



Diretrizes relativas a processos judiciais

Agências governamentais e de aplicação da lei fora dos Estados Unidos

As presentes diretrizes destinam-se a agências governamentais e de aplicação da lei fora dos Estados Unidos que procurem informações junto de entidades da Apple na região ou país relevante sobre os clientes de dispositivos, produtos ou serviços da Apple. A Apple procederá à atualização das presentes diretrizes sempre que isso for necessário.

Nas presentes diretrizes, a Apple é a entidade relevante responsável pelas informações do cliente numa determinada região ou país. Enquanto empresa global, a Apple detém várias entidades jurídicas em diferentes jurisdições, que são responsáveis pelas informações pessoais que recolhem e são tratadas em seu nome pela Apple Inc. Por exemplo, as informações recolhidas nos pontos de venda nas entidades de venda a retalho da Apple fora dos EUA são controladas individualmente pelas referidas entidades em cada país. As informações pessoais relativas a Apple.com e aos Serviços multimédia da Apple poderão ser também controladas por entidades jurídicas fora dos EUA, conforme indicado nos termos de cada serviço no âmbito de uma jurisdição específica. Normalmente, as entidades jurídicas da Apple fora dos EUA na Austrália, Canadá, Irlanda e Japão são responsáveis pelos dados de clientes relativos a serviços Apple dentro das respetivas regiões.

Todos os restantes pedidos de informação relativos a clientes da Apple, incluindo questões de clientes acerca da divulgação de informações, deverão ser direcionados para www.apple.com/pt/privacy/contact/. Estas diretrizes não se aplicam aos pedidos de agências governamentais e de aplicação da lei dos Estados Unidos efetuados à Apple Inc.

No que respeita aos pedidos de informação de agências governamentais e de aplicação da lei, a Apple cumpre as leis relacionadas com as entidades globais que controlam os nossos dados e divulgamos detalhes nos termos do legalmente exigido. Todos os pedidos de agências governamentais e de aplicação da lei fora dos Estados Unidos relativos a conteúdos, salvo nos casos de emergência (definidas a seguir em Pedidos de emergência), têm de cumprir a legislação aplicável, incluindo a lei dos Estados Unidos relativa à privacidade nas comunicações eletrónicas (ECPA — Electronic Communications Privacy Act). Qualquer pedido ao abrigo de um tratado de auxílio judiciário mútuo ou ao abrigo de um Acordo executivo sob a "Clarifying Lawful Overseas Use of Data Act" ("Acordo da Lei CLOUD") cumpre a ECPA. A Apple disponibilizará conteúdos do cliente, tal como se encontram na sua conta, exclusivamente em resposta ao referido processo legalmente válido.

Para pedidos de entidades privadas, a Apple cumpre as leis relativas às entidades locais que controlam os dados dos clientes e disponibiliza detalhes conforme legalmente exigido.

A Apple tem um processo centralizado para receber, monitorizar, processar e responder a pedidos judiciais legítimos de agências governamentais, de aplicação da lei e entidades privadas entre o momento da sua receção à apresentação de uma resposta. Uma equipa especializada do nosso departamento jurídico analisa e avalia todos os pedidos recebidos e, se a Apple considerar que não existe qualquer base jurídica válida ou que os pedidos são imprecisos, desadequados ou pouco específicos, estes serão contestados, questionados ou rejeitados.

A Apple fornece respostas à agência de aplicação da lei requerente no endereço de email oficial do

agente requerente. A preservação de todas as provas de acordo com as respostas fornecidas pela Apple é da responsabilidade da agência de aplicação da lei requerente.

ÍNDICE

I. Informações gerais

II. Pedidos judiciais à Apple

- A. Pedidos de informação de agências governamentais e de aplicação da lei
- B. Gerir e responder a pedidos de informação de agências governamentais e de aplicação da lei
- C. Pedidos de conservação
- D. Pedidos de emergência
- E. Pedidos de restrição/eliminação de contas
- F. Aviso aos clientes

III. Informações disponíveis da Apple

- A. Registo de dispositivos
- B. Registos do serviço de assistência
- C. Serviços multimédia da Apple
- D. Transações da Apple Store
- E. Encomendas efetuadas em Apple.com
- F. Vales-oferta
- G. Apple Pay
- H. iCloud
- I. Encontrar
- J. Programa acessório da rede Encontrar e AirTag
- K. Extrair dados de dispositivos iOS protegidos por código
- L. Pedido de endereço IP
- M. Outras informações disponíveis do dispositivo
- N. Pedidos de dados de CCTV da Apple Store
- O. Game Center
- P. Ativação de dispositivos iOS
- Q. Registos de ligação
- R. Registos de O meu ID Apple e 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 dispositivos móveis de comunicação e multimédia, computadores pessoais e leitores de música digitais portáteis e vende uma variedade de software, serviços, periféricos, soluções de rede e conteúdos digitais e aplicações de terceiros relacionados. Os produtos e serviços da Apple incluem Mac, iPhone, iPad, iPod touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, um portefólio de apps de software para consumidores e profissionais, os sistemas operativos iOS e macOS X, iCloud, bem como uma grande variedade de ofertas de acessórios, serviços e suporte. A Apple também vende e fornece conteúdos digitais e apps através da Apple Music, App Store, Apple Books e Mac App Store. As informações dos utilizadores são detidas pela Apple em conformidade com a [política de privacidade](#) da Apple e com os [termos de serviço](#) aplicáveis à oferta de serviço específica. A Apple está empenhada em garantir a privacidade dos clientes dos produtos e serviços da Apple ("clientes da Apple"). Por conseguinte, salvo em situações de emergência previstas por lei, as informações sobre os clientes da Apple serão divulgadas apenas no âmbito de um processo judicial válido.

As informações incluídas nas presentes diretrizes foram concebidas para fornecer informações às agências governamentais e de aplicação da lei fora dos Estados Unidos relativas ao processo judicial exigido pela Apple de modo a divulgar informações eletrónicas às agências governamentais e de aplicação da lei fora dos Estados Unidos. Estas diretrizes não se destinam ao fornecimento de apoio jurídico. A secção de perguntas frequentes destas diretrizes destina-se a fornecer respostas a algumas das perguntas mais comuns que a Apple recebe. Estas diretrizes e as perguntas frequentes não abrangerão todas as circunstâncias imagináveis que possam surgir.

Caso tenha mais questões, contacte lawenforcement@apple.com.

A caixa de correio acima destina-se exclusivamente a ser utilizada pelos funcionários das agências governamentais e de aplicação da lei. Se optar por enviar um e-mail para esta caixa de correio, deverá ser de um endereço de e-mail válido e oficial de uma agência governamental ou de aplicação da lei.

