Recommandations concernant les procédures en justice

Application de la loi en dehors des États-Unis

Ces recommandations sont destinées aux autorités chargées de l'application de la loi et autres autorités publiques en dehors des États-Unis sollicitant des informations sur la clientèle des appareils, produits ou services Apple auprès des entités d'Apple qui fournissent des services dans cette région ou ce pays. Apple mettra à jour ces recommandations, le cas échéant.

Dans ces recommandations, Apple désignera l'entité responsable des informations de la clientèle dans une région ou un pays particulier. En tant qu'entreprise internationale, Apple possède de nombreuses entités juridiques situées au sein de différentes juridictions qui sont responsables des informations personnelles qu'elles collectent et qui sont traitées en leur nom par Apple Inc. Par exemple, les informations sur le point de vente au sein des entités commerciales d'Apple situées en dehors des États-Unis sont contrôlées par les entités commerciales individuelles d'Apple dans chaque pays. Les informations personnelles associées à apple.com et aux services multimédias Apple peuvent également être contrôlées par des entités juridiques en dehors des États-Unis, comme spécifié dans les conditions générales de chaque service dans une juridiction spécifique. En général, les entités juridiques d'Apple en dehors des États-Unis en Australie, au Canada, en Irlande et au Japon sont responsables des données de la clientèle relatives aux services Apple dans leurs régions respectives.

Toutes les autres demandes d'informations concernant la clientèle d'Apple, y compris les questions de la clientèle sur la divulgation d'informations, doivent être formulées sur la page www.apple.com/fr/privacy/contact/. Ces recommandations ne s'appliquent pas aux demandes provenant des autorités chargées de l'application de la loi et autres autorités publiques aux États-Unis reçues par Apple Inc.

Pour les demandes d'informations émanant des autorités chargées de l'application de la loi et autres autorités publiques, nous respectons les lois applicables aux entités mondiales qui contrôlent nos données et fournissons les informations requises au titre de la loi. Toutes les demandes émanant des autorités chargées de l'application de la loi et autres autorités publiques en dehors des États-Unis concernant du contenu, à l'exception des situations d'urgence (définies ci-dessous dans la section Demandes urgentes), doivent être conformes aux lois applicables, y compris à la loi ECPA (Electronic Communications Privacy Act) des États-Unis. Une demande effectuée en vertu d'un Traité d'entraide judiciaire mutuelle ou un Accord exécutif en vertu de la loi fédérale des États-Unis « Clarifying Lawful Overseas Use of Data Act » (CLOUD Act) est conforme à la loi ECPA. Apple fournit le contenu du client, tel qu'il existe sur son compte, uniquement en réponse à une procédure judiciaire valide.

Pour les demandes émanant d'une personne physique privée, Apple se conforme aux lois applicables aux entités locales qui contrôlent les données de la clientèle et fournit les données requises au titre de la loi.

Apple a mis en place une procédure centralisée de réception, de suivi et de traitement des demandes juridiques légitimes émanant des autorités publiques, des autorités chargées de l'application de la loi et des particuliers, à partir de leur réception et jusqu'à ce qu'une réponse soit fournie. Une équipe formée de notre département juridique examine et évalue toutes les demandes reçues, et nous formulons des objections, contestons ou rejetons les demandes qui selon nous n'ont pas de légitimité juridique, ou semblent incertaines, inappropriées ou trop générales.

Apple envoie ses réponses à l'adresse e-mail officielle de l'organisme chargé de l'application de la loi qui est à l'origine de la demande. La responsabilité de la conservation des preuves en vertu des réponses fournies par Apple revient à l'organisme chargé de l'application de la loi qui est à l'origine de la demande.

INDEX

I. Informations générales

Apple conçoit, fabrique et commercialise des appareils multimédias et de communication, des ordinateurs personnels, des lecteurs de musique numérique portables, et vend une diversité de logiciels, services, périphériques et solutions de mise en réseau, ainsi que des applications et du contenu numérique de tiers. Les produits et services d'Apple sont les suivants : Mac, iPhone, iPad, iPod touch, Apple TV, Apple TV+, Apple Watch, HomePod, AirPods, AirTag, un portefeuille d'applications logicielles pour les particuliers et les professionnels, les systèmes d'exploitation iOS et macOS X, iCloud et une diversité d'offres d'accessoires, de services et d'assistance. Apple vend également des applications et du contenu numérique via Apple Music, l'App Store, Apple Books et le Mac App Store. Les informations sur la clientèle sont détenues par Apple conformément à son Engagement de confidentialité et aux conditions de service applicables à l'offre de service concernée. Apple s'engage à respecter la vie privée des personnes utilisant ses produits et services (« clientèle d'Apple »). Par conséquent, hormis dans les situations d'urgence prévues par la loi, aucune information sur la clientèle d'Apple ne sera divulguée sans une procédure judiciaire valide.

