves de criptografia para os dados criptografados de ponta a ponta do cliente.

A Proteção Avançada de Dados usa criptografia de ponta a ponta, e a Apple não pode descriptografar determinados conteúdos do iCloud, incluindo Fotos, iCloud Drive, Backup, Notas e Favoritos do Safari. Em algumas circunstâncias, a Apple pode reter informações limitadas relacionadas a esses serviços do iCloud que podem ser obtidas, caso estejam disponíveis, com a solicitação legalmente válida para o país do solicitante.

III. Retransmissão Privada do iCloud

A Retransmissão Privada do iCloud é um serviço de privacidade na Internet oferecido como parte de uma assinatura do iCloud +. A Retransmissão Privada protege a navegação na web dos usuários no Safari, as consultas de resolução de DNS (Domain Name Space) e o tráfego de apps http não criptografados. Os usuários devem ter uma assinatura do iCloud+ e um aparelho com iOS 15, iPadOS 15 ou macOS Monterey (macOS 12) ou posterior para utilizar a Retransmissão Privada do iCloud. Mais informações sobre a Retransmissão Privada podem ser encontradas em support.apple.com/pt-br/HT212614 e www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.

Quando a Retransmissão Privada está ativada, as solicitações de navegação na web do usuário são enviadas por meio de duas retransmissões de internet separadas e seguras. O endereço IP do usuário fica visível para o provedor de rede do usuário e para a primeira retransmissão, que é operada pela Apple. Os registros de DNS do usuário são criptografados, então nenhuma das partes pode ver o endereço do site que o usuário está tentando visitar. A segunda retransmissão, que é operada por um provedor de conteúdo de terceiros, gera um endereço IP temporário, descriptografa o nome do usuário do site solicitado e conecta o usuário ao site. A Retransmissão Privada valida se o cliente conectado é um iPhone, iPad ou Mac. A Retransmissão Privada substitui o endereço IP original do usuário por um atribuído a partir do intervalo de endereços IP usados pelo serviço. O endereço IP de retransmissão atribuído pode ser compartilhado por mais de um usuário de Retransmissão Privada na mesma área.

Quando as solicitações de navegação na web do usuário utilizam a Retransmissão Privada, a Apple não consegue identificar o endereço IP do cliente do usuário ou a conta do usuário correspondente a partir dos endereços IP da Retransmissão Privada. A Apple não tem informações para fornecer sobre o ID Apple associado ao endereço IP de Retransmissão Privada.

Nota: a Retransmissão Privada do iCloud não está disponível em todos os países ou regiões. Se os usuários tiverem o recurso Retransmissão Privada ativado e viajarem para algum lugar em que a Retransmissão Privada não esteja disponível, ela será desligada de forma automática e ligada outra vez quando os usuários entrarem novamente em um país ou região que o suporte.

I. Buscar

Buscar é um recurso ativado pelo usuário por meio do qual um cliente do iCloud consegue localizar um iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac ou AirTag perdidos e/ou realizar determinadas ações, por exemplo, bloquear ou apagar o aparelho ou colocá-lo no Modo Perdido. Mais informações sobre esse serviço estão disponíveis na página www.apple.com/br/icloud/find-my/.

Para que funcione para um cliente que perdeu um aparelho, é preciso que o recurso Buscar já tenha sido ativado nesse aparelho específico antes da perda. Não é possível ativar o recurso Buscar em um aparelho após a perda do aparelho, remotamente ou mediante uma solicitação de uma autoridade governamental ou policial. As informações dos serviços de localização do aparelho são armazenadas em cada aparelho individual, e a Apple não consegue recuperá-las de nenhum aparelho específico. As informações dos serviços de localização referentes a um aparelho localizado por meio do recurso Buscar são voltadas para o cliente, e a Apple não promove a transmissão do conteúdo de mapas ou alertas por meio do serviço. Este link de suporte traz informações e etapas que um cliente pode seguir em caso de perda ou roubo de um aparelho com iOS: support.apple.com/pt-br/HT201472.

Os registros de conexões do recurso Buscar ficam disponíveis por um período de no máximo 25 dias e, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante. A atividade das transações do recurso Buscar envolvendo solicitações para bloquear ou apagar um aparelho remotamente, caso esteja disponível, poderá ser obtida mediante a solicitação judicialmente válida pertinente para o país do solicitante.

J. AirTag e Programa de Acessórios da Rede do App Buscar

Com o app Buscar no iPhone, iPad, iPod touch e Mac, os clientes localizam facilmente itens pessoais. Basta prender um AirTag no item ou usar um produto que faça parte do programa de acessórios da rede do app Buscar.