Os pedidos judiciais à Apple devem procurar informações relativas a um determinado dispositivo ou cliente Apple e aos serviços específicos que a Apple possa prestar a esse cliente. A Apple pode fornecer informações sobre os dispositivos ou clientes Apple, desde que ainda disponha das informações solicitadas de acordo com as suas políticas de conservação de dados. A Apple conserva dados nos termos descritos em determinadas secções "Informações disponíveis" a seguir. Todos os restantes dados são retidos durante o período necessário para cumprimento das finalidades indicadas na nossa [política de privacidade](#). As agências governamentais e de aplicação da lei deverão ser o mais detalhadas e específicas possível no momento da criação dos pedidos, para evitarem interpretações erradas, objeções, recusas e/ou rejeições em resposta a um pedido impreciso, desadequado ou pouco específico. Todos os pedidos de agências governamentais e de aplicação da lei fora dos Estados Unidos relativos a conteúdo, salvo nos casos de emergência (definidas a seguir em Pedidos de emergência), têm de cumprir a legislação aplicável, incluindo a lei dos Estados Unidos relativa à privacidade nas comunicações eletrónicas (ECPA — Electronic Communications Privacy Act). Qualquer pedido ao abrigo de um tratado de auxílio judiciário mútuo ou ao abrigo de um Acordo executivo sob a "Clarifying Lawful Overseas Use of Data Act" ("Acordo da Lei CLOUD") cumpre a ECPA. A Apple disponibilizará conteúdos do cliente, tal como se encontram na sua conta, exclusivamente em resposta ao referido processo legalmente válido.

Nenhuma disposição das presentes diretrizes visa criar direitos aplicáveis contra a Apple, podendo as políticas da Apple ser atualizadas ou alteradas no futuro sem qualquer aviso às agências governamentais e de aplicação da lei.

II. Pedidos judiciais à Apple

A. Pedidos de informação de agências governamentais e de aplicação da lei

A Apple aceita receber pedidos de informação de agências governamentais ou de aplicação da lei legalmente válidos por e-mail de agências governamentais e de aplicação da lei, contanto que estes sejam transmitidos a partir do endereço de e-mail oficial da agência governamental ou de aplicação da lei que faz o pedido. Os funcionários de agências governamentais e de aplicação da lei fora dos Estados Unidos que transmitem um pedido de informações à Apple devem preencher um [modelo Government & Law Enforcement Information Request](#) (Pedido de informação de agências governamentais e de aplicação da lei) e transmiti-lo diretamente a partir do respetivo endereço de email oficial das agências governamentais e de aplicação da lei para lawenforcement@apple.com.

A caixa de correio acima destina-se exclusivamente a ser utilizada pelos funcionários das agências governamentais e de aplicação da lei. Se os pedidos tiverem 5 ou mais identificadores, tais como números de série/IMEI do dispositivo, ID Apple, endereços de e-mail ou números de fatura/encomenda, estes deverão ser transmitidos num formato editável (exemplo: documento do Numbers, Excel, Pages ou Word, etc.). Geralmente, os identificadores semelhantes a estes são necessários para realizar pesquisas para informações relacionadas com dispositivos, contas ou transações financeiras.

Nota: tendo em conta as normas de segurança do sistema, a Apple não irá descarregar pedidos judiciais ou documentos relacionados enviados por email através de uma ligação.

Para que a Apple divulgue informações dos clientes em resposta a um pedido de uma agência de aplicação da lei, é necessário que o agente que faz o pedido indique a base jurídica que autoriza a recolha de informações probatórias sob a forma de dados pessoais, por parte de uma agência de aplicação da lei, de um Controlador de dados como a Apple. Exemplos de pedidos que a Apple considera legalmente válidos são: Production Orders (Austrália, Canadá, Nova Zelândia), lettres de réquisition ou commissions rogatoires (França), Solicitud Datos (Espanha), Ordem Judicial (Brasil), Auskunftersuchen (Alemanha), Obligation de dépôt (Suíça), 個人情報の開示依頼 (Japão), Personal Data Request, Orders, Warrants and Communications Data Authorisations (Reino Unido), bem como ordens judiciais equivalentes e/ou pedidos de outros países.

B. Gerir e responder a pedidos de informação de agências governamentais e de aplicação da lei

A Apple analisa cuidadosamente todos os pedidos judiciais para garantir a existência de uma base jurídica válida para cada pedido e dá resposta aos pedidos legalmente válidos. Se a Apple considerar que não existe uma base jurídica válida ou se o pedido for impreciso, desadequado ou pouco específico, a Apple irá contestar, questionará ou rejeitar o pedido.

Para efeitos de tratamento e devido às limitações do sistema, a Apple não pode aceitar pedidos judiciais que contenham mais de 25 identificadores de contas. Se a agência de aplicação da lei submeter pedidos judiciais com mais de 25 identificadores de contas, a Apple responderá aos primeiros 25 e a agência de aplicação da lei terá de voltar a enviar um novo pedido jurídico para identificadores adicionais.

C. Pedidos de conservação

Todos os pedidos de agências governamentais e de aplicação da lei fora dos Estados Unidos relativos a conteúdos, salvo nos casos de emergência (definidas a seguir em Pedidos de emergência), têm de cumprir a legislação aplicável, incluindo a lei dos Estados Unidos relativa à privacidade nas comunicações eletrónicas (ECPA — Electronic Communications Privacy Act). A qualquer pedido ao abrigo de um tratado de auxílio judiciário mútuo ou ao abrigo de um Acordo executivo sob "Clarifying Lawful Overseas Use of Data Act" ("Acordo da Lei CLOUD") cumpre a ECPA. Um pedido para conservar os dados antes do iminente pedido de cumprimento da ECPA deverá ser enviado por e-mail para: lawenforcement@apple.com.

Os pedidos de conservação têm de incluir o endereço de e-mail relevante do ID Apple/conta, nome completo e número de telefone, e/ou nome completo e endereço físico do cliente da conta Apple da pessoa. Ao receber um pedido de conservação, a Apple conserva uma extração de dados única dos dados de cliente existentes solicitados, disponíveis no momento do pedido, durante 90 dias. Após este período de 90 dias, a conservação será automaticamente suprimida do servidor de armazenamento. No entanto, este período pode ser alargado por um período adicional de 90 dias mediante novo pedido. Em caso de tentativa de apresentar mais de dois pedidos de conservação para a mesma conta, o segundo pedido será tratado como um pedido de extensão da conservação original e não como uma conservação separada de novos dados.

D. Pedidos de emergência

A Apple considera que um pedido é de emergência se o mesmo estiver relacionado com circunstâncias que envolvam ameaças iminentes e graves para a vida/segurança de pessoas; a segurança de um Estado; ou a segurança de infraestruturas/instalações críticas.

Se o agente governamental ou de aplicação da lei requerente apresentar uma confirmação satisfatória de que o seu pedido está relacionado com circunstâncias de emergência que envolvem um ou mais dos critérios referidos anteriormente, a Apple examinará o referido pedido no âmbito de uma emergência.