Ces recommandations sont conçues pour fournir des informations aux autorités chargées de l'application de la loi et autres autorités publiques en dehors des États-Unis sur la procédure judiciaire exigée par Apple pour leur divulguer des informations électroniques en dehors des États-Unis. Elles n'ont pas pour objectif de fournir des conseils juridiques. La section Questions et réponses de ce document a pour but de répondre à certaines des questions les plus souvent reçues par Apple. Ni ces recommandations ni les Questions et réponses ne couvrent toutes les circonstances imaginables susceptibles de se produire.

Si vous avez des questions, veuillez envoyer un e-mail à l'adresse lawenforcement@apple.com.

L'adresse e-mail ci-dessus est réservée exclusivement aux agents des autorités chargées de l'application de la loi et autres autorités publiques. Si vous décidez d'envoyer un e-mail à cette adresse, celui-ci doit provenir de l'adresse valide et officielle d'une autorité publique ou d'une autorité chargée de l'application de la loi.

Les demandes juridiques reçues par Apple visent à obtenir des informations sur un client ou un appareil Apple particulier et sur les services spécifiques qu'Apple peut fournir à la personne concernée. Apple peut fournir des informations sur un client ou un appareil Apple dans la mesure où Apple possède les informations requises conformément à ses politiques sur la conservation des données. Apple conserve les données comme il est indiqué dans la partie « Informations disponibles » ci-dessous. Toutes les autres données sont conservées pendant la période nécessaire pour répondre aux objectifs stipulés dans notre Engagement de confidentialité. Les autorités chargées de l'application de la loi et autres autorités publiques doivent être aussi concises et spécifiques que possible dans l'établissement de leurs requêtes afin d'éviter toute interprétation erronée, objection, incertitude et/ou rejet en réponse à une demande imprécise, inappropriée ou trop large. Toutes les demandes émanant des autorités chargées de l'application de la loi et autres autorités publiques en dehors des États-Unis concernant du contenu, à l'exception des situations d'urgence (définies ci-dessous dans la section Demandes urgentes), doivent être conformes aux lois applicables, y compris à la loi ECPA (Electronic Communications Privacy Act) des États-Unis. Une demande effectuée en vertu d'un Traité d'entraide judiciaire mutuelle ou un Accord exécutif en vertu de la loi fédérale des États-Unis « Clarifying Lawful Overseas Use of Data Act » (CLOUD Act) est conforme à la loi ECPA. Apple fournit le contenu du client, tel qu'il existe sur son compte, uniquement en réponse à une procédure judiciaire valide.

Aucune disposition de ces recommandations n'a pour but de créer des droits juridiquement exécutoires contre Apple, et les politiques d'Apple pourront être actualisées et modifiées à l'avenir sans en aviser les autorités chargées de l'application de la loi ou autres autorités publiques.

II. Demandes juridiques reçues par Apple

A. Demandes d'informations provenant des autorités chargées de l'application de la loi et autres autorités publiques

Apple accepte de répondre aux demandes d'informations juridiquement valides adressées par e-mail par les autorités publiques et les autorités chargées de l'application de la loi, sous réserve que celles-ci soient transmises via l'adresse e-mail officielle de l'autorité à l'origine de la demande. Les membres du personnel des autorités publiques et des autorités chargées de l'application de la loi en dehors des États-Unis qui soumettent une demande d'informations à Apple doivent remplir le formulaire Demande d'informations pour une autorité publique ou une autorité chargée de l'application de la loi et l'envoyer directement depuis leur adresse e-mail officielle à lawenforcement@apple.com.