Com o AirTag e iOS 14.5 e macOS 11.3 ou posterior, os clientes podem ser ajudados a encontrar itens pessoais perdidos (chaves, mochilas, bagagens, etc.) usando o app Buscar. O AirTag deve estar dentro do alcance do Bluetooth do iPhone, iPad ou iPod touch emparelhado para emitir um som ou para usar a Busca Precisa com os modelos de iPhone compatíveis. Quando o objeto não estiver perto da pessoa, será possível obter a localização aproximada do AirTag se ele estiver dentro do alcance de um aparelho na rede do app Buscar, formada por centenas de milhões de aparelhos Apple espalhados pelo mundo. Você encontra mais informações em: support.apple.com/pt-br/HT212227 e support.apple.com/pt-br/HT210967.

O programa de acessórios disponibiliza a rede do app Buscar para que produtos de outros fabricantes de aparelhos (bicicletas, fones de ouvido, etc.) utilizem o serviço, assim, os clientes conseguem localizar produtos de terceiros compatíveis por meio do app Buscar com o iOS 14.3 e o macOS 11.1 ou posterior.

Para adicionar o AirTag ou produtos de terceiros compatíveis à aba Itens do app Buscar, os clientes precisam ter um ID Apple, iniciar sessão na conta do iCloud com o recurso Buscar ativado e registrar o AirTag ou os produtos de terceiros no ID Apple. A interação é criptografada de ponta a ponta, e a Apple não vê a localização do AirTag ou dos produtos de terceiros compatíveis. Mais informações estão disponíveis no artigo support.apple.com/pt-br/HT211331.

Com um número de série, a Apple poderá fornecer os dados da conta emparelhada mediante a

solicitação judicialmente válida pertinente para o país do solicitante. O histórico de emparelhamento do AirTag fica disponível por um período de no máximo 25 dias. Este link de suporte traz informações sobre como encontrar o número de série de um AirTag: support.apple.com/pt-br/HT211658.

Deve-se observar que os números de série dos aparelhos Apple não contêm as letras "O" ou "I"; em vez disso, a Apple utiliza os algarismos 0 (zero) e 1 (um) nos números de série. As solicitações por números de série com a letra "O" ou "I" não produzirão resultados. Nos casos em que uma solicitação judicial tiver cinco ou mais números de série, a Apple solicitará que esses números também sejam enviados em formato eletrônico editável (por exemplo, documento do Numbers, Excel, Pages ou Word).

K. Extração de Dados de Aparelhos com iOS Bloqueados pelo Código de Acesso

Em todos os aparelhos que executam o iOS 8.0 e versões posteriores, a Apple não tem como executar uma extração de dados do aparelho com iOS, uma vez que os dados geralmente requisitados pelas autoridades policiais estão criptografados e a Apple não dispõe da chave de criptografia. Todos os modelos de aparelhos iPhone 6 e posteriores são fabricados com o iOS 8.0 ou uma versão posterior do iOS instalada.

Nos aparelhos com iOS 4 até iOS 7, dependendo do status do aparelho, a Apple poderá executar extrações de dados do iOS, de acordo com a Lei de Privacidade de Comunicações Eletrônicas da Califórnia (CalECPA, §§ 1546–1546.4 do Código Penal da Califórnia). Para que a Apple execute uma extração de dados do iOS em um aparelho que atenda a esses critérios, a autoridade policial deverá obter um mandado de busca expedido mediante demonstração de causa provável de acordo com a CalECPA. À parte da CalECPA, a Apple não identificou nenhuma autoridade legal estabelecida que exija que a Apple extraia dados como terceiro em uma investigação policial.

L. Solicitação de Endereço IP

Antes de encaminhar um processo legal com um endereço IP como um identificador, a Apple solicita que a autoridade jurídica defina que o endereço IP em questão não é um endereço IP público ou de roteador e não está usando a Tradução de Endereço de Rede de Operadora (CGNAT) e confirme à Apple durante a entrega de citação do processo legal de que é um endereço IP não público. Além disso, essas solicitações devem incluir uma restrição de data de no máximo três dias. Em resposta a essa solicitação, a Apple pode produzir registros de conexão (ver abaixo, seção III.Q) a partir dos quais a autoridade policial pode tentar identificar uma conta Apple ou ID Apple específico para usar como um identificador em uma solicitação de acompanhamento de processo legal. Os dados do cliente da Apple com base em um endereço IP, caso estejam disponíveis, podem ser obtidos com a solicitação legalmente válida apropriada para o país do solicitante.