Para efetuar um pedido de divulgação de informações por parte da Apple com base numa emergência, o agente governamental ou de aplicação da lei requerente deverá preencher o [formulário Emergency Government & Law Enforcement Information Request](#) (Pedido de informação de emergência de agências governamentais e de aplicação da lei) e transmiti-lo diretamente a partir do respetivo endereço de email oficial da respetiva agência governamental e de aplicação da lei para exigent@apple.com com as palavras "Emergency Request (Pedido de emergência)" na linha do assunto.

Se uma agência governamental ou de aplicação da lei procurar dados de clientes em resposta a um pedido de informação de emergência de uma agência governamental e de aplicação da lei, um supervisor do agente governamental e de aplicação da lei que submeteu o Emergency Government & Law Enforcement Information Request (Pedido de informação de emergência de agências governamentais e de aplicação da lei) poderá ser contactado e terá de confirmar à Apple que o pedido de emergência era legítimo. O agente governamental e de aplicação da lei que apresenta o Emergency Government & Law Enforcement Information Request (Pedido de informação de emergência de agências governamentais e de aplicação da lei) deve fornecer as informações de contacto do supervisor no respetivo pedido.

Se uma agência governamental ou de aplicação da lei necessitar de contactar a Apple para uma consulta de emergência, deve contactar o Centro de operações de segurança global da Apple (GSOC) através do número 001 408 974-2095. Este número de telefone presta apoio em vários idiomas.

E. Pedidos de restrição/eliminação de contas

Se uma agência governamental ou de aplicação da lei solicitar à Apple a restrição/eliminação do ID Apple de um cliente, a Apple exige uma ordem judicial ou outro processo judicial interno equivalente (com frequência, uma sentença condenatória ou mandado) que demonstre que a conta a restringir/eliminar foi utilizada de forma ilegal.

A Apple analisa cuidadosamente todos os pedidos de agências governamentais e de aplicação da lei de modo a garantir a existência de uma base jurídica válida para cada pedido. Nos casos em que a Apple determinar que não existe base jurídica válida ou quando a ordem judicial não demonstrar que a conta a ser restringida/eliminada foi utilizada de forma ilegal, a Apple rejeitará/contestará o pedido.

Sempre que a Apple receber uma ordem judicial satisfatória ou outro processo judicial interno equivalente (frequentemente, uma sentença condenatória ou mandado) de uma agência governamental ou de aplicação da lei que demonstrar que a conta a restringir/eliminar foi utilizada de forma ilegal, a Apple tomará as medidas necessárias para restringir/eliminar a conta em conformidade com a ordem judicial e notificará o agente requerente em conformidade.

F. Aviso aos clientes

A Apple notificará os clientes quando as informações da sua conta Apple estiverem a ser solicitadas em resposta a um pedido judicial válido de uma agência governamental ou de aplicação da lei, salvo se o aviso for expressamente proibido pelo pedido judicial válido, por uma ordem judicial recebida pela Apple, pela lei aplicável ou se a Apple, ao seu critério exclusivo, considerar que o aviso cria um risco de lesão ou morte para uma pessoa identificável, em situações em que o processo possa constituir um perigo para as crianças ou se o aviso não se aplicar aos factos que fundamentam o processo.

Passados 90 dias, a Apple enviará um aviso tardio relativo a divulgações de emergência, salvo se o aviso for proibido por ordem judicial, pela lei aplicável ou se a Apple, ao seu critério exclusivo, considerar que o envio de avisos poderá criar um risco de lesão ou morte para uma pessoa identificável ou grupo de pessoas ou em situações em que o processo possa constituir um perigo para as crianças. A Apple enviará um aviso tardio após o termo do período de não divulgação especificado numa ordem judicial, salvo se a Apple, ao seu critério exclusivo, considerar de forma razoável que o envio de avisos poderá criar um risco de lesão ou morte para uma pessoa identificável ou grupo de pessoas, em situações em que o processo possa constituir um perigo para as crianças ou se o aviso não se aplicar aos factos que estão na base do processo.

A Apple notificará os seus clientes quando a sua conta Apple tiver sido restringida/eliminada em cumprimento de uma ordem judicial (frequentemente, uma sentença condenatória ou mandado) que demonstre que a conta a restringir/eliminar foi utilizada de forma ilegal ou viola os termos de serviço da Apple; salvo se o aviso for proibido pelo próprio processo judicial, por uma ordem judicial recebida pela Apple, pela lei aplicável, em situações em que o processo possa constituir um perigo para as crianças, se a Apple, ao seu critério exclusivo, considerar de forma razoável que, ao enviar avisos, pode criar um risco de lesão ou morte para uma pessoa identificável ou grupo de pessoas ou se o aviso não se aplicar aos factos que fundamentam o processo.

III. Informações disponíveis da Apple

Esta secção abrange os tipos gerais de informação que podem estar disponíveis na Apple no momento da publicação destas diretrizes.

A. Registo de dispositivos

As informações básicas de registo ou de cliente, incluindo nome, endereço, endereço de email e número de telefone, são fornecidas à Apple pelos clientes ao registarem um dispositivo Apple antes do iOS 8 e do macOS Sierra 10.12. A Apple não verifica estas informações e podem não ser exatas nem refletir o proprietário do dispositivo. As informações de registo de dispositivos com iOS 8 e versões posteriores, bem como Macs com macOS Sierra 10.12 e versões posteriores são recebidas quando um cliente associa um dispositivo a um ID Apple do iCloud. Estas informações poderão não ser exatas nem refletir o proprietário do dispositivo. Registo de registo, se houver, poderão ser obtidas com o pedido adequado legalmente válido relativo ao país do requerente.

Deve ter-se em atenção que os números de série dos dispositivos Apple não contêm as letras "O" ou "I"; em vez disso, a Apple utiliza os números 0 (zero) e 1 (um) nos números de série. Os pedidos de números de série com a letra "O" ou "I" não produzirão resultados. Se um pedido judicial contiver 5 ou mais números, a Apple solicita que estes números de série sejam também apresentados em formato eletrónico editável (exemplo: documento do Numbers, Excel, Pages ou Word).

B. Registos do serviço de assistência

Os contactos que os clientes tenham tido com o serviço de assistência da Apple relativos a um dispositivo ou serviço poderão ser obtidos junto da Apple. Estas informações poderão incluir registos de interações entre o serviço de assistência e os clientes relativamente a um dispositivo ou serviço específico da Apple. Adicionalmente, informações relativas ao dispositivo, garantia e reparação poderão também estar disponíveis. Estas informações, se houver, poderão ser obtidas com o pedido adequado legalmente válido relativo ao país do requerente.