L'adresse e-mail ci-dessus est réservée exclusivement aux agents des autorités chargées de l'application de la loi et autres autorités publiques. Lorsque les demandes contiennent cinq identifiants ou plus, tels que le numéro de série/IMEI de l'appareil, l'identifiant Apple, l'adresse e-mail, ou le numéro de facture ou de commande, ceux-ci doivent être transmis dans un format modifiable (par exemple, un document Numbers, Excel, Pages ou Word). Les identifiants de ce type sont généralement requis afin de rechercher des informations relatives aux appareils, aux comptes ou aux transactions financières.

Remarque : en raison des normes de sécurité du système, Apple ne téléchargera pas les demandes juridiques ou les documents associés à partir d'un lien envoyé par e-mail.

Pour qu'Apple divulgue des informations sur sa clientèle en réponse à une demande adressée par une autorité chargée de l'application de la loi, cette dernière doit indiquer la base juridique l'autorisant à collecter des informations probantes sous la forme de données personnelles auprès d'un contrôleur de données comme Apple. Voici des exemples de demandes qu'Apple considère comme juridiquement valides : Production Orders (Australie, Canada, Nouvelle-Zélande), lettres de réquisition ou commissions rogatoires (France), Solicitud Datos (Espagne), Ordem Judicial (Brésil), Auskunftsersuchen (Allemagne), Obligation de dépôt (Suisse), 個人情報の開示依頼 (Japon), Personal Data Request, Orders, Warrants and Communications Data Authorisations (Royaume-Uni), ainsi que les ordonnances et/ou demandes des tribunaux équivalentes d'autres pays.

B. Gérer les demandes d'informations provenant des autorités chargées de l'application de la loi et autres autorités publiques et y répondre

Apple étudie minutieusement chaque demande afin de vérifier la présence d'une base juridique valide et répond à toutes les demandes légitimes. Si Apple détermine qu'une demande n'a pas de légitimité juridique ou semble incertaine, inappropriée ou trop générale, Apple formule une objection, conteste ou rejette la demande.

Pour garantir le bon traitement des dossiers et en raison de limitations du système, Apple ne peut pas accepter les demandes concernant plus de 25 identifiants de compte. Si une autorité chargée de l'application de la loi soumet une telle demande, Apple répondra pour les 25 premiers identifiants, et une nouvelle demande juridique devra être formulée pour les suivants.

C. Demandes de préservation

Toutes les demandes émanant des autorités chargées de l'application de la loi et autres autorités

publiques en dehors des États-Unis concernant du contenu, à l'exception des situations d'urgence (définies ci-dessous dans la section Demandes urgentes), doivent être conformes aux lois applicables, y compris à la loi ECPA (Electronic Communications Privacy Act) des États-Unis. Une demande effectuée en vertu d'un Traité d'entraide judiciaire mutuelle ou un Accord exécutif en vertu de la loi fédérale des États-Unis « Clarifying Lawful Overseas Use of Data Act » (CLOUD Act) est conforme à la loi ECPA. Une demande de préservation des données soumise avant une demande de conformité imminente dans le cadre de la loi ECPA doit être envoyée par e-mail à lawenforcement@apple.com.

Les demandes de préservation doivent comporter l'identifiant Apple/l'adresse e-mail du compte, ou le nom complet **et** le numéro de téléphone, et/ou le nom complet **et** l'adresse postale de la personne détentrice du compte Apple en question. Une fois la demande de préservation reçue, Apple préservera une seule importation des données existantes demandées et disponibles au moment de la demande, pendant une durée de 90 jours. Au-delà de cette période de 90 jours, les données préservées seront automatiquement supprimées du serveur de stockage. Cependant, cette période pourra être prolongée de 90 jours si la demande est renouvelée. Si un même compte fait l'objet de deux demandes de préservation, la deuxième sera traitée comme une demande d'extension de la première préservation et non comme une préservation distincte des nouvelles données.

D. Demandes urgentes

Apple considère une demande comme urgente lorsqu'elle est liée à des circonstances qui constituent une menace immédiate et sérieuse pour la vie ou la sécurité d'individus, la sécurité d'un État ou celle d'une infrastructure/installation critique.

Si l'autorité publique ou l'autorité chargée de l'application de la loi à l'origine de la demande apporte la confirmation satisfaisante que sa requête porte sur des circonstances urgentes satisfaisant à un ou plusieurs des critères ci-dessus, Apple l'examinera en urgence.