M. Outras Informações Disponíveis sobre os Aparelhos

Endereço MAC: um endereço MAC (Media Access Control) é um identificador exclusivo atribuído a interfaces de rede para comunicações no segmento de rede física. Qualquer produto Apple com interfaces de rede terá um ou mais endereços MAC, como Bluetooth, Ethernet, Wi-Fi ou FireWire. Ao fornecer à Apple um número de série (ou um IMEI, MEID ou UDID no caso de um aparelho com iOS), informações responsivas do endereço MAC, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

N. Solicitações por Dados de CFTV de Apple Stores

Os dados de circuito fechado de televisão (CFTV) variam conforme a região da loja. Normalmente, os dados de CFTV são mantidos em uma Apple Store por, no máximo, 30 dias. Em várias jurisdições, esse período é de apenas 24 (vinte e quatro) horas, dependendo da legislação local. Passado esse período, pode ser que os dados não estejam disponíveis. As solicitações voltadas exclusivamente para dados de CFTV podem ser enviadas para o endereço lawenforcement@apple.com. A autoridade governamental ou policial deverá especificar a data, a hora e as informações de transações relacionadas aos dados requisitados.

O. Game Center

Game Center é a rede social de jogos da Apple. Informações sobre as conexões do Game Center relacionadas a um cliente ou aparelho podem estar disponíveis. Os registros de conexão, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante.

P. Ativação de Aparelhos com iOS

Quando um cliente ativa um aparelho com iOS usando uma operadora de celular ou faz upgrade do software, determinadas informações são fornecidas à Apple pela operadora ou pelo aparelho, dependendo do evento. Endereços IP do evento, números de ICCID e outros identificadores do aparelho podem estar disponíveis. Essas informações, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

Dual SIM: no caso de aparelhos com Dual SIM, as informações da operadora do nano SIM e/ou eSIM, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante. eSIM é um SIM digital que permite aos clientes ativar um plano de celular de uma operadora sem precisar usar um nano-SIM físico. Mais informações estão disponíveis em support.apple.com/pt-br/HT209044. Na China continental, em Hong Kong e em Macau, o iPhone 12, iPhone 12 Pro, iPhone 12 Pro Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone XS Max e iPhone XR têm Dual SIM com dois cartões nano-SIM.

Q. Registros de Conexão

A atividade de conexão de um cliente ou aparelho com os serviços da Apple, como Apple Music, app Apple TV, Apple Podcasts, Apple Books, iCloud, Meu ID Apple e Fóruns da Apple, quando disponíveis, poderá ser obtida na Apple. Esses registros de conexão com endereços IP, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante.

R. Registros do Meu ID Apple e do iForgot

Os registros do Meu ID Apple e do iForgot referentes a um cliente podem ser obtidos com a Apple. Esses registros podem incluir informações relacionadas a ações de redefinição de senha. Os registros de conexão com endereços IP, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país da pessoa solicitante.

S. FaceTime

As comunicações do FaceTime são criptografadas de ponta a ponta, e a Apple não tem como decodificar os dados do FaceTime quando estão em trânsito entre os aparelhos. A Apple não intercepta as comunicações do FaceTime. A Apple dispõe de registros de convites de chamada do FaceTime quando tal convite é iniciado. Esses registros não indicam se realmente ocorreu uma comunicação entre os clientes. Os registros de convites de chamada do FaceTime são retidos por até 25 dias. Esses registros, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante.

T. iMessage

As comunicações do iMessage são criptografadas de ponta a ponta, e a Apple não tem como decodificar os dados do iMessage quando estão em trânsito entre os aparelhos. A Apple não intercepta as comunicações do iMessage nem tem os registros das comunicações do iMessage. A Apple dispõe de registros de consultas de recursos do iMessage. Esses registros indicam que uma consulta foi iniciada por um aplicativo do aparelho (Mensagens, Contatos, Telefone, etc.) e encaminhada para os servidores da Apple em busca de um identificador de pesquisa (o qual pode ser um número de telefone, endereço de e-mail ou ID Apple) para determinar se esse identificador de pesquisa é "compatível com o iMessage". Os registros de consulta de recursos do iMessage não indicam que houve comunicação entre os clientes. Não tem como a Apple determinar se realmente ocorreu uma comunicação do iMessage com base nos registros de consultas de recursos do iMessage. Além disso, a Apple não pode identificar o aplicativo específico que iniciou a consulta. Os registros de consultas de recursos do iMessage não confirmam se realmente houve uma tentativa de evento do iMessage. Os registros de consultas de recursos do iMessage são retidos por até 25 dias. Esses registros, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante.

U. App Apple TV

Com o app Apple TV, os clientes podem navegar, comprar, assinar e reproduzir programas de TV e filmes do Apple TV+, canais da Apple TV e apps e serviços de terceiros. O histórico de compras e downloads pode estar disponível.