C. Serviços multimédia da Apple

A App Store, Apple Music, a app Apple TV, Apple Podcasts e Apple Books ("Serviços multimédia da Apple") são aplicações de software que os clientes utilizam para organizar e utilizar apps, reproduzir música e vídeo digital e fazer streaming de conteúdos. Os Serviços multimédia da Apple fornecem também conteúdos que os clientes podem transferir para os seus computadores e dispositivos iOS. Quando um cliente abre uma conta Apple, o cliente poderá fornecer informações básicas como o nome, endereço físico, endereço de e-mail e número de telefone. Além disso, poderão também estar disponíveis informações relativas a transações e ligações de compra/download e ligações de atualização/download repetido do Serviço de multimédia da Apple. As informações de endereço IP poderão estar limitadas aos últimos 18 meses. Informações dos clientes do Serviço de multimédia da Apple e registos de ligações com endereços IP, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

Os pedidos de dados do Serviço de multimédia da Apple têm de incluir o identificador de dispositivo Apple (número de série, IMEI, MEID ou GUID) ou o endereço de e-mail da conta/ID Apple. Se o ID Apple/endereço de e-mail da conta não for conhecido, é necessário apresentar à Apple as informações do cliente do Serviço de multimédia da Apple na forma de nome completo e número de telefone, e/ou nome completo e endereço físico, para identificar a conta de cliente do Serviço de multimédia da Apple da pessoa. Os agentes governamentais ou de aplicação da lei poderão também fornecer o número de encomenda do Serviço de multimédia da Apple válido ou um número de cartão de débito ou de crédito completo associado às compras no Serviço de multimédia da Apple. É também possível fornecer o nome de um cliente em combinação com estes parâmetros, mas o nome do cliente por si só não é suficiente para obter informações.

Nota: sempre que o seu pedido judicial contiver dados completos de cartões de crédito/débito, para efeitos de segurança, os dados dos cartões de crédito/débito deverão ser enviados num documento protegido por palavra-passe/encryptado (formato .PDF e editável, exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado. Além disso, tendo em conta as normas de segurança do sistema, a Apple não irá descarregar documentos de pedidos judiciais enviados por email através de uma ligação.

D. Transações da Apple Store

As transações de ponto de venda são em dinheiro, com cartão de crédito/débito ou cartão-oferta que ocorrem numa loja Apple Store. Os pedidos de registos de pontos de venda têm de incluir o número do cartão de crédito/débito completo utilizado e poderão também incluir informações adicionais, como data e hora da transação, valor e artigos adquiridos. As informações relativas ao tipo de cartão associado a uma determinada compra, nome do comprador, endereço de e-mail, data/hora da transação, valor da transação e localização da loja, se disponíveis, poderão ser obtidas com o pedido adequado legalmente válido relativo ao país do requerente.

Os pedidos de cópias de recibos têm de incluir o número da transação de venda a retalho associado à compra e, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

Nota: sempre que o seu pedido judicial contiver dados completos de cartões de crédito/débito, para efeitos de segurança, os dados dos cartões de crédito/débito deverão ser enviados num documento protegido por palavra-passe/encryptado (formato .PDF e editável, exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado. Além disso, tendo em conta as normas de segurança do sistema, a Apple não irá descarregar documentos de pedidos judiciais enviados por email através de uma ligação.

E. Encomendas efetuadas em Apple.com

A Apple conserva informações relativas às encomendas online efetuadas em apple.com, as quais poderão incluir o nome do comprador, endereço de envio, número de telefone, endereço de email, produtos comprados, montante da compra e endereço IP da compra. Os pedidos de informação relativos às encomendas online efetuadas em apple.com devem incluir um número de cartão de crédito/débito completo ou um número de encomenda, ou o número de série do artigo adquirido. É também possível fornecer o nome de um cliente em combinação com estes parâmetros, porém, o nome do cliente por si só não é suficiente para obter informações. Em alternativa, os pedidos de informação relativos às encomendas online efetuadas em apple.com poderão incluir o endereço de email da conta/ID Apple relevante.

Se o endereço de e-mail da conta/ID Apple não for conhecido, é 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 da pessoa. As informações de compras das encomendas online efetuadas em apple.com, caso estejam disponíveis, podem ser obtidas com um pedido adequado legalmente válido relativo ao país do requerente.

Nota: sempre que o seu pedido judicial contiver dados completos de cartões de crédito/débito, para efeitos de segurança, os dados dos cartões de crédito/débito deverão ser enviados num documento protegido por palavra-passe/encryptado (formato .PDF e editável, exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado. Além disso, tendo em conta as normas de segurança do sistema, a Apple não irá descarregar documentos de pedidos judiciais enviados por email através de uma ligação.

F. Vales-oferta

Os Vales-oferta da Apple Store e Vales-oferta da App Store e iTunes possuem um número de série. Estes números de série possuem múltiplos formatos dependendo de variáveis, por exemplo, o design e/ou a data de emissão. A Apple poderá fornecer informações disponíveis relativas a Vales-oferta da Apple Store e Vales-oferta da App Store e iTunes para dar resposta ao pedido adequado legalmente válido relativo ao país do requerente. Se um pedido judicial contiver 5 ou mais números de série de vales-oferta, a Apple solicita que estes números de série de vales-oferta sejam enviados num documento protegido por palavra-passe/encryptado (exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado.

i. Vales-oferta da Apple Store

Os Vales-oferta da Apple Store poderão ser utilizados para compras em Apple.com ou numa loja Apple Store. Os registos disponíveis poderão incluir informações do comprador do cartão-oferta (se adquirido na Apple e não junto de um comerciante externo), transações de compras associadas e artigos adquiridos. Em certos casos, a Apple poderá cancelar ou suspender um Cartão-oferta da Apple Store, consoante o estado do cartão-oferta específico. As informações do Cartão-oferta da Apple Store, se houver, poderão ser obtidas com o pedido adequado legalmente válido para o país do requerente.

Nota: sempre que o seu pedido judicial contiver dados completos de vales-oferta da Apple Store, para efeitos de segurança, os dados dos vales-oferta da Apple Store deverão ser enviados num documento protegido por palavra-passe/encryptado (formato .PDF e editável, exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado. Além disso, tendo em conta as normas de segurança do sistema, a Apple não irá descarregar documentos de pedidos judiciais enviados por email através de uma ligação.

ii. Vales-oferta da App Store e iTunes

Os Vales-oferta da App Store e iTunes podem ser utilizados na Apple Music, App Store, Apple Books e Mac App Store. Com o número de série, a Apple pode determinar se o Cartão-oferta da App Store e iTunes foi ativado (comprado num ponto de venda) ou utilizado (adicionado ao saldo de crédito de loja de uma conta Apple).

Se um Cartão-oferta da App Store e iTunes for ativado, os registos disponíveis poderão incluir o nome da loja, o local, a data e a hora. Se um Cartão-oferta da App Store e iTunes for utilizado, os registos disponíveis poderão incluir informações dos clientes da conta Apple relacionada, data e hora da ativação e/ou utilização e endereço IP de compra. Em certos casos, a Apple

poderá desativar um Cartão-oferta da App Store e iTunes, consoante o estado do cartão-oferta específico. As informações do Cartão-oferta da App Store e iTunes, se houver, poderão ser obtidas com o pedido adequado legalmente válido para o país do requerente.