Pour demander à ce qu'Apple divulgue volontairement des informations en urgence, l'autorité publique ou l'autorité chargée de l'application de la loi à l'origine de la demande doit remplir le formulaire intitulé Demande d'informations urgente pour une autorité publique et une autorité chargée de l'application de la loi et le transmettre directement depuis l'adresse e-mail officielle de son service à exigent@apple.com avec la mention « Demande urgente » dans la ligne d'objet.

Si une autorité publique ou une autorité chargée de l'application de la loi cherche des données liées à la clientèle dans le cadre d'une telle demande, le responsable de l'agent de l'autorité publique ou de l'autorité chargée de l'application de la loi ayant soumis cette demande d'informations urgente peut être contacté et invité à confirmer à Apple la légitimité de cette demande urgente. Apple exige que l'agent de l'autorité publique ou de l'autorité chargée de l'application de la loi ayant soumis la demande d'informations urgente pour une autorité publique et une autorité chargée de l'application de la loi communique les coordonnées de son responsable dans cette demande.

Pour toute demande urgente, les autorités publiques ou autorités chargées de l'application de la loi peuvent contacter le centre des opérations de sécurité globale (GSOC, Global Security Operations Center) d'Apple au 001 408 974-2095. Ce numéro offre une assistance dans plusieurs langues.

E. Demandes de restriction/suppression de compte

Si une autorité publique ou une autorité chargée de l'application de la loi demande à Apple de

restreindre/supprimer l'identifiant Apple d'un client, elle sera tenue de fournir à Apple une ordonnance d'un tribunal ou son équivalent juridique dans le pays concerné (souvent un jugement de condamnation ou un mandat), démontrant que le compte à restreindre/supprimer a été utilisé de façon illicite.

Apple examine attentivement chaque demande émanant des autorités publiques et des autorités chargées de l'application de la loi pour vérifier qu'elle est fondée sur le plan juridique. Si Apple détermine qu'une demande n'a pas de légitimité juridique ou à restreindre/supprimer a été utilisé de façon illicite, Apple contestera ou rejettera la demande.

Si Apple reçoit de la part de l'autorité publique ou de l'autorité chargée de l'application de la loi une ordonnance du tribunal satisfaisante ou son équivalent juridique dans le pays concerné (souvent un jugement de condamnation ou un mandat), démontrant que le compte à restreindre/supprimer a été utilisé de façon illicite, Apple prendra les mesures requises pour restreindre/supprimer le compte conformément à l'ordonnance du tribunal, et informera la personne à l'origine de la demande en conséquence.

F. Notification à la clientèle

Apple avertit ses clients quand les informations de leur compte Apple sont recherchées en réponse à une demande juridique valide d'une autorité publique ou d'une autorité chargée de l'application de la loi, excepté si ladite notification est explicitement interdite par la demande juridique valide, par une ordonnance de tribunal remise à Apple, par la loi en vigueur, ou si Apple, à sa seule discrétion, estime que l'envoi d'une notification crée un risque de blessure ou de décès d'une personne identifiable, dans les cas de mise en danger d'enfants, ou si la notification n'est pas applicable aux faits en cause dans l'affaire.

Après un délai de 90 jours, Apple délivrera une notification différée pour les divulgations urgentes, excepté si la notification est interdite par une ordonnance du tribunal ou la loi applicable, ou si Apple, à sa seule discrétion, estime que l'envoi d'une notification crée un risque de blessure ou de décès d'une personne identifiable, ou dans les cas de mise en danger d'enfants. Apple délivre les notifications différées de ces demandes après l'expiration de la période de non-divulgation spécifiée dans l'ordonnance du tribunal, sauf si Apple juge raisonnablement et à sa seule discrétion que cette mesure pourrait créer un risque de blessure ou de décès d'une personne ou d'un groupe de personnes identifiable, dans les cas de mise en danger d'enfants, ou si la notification n'est pas applicable aux faits en cause dans l'affaire.

Apple avertit ses clients quand leur compte Apple a été restreint/supprimé en réponse à une ordonnance d'un tribunal (souvent un jugement de condamnation ou un mandat) démontrant que le compte à restreindre/supprimer a été utilisé de façon illicite ou en infraction avec les conditions générales d'Apple, excepté si ladite notification est explicitement interdite par la procédure judiciaire elle-même, par une ordonnance de tribunal remise à Apple, par la loi applicable, ou si Apple, à sa seule discrétion, estime que l'envoi d'une notification crée un risque de blessure ou de décès d'une personne identifiable, dans les cas de mise en danger d'enfants, ou si la notification n'est pas applicable aux faits en cause dans l'affaire, ou encore si Apple juge raisonnablement qu'une notification serait susceptible d'entraver le cours de la justice ou de nuire à l'administration de la justice.