As solicitações de dados do cliente do app Apple TV devem incluir o identificador do aparelho Apple (número de série, IMEI, MEID ou GUID) ou ID Apple/endereço de e-mail da conta pertinente. Se o ID Apple/endereço de e-mail da conta forem desconhecidos, será necessário fornecer à Apple as informações do cliente na forma de nome completo e número de telefone e/ou nome completo e endereço físico para identificar a conta de cliente em questão. As autoridades governamentais ou policiais também podem fornecer um número de pedido válido da Apple ou um número completo de cartão de crédito/débito associado à(s) compra(s) no app Apple TV. Um nome de cliente em combinação com esses parâmetros também poderá ser fornecido, mas apenas o nome do cliente não é suficiente para obter informações.

Nota: nos casos em que a solicitação judicial tiver dados completos de cartão de crédito/débito, para fins de segurança dos dados, tais dados deverão ser enviados para lawenforcement@apple.com em um documento protegido por senha/criptografado, e a senha deverá ser enviada em outro e-mail. Odocumento pode ser .PDF e formato editável, por exemplo, documento do Numbers, Excel, Pages ou o Word. Além disso, a Apple não baixará documentos de solicitação judicial por meio de qualquer link fornecido em um e-mail devido a padrões de segurança do sistema.

V. Iniciar Sessão com a Apple

O recurso Iniciar Sessão com a Apple é uma forma mais privada de os clientes iniciarem sessão em apps e sites de terceiros usando o ID Apple existente. Um botão Iniciar Sessão com a Apple exibido em um app ou site participantes possibilita que um cliente configure uma conta e inicie sessão usando o ID Apple. Em vez de usar uma conta de mídia social ou preencher formulários e selecionar uma nova senha, basta o cliente tocar no botão Iniciar Sessão com a Apple, analisar as informações e iniciar sessão de forma rápida e segura com o Face ID, o Touch ID ou o código de acesso do aparelho. Mais informações estão disponíveis no artigo support.apple.com/pt-br/HT210318.

Ocultar Meu E-mail é um recurso de Iniciar Sessão com a Apple. Ele usa o serviço de retransmissão de e-mail privado da Apple para criar e compartilhar um endereço de e-mail único e aleatório que encaminha e-mails para o endereço de e-mail pessoal de um cliente. As informações básicas do cliente, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante.

IV.Perguntas frequentes

P: Posso enviar à Apple um e-mail com perguntas sobre minha solicitação de informações por autoridade policial?
R: Sim. Dúvidas ou perguntas sobre processos judiciais do governo podem ser enviadas por e-mail para lawenforcement@apple.com.

P: Um aparelho precisa estar registrado na Apple para poder funcionar ou ser usado?
R: Um aparelho não precisa estar registrado na Apple para poder funcionar ou ser usado.

P: A Apple pode me informar o código de acesso de um aparelho iOS que esteja bloqueado?
R: Não. Não tem como Apple obter o código de acesso de um usuário.

P: Vocês podem me ajudar a devolver um aparelho perdido ou roubado para a pessoa que o perdeu?
R: Nesses casos, entre em contato com lawenforcement@apple.com. Inclua no e-mail o número de série do aparelho (ou IMEI, se for o caso) e outras informações relevantes. As informações sobre como encontrar o número de série estão disponíveis aqui: support.apple.com/pt-br/HT204308.

Se houver informações do cliente disponíveis, a Apple entrará em contato com o cliente e fornecerá dados para que ele entre em contato com as autoridades policiais a fim de recuperar o aparelho. Porém, se não for possível determinar o cliente pelas informações disponíveis, você poderá ser instruído a enviar uma solicitação judicial válida.

P: A Apple mantém uma lista dos aparelhos perdidos ou roubados?
R: Não. A Apple não mantém uma lista dos aparelhos perdidos ou roubados.

P: O que deverá ser feito com as informações de resposta quando a autoridade policial tiver concluído a investigação ou o processo penal?
R: As informações e os dados fornecidos às autoridades governamentais ou policiais contendo informações de identificação pessoal (incluindo todas as cópias que tiverem sido feitas) deverão ser destruídos uma vez concluída respectiva investigação ou processo penal e esgotados todos os recursos.

P: A Apple notifica os clientes quando recebem solicitações de informações por autoridades policiais em que eles estão envolvidos?
R: Sim. A política de notificação da Apple aplica-se às solicitações de contas por parte de autoridades policiais, autoridades governamentais e entidades privadas. A Apple notificará os clientes e os titulares de contas, salvo se houver uma ordem de não divulgação ou uma legislação aplicável que proíba a notificação, ou quando a Apple, a critério exclusivo dela, tiver motivos razoáveis para acreditar que tal notificação possa acarretar risco imediato de lesão grave ou morte para qualquer cidadão, quando o caso envolver exposição infantil a situações de risco ou quando a notificação não for aplicável aos fatos pertinentes do caso.