Nota: sempre que o seu pedido judicial contiver dados completos de vales-oferta da App Store e iTunes, para efeitos de segurança, os dados dos vales-oferta da App Store e iTunes deverão ser enviados num documento protegido por palavra-passe/encryptado (formato .PDF e editável, exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado. Além disso, tendo em conta as normas de segurança do sistema, a Apple não irá descarregar documentos de pedidos judiciais enviados por email através de uma ligação.

G. Apple Pay

As transações do Apple Pay efetuadas em lojas (por exemplo, para comunicações sem contacto/NFC) e em apps ou pontos de venda online são autenticadas de forma segura no dispositivo do cliente e enviadas em formato encryptado para o comerciante ou o processador de pagamento do comerciante. Embora a segurança da transação seja verificada por um servidor Apple, a Apple não processa pagamentos nem armazena tais transações, nem os números de cartões de crédito/débito completos associados a compras efetuadas com o Apple Pay. Estas informações poderão estar disponíveis por via do banco emissor da rede de pagamento ou do comerciante relevante.

Mais informações acerca de países e regiões que permitem utilizar o Apple Pay estão disponíveis em support.apple.com/pt-pt/HT207957.

Para solicitar dados de transações relativas a compras realizadas em instalações da Apple Store ou em Apple.com, a Apple precisa do Número de conta do dispositivo principal ("DPAN") utilizado para a transação. O DPAN possui 16 dígitos e pode ser obtido junto do banco emissor. Nota: o DPAN é utilizado em transações de pagamentos sem contacto com o comerciante em substituição do número do cartão de crédito/débito (FPAN/Funding PAN). O DPAN é convertido no FPAN correspondente pelo processador do pagamento. Com as informações de DPAN relevantes, a Apple poderá conduzir uma investigação razoável para localizar informações adequadas através do respetivo sistema de ponto de venda. Estes registos, se disponíveis, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

A Apple poderá conseguir fornecer informações do Apple Pay relativas aos tipos de cartões de crédito/débito que um cliente adicionou ao Apple Pay em conjunto com as informações do cliente. Estas informações, se houver, poderão ser obtidas com o pedido adequado legalmente válido relativo ao país do requerente. Para solicitar estas informações, a Apple necessitaria de um identificador do dispositivo (número de série da Apple, SEID, IMEI ou MEID), ou um endereço de e-mail de conta/ID Apple.

Nota: sempre que o seu pedido judicial contiver o DPAN, para efeitos de segurança, os referidos dados deverão ser enviados num documento protegido por palavra-passe/encryptado (formato .PDF e editável, exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado. Além disso, tendo em conta as normas de segurança do sistema, a Apple não irá descarregar documentos de pedidos judiciais enviados por email através de uma ligação.

H. iCloud

O iCloud é o serviço na nuvem da Apple que permite aos clientes aceder às suas fotografias, documentos e muito mais a partir de todos os seus dispositivos. O iCloud também permite que os clientes façam cópias de segurança dos seus dispositivos iOS e iPadOS no iCloud. Com o serviço

iCloud, os clientes podem configurar uma conta de email iCloud.com. Os domínios de email do iCloud podem ser @icloud.com, @me.com e @mac.com. Todos os dados de conteúdos do iCloud armazenados pela Apple são encriptados na localização do servidor. Para os dados que a Apple consegue descriptar, a Apple mantém as chaves de encriptação nos seus centros de dados nos EUA. A Apple não recebe nem retém chaves de encriptação para os dados totalmente encriptados do cliente.

O iCloud é um serviço com base nos clientes. Os pedidos de dados do iCloud têm de incluir o endereço de e-mail da conta/ID Apple relevante. Se o endereço de e-mail da conta/ID Apple não for conhecido, é 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 da pessoa. Se for fornecido apenas um número de telefone ou um endereço de e-mail de conta/ID Apple, poderão ser apresentadas informações disponíveis de contas verificadas associadas a estes critérios.

I. As informações seguintes poderão estar disponíveis a partir do iCloud:

I. Informações do cliente

Se um cliente configurar uma conta do iCloud, poderão ser fornecidas à Apple informações básicas dos clientes como o nome, endereço físico, endereço de e-mail e número de telefone. Além disso, poderão estar disponíveis informações relativas às ligações da funcionalidade iCloud. Informações dos clientes e registos de ligações com endereços IP, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente. Os registos de ligação são conservados durante 25 dias, no máximo.

II. Registos de Mail

Os registos de email incluem registos de comunicações recebidas e enviadas, como hora, data, endereços de email dos remetentes e endereços de email dos destinatários. Os registos de email do iCloud são retidos durante até 25 dias; e, se disponíveis, podem ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

III. Conteúdos de e-mail e outros conteúdos do iCloud, A minha partilha de fotografias, Biblioteca de fotografias do iCloud, iCloud Drive, Contactos, Calendários, Marcadores, Histórico de navegação do Safari, Histórico de pesquisa da app Mapas, Mensagens, Cópias de segurança de dispositivos iOS

O iCloud armazena conteúdos dos serviços que o cliente escolheu manter na conta enquanto a conta do cliente permanecer ativa. A Apple não retém conteúdo eliminado depois de eliminado dos servidores da Apple. O conteúdo do iCloud pode incluir email, fotografias armazenadas, documentos, contactos, calendários, marcadores, histórico de navegação do Safari, histórico de pesquisa em Mapas, Mensagens e cópias de segurança de dispositivos iOS. As cópias de segurança de dispositivos iOS podem incluir fotografias e vídeos no Rolo da Câmara, definições do dispositivo, dados de apps, iMessage, Business Chat, mensagens SMS e MMS e correio de voz. Todos os dados de conteúdos do iCloud armazenados pela Apple são encriptados na localização do servidor. Para os dados que a Apple consegue descriptar, a Apple mantém as chaves de encriptação nos seus centros de dados nos EUA. A Apple não recebe nem retém chaves de encriptação para os dados totalmente encriptados do cliente.

Todos os pedidos de agências governamentais e de aplicação da lei fora dos Estados Unidos

relativos a conteúdos, salvo nos casos de emergência (definidas anteriormente em Pedidos de emergência), têm de cumprir a legislação aplicável, incluindo a lei dos Estados Unidos relativa a privacidade nas comunicações eletrónicas (ECPA — Electronic Communications Privacy Act). Qualquer pedido ao abrigo de um tratado de auxílio judiciário mútuo ou ao abrigo de um Acordo executivo sob a "Clarifying Lawful Overseas Use of Data Act" ("Acordo da Lei CLOUD") cumpre a ECPA. A Apple disponibilizará conteúdos do cliente, tal como se encontram na sua conta, exclusivamente em resposta ao referido pedido legalmente válido.

II. Proteção de dados avançada

A Proteção de Dados Avançada para iCloud é uma funcionalidade que utiliza encriptação completa para proteger os dados do iCloud com o nível mais elevado de segurança de dados da Apple. Para os utilizadores que ativam a Proteção de dados avançada para iCloud, podem estar disponíveis dados limitados do iCloud. Mais informações sobre Proteção Avançada de Dados podem ser encontradas em support.apple.com/pt-pt/guide/security/advanced-data-protection-for-icloud-sec973254c5f/ e support.apple.com/pt-pt/HT212520.

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

a. Informações do cliente

Se um cliente configurar uma conta do iCloud, poderão ser fornecidas à Apple informações básicas dos clientes como o nome, endereço físico, endereço de e-mail e número de telefone. Além disso, poderão estar disponíveis informações relativas às ligações da funcionalidade iCloud. As informações dos clientes do iCloud e os registos de ligações com endereços IP, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente. Os registos de ligação são conservados durante 25 dias, no máximo.

b. Registos de email

Os registos de email incluem registos de comunicações recebidas e enviadas, como hora, data, endereços de email dos remetentes e endereços de email dos destinatários. Os registos de email do iCloud são retidos durante até 25 dias; e, se disponíveis, podem ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

c. Conteúdos de emails e outros conteúdos do iCloud

Para os utilizadores que ativam a Proteção de dados avançada, o iCloud armazena conteúdos de emails, contactos e calendários que o cliente optou por manter na conta enquanto a conta do cliente permanece ativa. Estes dados podem ser fornecidos, tal como existem na conta do cliente, com o pedido adequado legalmente válido relativo ao país do requerente. Estes dados limitados são armazenados pela Apple e encriptados adicionalmente na localização

do servidor. Para os dados que a Apple consegue descriptar, a Apple mantém as chaves de encriptação nos seus centros de dados nos EUA. A Apple não recebe nem retém chaves de encriptação para os dados totalmente encriptados do cliente.

A Proteção de dados avançada utiliza encriptação completa e a Apple não consegue descriptar determinados conteúdos do iCloud, incluindo Fotografias, iCloud Drive, cópias de segurança, Notas e marcadores do Safari. Em algumas circunstâncias, a Apple pode reter informações limitadas relacionadas com estes serviços do iCloud que podem ser obtidas, se houver, com o pedido legalmente válido relativo ao país do requerente.

III. Reencaminhamento privado iCloud

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

Quando o Reencaminhamento privado está ativado, os pedidos de navegação na internet do utilizador são enviados através de dois reencaminhamentos de internet seguros e separados. O endereço IP do utilizador é visível para a operadora de rede do utilizador e para o primeiro reencaminhamento, que é realizado pela Apple. Os registos DNS do utilizador são encriptados, pelo que nenhuma das partes consegue ver o endereço do site que o utilizador está a tentar visitar. O segundo reencaminhamento, que é realizado por um fornecedor de conteúdos independente, gera um endereço IP temporário, descripta o nome do site solicitado pelo utilizador e conecta-o ao site. O Reencaminhamento privado confirma que o cliente a efetuar a ligação é um iPhone, iPad ou Mac. O Reencaminhamento privado substitui o endereço IP original do utilizador por um atribuído a partir do intervalo de endereços IP utilizados pelo serviço. O endereço IP de reencaminhamento atribuído pode ser partilhado entre mais do que um utilizador de Reencaminhamento privado na mesma área.

Quando os pedidos de navegação na internet dos utilizadores utilizam o Reencaminhamento privado, a Apple não consegue determinar o endereço IP do cliente do utilizador nem a conta de utilizador correspondente a partir dos endereços IP do Reencaminhamento privado. A Apple não tem informações a fornecer relativamente ao ID Apple associado ao endereço IP do Reencaminhamento privado.

Nota: o Reencaminhamento privado iCloud não está disponível em todos os países ou regiões. Se os utilizadores tiverem a funcionalidade de Reencaminhamento privado ativada e viajarem para algum lugar em que o Reencaminhamento privado não esteja disponível, este será automaticamente desativado e ativado novamente quando os utilizadores regressarem a um país ou região que a suporte.

I. Encontrar

Encontrar é uma funcionalidade ativada pelo utilizador que um cliente do iCloud pode utilizar para localizar o iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac ou AirTag que perdeu e/ou efetuar determinadas ações, incluindo a ativação do modo perdido no dispositivo ou a eliminação dos dados ou o bloqueio do dispositivo. Pode obter mais informações sobre este serviço em www.apple.com/icloud/find-my/.

Para que a funcionalidade Encontrar funcione para um cliente que perdeu o dispositivo, tem de já ter sido ativada no dispositivo em questão antes ser perdido. A funcionalidade Encontrar num dispositivo não pode ser ativada remotamente nem depois da perda do dispositivo nem mediante um pedido de uma agência governamental ou de aplicação da lei. As informações dos serviços de localização de dispositivos são armazenadas em cada dispositivo individual e a Apple não pode recuperar estas informações de nenhum dispositivo específico. As informações dos serviços de localização de um

dispositivo localizado através da funcionalidade Encontrar são orientadas para o cliente e a Apple não tem conteúdos de mapas ou alertas transmitidos através do serviço. A seguinte ligação de apoio fornece informações e passos que podem ser executados por um cliente em caso de perda ou roubo de um dispositivo iOS: support.apple.com/pt-pt/HT201472. Os registos de ligação da funcionalidade Encontrar estão disponíveis durante 25 dias, no máximo, e, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente. A atividade de transações da funcionalidade Encontrar relativa a pedidos para bloquear ou apagar remotamente os dados de um dispositivo, se houver, pode ser obtida com o pedido adequado legalmente válido relativo ao país do requerente.

J. Programa acessório da rede Encontrar e AirTag

A app Encontrar no iPhone, iPad, iPod touch e Mac facilita a localização por parte dos clientes dos seus itens pessoais através da aplicação de um AirTag ou utilizando um produto que faz parte do programa acessório da rede Encontrar.

Com o AirTag e o iOS 14.5 e o macOS 11.3 ou posterior, os clientes podem receber assistência para encontrar itens pessoais em falta (chaves, mochilas, bagagem, etc.) através da app Encontrar. O AirTag tem de estar no alcance do Bluetooth do iPhone, iPad ou iPod touch emparelhado de modo a reproduzir um som ou utilizar a Detecção de Precisão com modelos de iPhone compatíveis. Se não estiver perto do proprietário, a localização aproximada do AirTag poderá ser indicada se o AirTag estiver no alcance de um dispositivo na rede Encontrar, que é composta de centenas de milhões de dispositivos Apple em todo o mundo. Mais informações podem ser encontradas em: support.apple.com/pt-pt/HT212227 e support.apple.com/pt-pt/HT210967.

O programa de acessórios de rede Encontrar abre a rede Encontrar para produtos de fabricantes independentes de dispositivos (bicicletas, auscultadores, etc.) para utilizarem o serviço para que os clientes possam localizar os seus produtos de terceiros suportados com a app Encontrar com iOS 14.3 e macOS 11.1 ou posterior.

Para adicionar um AirTag ou produtos terceiros suportados ao separador Itens na aplicação Encontrar, os clientes têm de possuir um ID Apple, ter sessão iniciada na sua conta iCloud com Encontrar ativado e registar o seu AirTag ou produtos terceiros suportados no seu ID Apple. A interação é totalmente encriptada e a Apple não consegue visualizar a localização de qualquer AirTag ou produtos terceiros suportados. Pode obter mais informações em support.apple.com/pt-pt/HT211331.

Com o número de série, a Apple poderá fornecer detalhes da conta emparelhada para responder ao pedido adequado legalmente válido relativo ao país do requerente. O histórico de emparelhamento do AirTag está disponível durante 25 dias no máximo. A seguinte ligação de suporte fornece informações sobre como encontrar um número de série AirTag: support.apple.com/pt-pt/HT211658.

Deve ter-se em atenção que os números de série dos dispositivos Apple não contêm as letras "O" ou "I"; em vez disso, a Apple utiliza os números 0 (zero) e 1 (um) nos números de série. Os pedidos de números de série com a letra "O" ou "I" não produzirão resultados. Se um pedido judicial contiver 5 ou mais números, a Apple solicita que estes números de série sejam também apresentados em formato eletrónico editável (exemplo: documento do Numbers, Excel, Pages ou Word).

K. Extrair dados de dispositivos iOS protegidos por código

No que diz respeito a todos os dispositivos com o iOS 8.0 e versões posteriores, a Apple não pode efetuar uma extração de dados do dispositivo iOS, porque os dados normalmente pretendidos pelas agências de aplicação da lei são encriptados e a Apple não possui a chave de encriptação. Todos os iPhone 6 e modelos de dispositivos posteriores são fabricados com o iOS 8.0 ou uma versão posterior

do iOS.

Para dispositivos com o iOS 4 até ao iOS 7, a Apple poderá, consoante o estado do dispositivo, efetuar extrações de dados do iOS, em conformidade com a lei relativa a privacidade nas comunicações eletrónicas da Califórnia (CalECPA, Código penal da Califórnia §§1546-1546.4). Para que a Apple efetue uma extração de dados do iOS para um dispositivo que cumpra estes critérios, a agência de aplicação da lei deve obter um mandado de busca emitido mediante a demonstração de causa provável ao abrigo do CalECPA. Para além da lei CalECPA, a Apple não identificou nenhuma autoridade judicial estabelecida que exija que a Apple proceda à extração de dados como empresa terceira numa investigação de uma agência de aplicação da lei.

L. Pedido de endereço IP

Antes de enviar um processo legal com um endereço IP como identificador, a Apple solicita que a agência de aplicação da lei determine que o endereço IP em questão não é um endereço IP público ou de router e não está a utilizar Tradução de endereços de rede de nível de operadora (CGNAT) e confirme à Apple durante os trâmites do processo judicial que se trata de um endereço IP não público. Além disso, esses pedidos devem incluir uma restrição de data não superior a três dias. Em resposta a este pedido, a Apple poderá produzir registos de ligação (ver abaixo, secção III.Q) a partir dos quais a agência de aplicação da lei pode tentar identificar uma conta Apple/ID Apple em particular para utilizar como identificador num pedido de processo legal de seguimento. Os dados do cliente Apple com base num endereço IP, se disponível, podem ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

M. Outras informações disponíveis do dispositivo

Endereço MAC: um endereço do controlo de acesso a suportes (endereço MAC) é um identificador único atribuído a interfaces de rede para comunicações no segmento de rede físico. Qualquer produto Apple com interfaces de rede terá um ou mais endereços MAC, tais como Bluetooth, Ethernet, Wi-Fi ou FireWire. Ao fornecer à Apple um número de série (ou, no caso de um dispositivo iOS, IMEI, MEID ou UDID), as informações responsivas do endereço MAC, se houver, poderão ser obtidas com o pedido adequado legalmente válido relativo ao país do requerente.

N. Pedidos de dados de CCTV da Apple Store

Os dados de CCTV poderão variar consoante a loja. Os dados de CCTV são normalmente conservados numa loja Apple Store durante um máximo de 30 dias. Em muitas jurisdições, esse período poderá ser apenas de 24 (vinte e quatro) horas, tendo em conta a legislação local. Após este período, os dados poderão não estar disponíveis. Os pedidos relativos exclusivamente a dados de CCTV podem ser enviados para lawenforcement@apple.com. A agência governamental ou de aplicação da lei deve fornecer informações específicas de data, hora e transação relativas aos dados solicitados.

O. Game Center

O Game Center é a rede de jogos sociais da Apple. Poderão estar disponíveis informações relativas às ligações de um cliente ou dispositivo ao Game Center. Registos de ligações, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

P. Ativação de dispositivos iOS

Quando um cliente ativa um dispositivo iOS junto de uma operadora com serviço de rede móvel ou atualiza o software, são fornecidas determinadas informações à Apple a partir da operadora ou do dispositivo, consoante o evento. Poderão estar disponíveis endereços IP do evento, números ICCID e outros identificadores de dispositivos. Estas informações, se houver, poderão ser obtidas com o pedido adequado legalmente válido relativo ao país do requerente.

Dual SIM: no que diz respeito aos dispositivos com Dual SIM, as informações da operadora relativamente ao nano SIM e/ou eSIM, se houver, poderão ser obtidas com o pedido adequado legalmente válido relativo ao país do requerente. Um eSIM é um SIM digital que permite que os clientes ativem um plano de dados móveis de uma operadora sem terem de utilizar um nano SIM físico. Pode obter mais informações em support.apple.com/pt-pt/HT209044. Na China continental, Hong Kong e Macau, o iPhone 12, o iPhone 12 Pro, o iPhone 12 Pro Max, o iPhone 11, o iPhone 11 Pro, o iPhone 11 Pro Max, o iPhone XS Max e o iPhone XR incluem Dual SIM com dois cartões nano-SIM.

Q.Registos de ligação

A atividade de ligação de um cliente ou dispositivo a serviços da Apple como Apple Music, app Apple TV, Apple Podcasts, Apple Books, iCloud, O meu ID Apple e Apple Discussions, se houver, poderá ser obtida junto da Apple. Estes registos de ligações com endereços IP, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

R. Registos de O meu ID Apple e iForgot

Os registos de O meu ID Apple e iForgot de um cliente poderão ser obtidos junto da Apple. Os registos de O meu ID Apple e iForgot poderão incluir informações relativas a ações de reposição da palavra-passe. Os registos de ligações com endereços IP, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

S. FaceTime

As comunicações por FaceTime são totalmente encriptadas e a Apple não consegue descriptar dados do FaceTime quando estão a ser transferidos entre dispositivos. A Apple não pode intercepar comunicações por FaceTime. A Apple tem registos de convites de chamadas FaceTime quando o convite de uma chamada FaceTime é iniciado. Estes registos não indicam se foi efetivamente estabelecida comunicação entre os clientes. Os registos de convites de chamadas FaceTime são guardados durante 25 dias, no máximo. Os registos de convites de chamadas do FaceTime, se houver, poderão ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

T. iMessage

As comunicações do iMessage são totalmente encriptadas e a Apple não consegue descriptar dados do iMessage quando estão a ser transferidos entre dispositivos. A Apple não pode intercepar comunicações do iMessage e não possui registos de comunicação do iMessage. A Apple tem registos de consultas de capacidade do iMessage. Estes registos indicam que foi iniciada uma consulta por uma app do dispositivo (que pode ser Mensagens, Contactos, Telefone ou outra app do dispositivo) e encaminhada para os servidores da Apple para um identificador de pesquisa (que pode ser um número de telefone, endereço de email ou Apple ID) de modo a determinar se esse identificador de pesquisa é "compatível com iMessage". Os registos de consulta de capacidade do iMessage não indicam se foi efetivamente estabelecida comunicação entre os clientes. A Apple não pode determinar se foi efetivamente estabelecida alguma comunicação do iMessage com base nos registos de consultas de capacidade do iMessage. A Apple também não consegue identificar a app que efetivamente iniciou a consulta. Os registos de consulta de capacidade do iMessage não confirmam

se houve realmente uma tentativa de evento do iMessage. Os registos de consulta de capacidade do iMessage são retidos até 25 dias. Os registos de consulta de capacidade do iMessage, se disponíveis, podem ser obtidos com o pedido adequado legalmente válido relativo ao país do requerente.

U. App Apple TV

A app Apple TV permite que os clientes procurem, comprem, assinem e assistam a programas de TV e filmes da Apple TV+, canais da Apple TV e apps e serviços de outras empresas. O histórico de compras e transferências poderá estar disponível.

Os pedidos de dados dos clientes da app Apple TV têm de incluir o identificador de dispositivo Apple (número de série, IMEI, MEID ou GUID) ou o endereço de e-mail relevante da conta/ID Apple. Se o endereço de e-mail da conta/ID Apple não for conhecido, é necessário apresentar 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 da pessoa. Os agentes governamentais ou de aplicação da lei poderão também fornecer o número de encomenda da Apple válido ou um número de cartão de crédito/débito completo associado às compras na app Apple TV. É também possível fornecer o nome de um cliente em combinação com estes parâmetros, mas o nome do cliente por si só não é suficiente para obter informações.

Nota: sempre que o seu pedido judicial contiver dados completos de cartões de crédito/débito, para efeitos de segurança, esses dados deverão ser enviados num documento protegido por palavra-passe/encriptado (formato .PDF e editável, exemplo: documento do Numbers, Excel, Pages ou Word) para lawenforcement@apple.com e a palavra-passe deverá ser enviada num email em separado. Além disso, tendo em conta as normas de segurança do sistema, a Apple não irá descarregar documentos de pedidos judiciais enviados por email através de uma ligação.

V. Iniciar sessão com a Apple

Com a funcionalidade Iniciar sessão com a Apple, os clientes têm acesso a uma forma mais privada de iniciar sessão em sites e apps de outras empresas, utilizando os seus ID Apple existentes. Um botão Iniciar sessão com a Apple numa app ou site participante permite que o cliente configure uma conta e inicie sessão com o seu ID Apple. Em vez de utilizar uma conta das redes sociais ou preencher formulários e selecionar outra palavra-passe nova, o cliente pode simplesmente tocar no botão Iniciar sessão com a Apple, rever as informações e iniciar sessão de forma rápida e segura com o Face ID, Touch ID ou o código do dispositivo. Pode obter mais informações em support.apple.com/pt-pt/HT210318.

Ocultar o meu e-mail é uma funcionalidade de Iniciar sessão com a Apple. Utiliza o serviço de transmissão de e-mails privados da Apple para criar e partilhar um endereço de e-mail único e aleatório que encaminhe e-mails para o endereço de e-mail pessoal de um cliente. Podem ser obtidas informações básicas dos clientes com o pedido adequado legalmente válido relativo ao país do requerente.

IV. Perguntas frequentes

P: Posso enviar um email à Apple com perguntas sobre o meu pedido de informação de agências de aplicação da lei?

A: Sim, as perguntas ou as consultas relativas ao processo jurídico do governo podem ser enviadas por email para lawenforcement@apple.com.

P: O dispositivo tem de estar registado na Apple para poder funcionar ou para poder ser utilizado?

A: Não, o dispositivo não tem de estar registado na Apple para poder funcionar ou ser utilizado.

P: A Apple pode fornecer-me o código de um dispositivo iOS atualmente bloqueado?

A: Não, a Apple não tem acesso ao código do cliente.

P: Podem ajudar-me a devolver um dispositivo perdido ou roubado ao proprietário?

A: Nestes casos, contacte lawenforcement@apple.com. Inclua o número de série do dispositivo (ou IMEI, caso se aplique) do seu e-mail e quaisquer outras informações relevantes adicionais. As informações sobre como encontrar o número de série estão disponíveis aqui: support.apple.com/pt-pt/HT204308.

Se as informações do cliente estiverem disponíveis, o cliente será contactado pela Apple que fornecerá detalhes sobre como contactar a agência de aplicação da lei para recuperar o dispositivo. No entanto, se não for possível determinar o cliente a partir das informações disponíveis, poderá ser-lhe solicitado que envie um pedido judicial válido.

P: A Apple guarda uma lista dos dispositivos perdidos ou roubados?

A: Não, a Apple não guarda nenhuma lista dos dispositivos perdidos ou roubados.

P: O que deve ser feito com as informações da resposta quando a agência de aplicação da lei tiver concluído a investigação/o processo penal?

A: As informações e os dados fornecidos às agências governamentais e de aplicação da lei que contenham informações de identificação pessoal (incluindo quaisquer cópias efetuadas) devem ser destruídas depois de concluída a respetiva investigação/processo penal e esgotados todos os recursos.

P: A Apple notifica os clientes da receção de pedidos de informação de agências de aplicação da lei relacionados com os mesmos?

A: Sim, a política de aviso da Apple aplica-se a pedidos de conta de agências de aplicação da lei, agências governamentais e empresas privadas. A Apple notificará os clientes e os titulares de contas, salvo se existir uma ordem de não divulgação ou lei aplicável que proíba o aviso, ou se a Apple, ao seu critério exclusivo, considerar de forma razoável que o referido aviso poderá criar um risco imediato de lesão grave ou morte para o público, em situações em que o processo possa constituir um perigo para as crianças, se o aviso não se aplicar aos factos que estão na base do processo.