III. Informations disponibles auprès d'Apple

Cette section aborde les types d'informations générales pouvant être disponibles auprès d'Apple au moment de la publication des présentes recommandations.

A. Inscription d'appareils

Les clients qui inscrivent un appareil sous une version antérieure à iOS 8 et macOS Sierra 10.12 transmettent à Apple des informations d'inscription de base ou personnelles, notammment leurs nom, adresse postale, adresse e-mail et numéro de téléphone. Apple ne vérifie pas ces informations et elles peuvent donc être erronées ou ne pas correspondre au propriétaire de l'appareil. Nous recevons des informations d'inscription pour les appareils exécutant iOS 8 (ou versions ultérieures) et les Mac exécutant macOS Sierra 10.12 (ou versions ultérieures) lorsque le client associe son appareil à un identifiant Apple iCloud. Ces informations peuvent être erronées ou ne pas correspondre au propriétaire de l'appareil. Les informations d'inscription, le cas échéant, peuvent être obtenues sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Veuillez noter que les numéros de série des appareils Apple ne contiennent ni la lettre « O », ni la lettre « I », mais qu'Apple utilise les chiffres 0 (zéro) et 1 (un) dans ces numéros de série. Les demandes avec des numéros de série contenant les lettres « O » ou « I » ne donneront aucun résultat. Si une demande juridique comprend cinq numéros de série ou plus, Apple demande à ce qu'ils soient également soumis dans un format électronique modifiable (par exemple, un document Numbers, Excel, Pages ou Word).

B. Dossiers du service clientèle

Les contacts que les clients ont eus avec le service clientèle Apple à propos d'un appareil ou d'un service peuvent être obtenus auprès d'Apple. Ces informations peuvent inclure les dossiers sur les interactions avec la clientèle dans le cadre d'une assistance pour un appareil ou un service Apple particulier. En outre, des données concernant l'appareil, la garantie et les réparations peuvent aussi être mises à disposition. Ces informations peuvent être obtenues, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

C. Services multimédias Apple

L'App Store, Apple Music, l'app Apple TV, Apple Podcasts et Apple Books (« Services multimédias Apple ») sont des applications logicielles permettant d'organiser et de lire des apps, de la musique et des vidéos numériques ainsi que du contenu en streaming. Les services multimédias Apple fournissent également du contenu que la clientèle peut télécharger depuis un ordinateur ou appareil iOS. Lorsqu'une personne crée un compte Apple, elle peut communiquer des informations de base comme son nom, son adresse postale, son adresse e-mail et son numéro de téléphone. De plus, des données sur les transactions et connexions liées aux achats/téléchargements, ainsi que les connexions liées à des mises à jour/nouveaux téléchargements sur les services multimédias Apple peuvent aussi être mises à disposition. L'accès aux informations des adresses IP peut être limité aux 18 derniers mois. Les informations sur les clients des services multimédias Apple et les historiques de connexion avec les adresses IP peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Les demandes de données sur les services multimédias Apple doivent inclure l'identifiant de l'appareil Apple (numéro de série, IMEI, MEID ou GUID) ou l'identifiant Apple/l'adresse e-mail du compte. Si l'identifiant Apple ou l'adresse e-mail du compte ne sont pas connus, Apple exige des informations sur la personne comme son nom complet **et** son numéro de téléphone et/ou son nom complet **et** son adresse postale afin d'identifier le compte de services multimédias Apple concerné. L'autorité publique ou l'autorité chargée de l'application de la loi peut également fournir un numéro de commande lié aux services multimédias Apple valide, ou un numéro de carte bancaire complet associé aux achats sur les services multimédias Apple. Le nom du client associé à ces paramètres peut être également fourni, mais le nom seul ne suffit pas pour obtenir ces informations.

Remarque : pour préserver la sécurité des données, si une demande juridique contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (fichier PDF et autres formats modifiables, par exemple, un document Numbers, Excel, Pages ou Word). Le mot de passe doit être envoyé dans un e-mail séparé. En outre, en raison des normes de sécurité du système, Apple ne téléchargera aucun document associé à une demande juridique à partir d'un lien envoyé par e-mail.

D. Transactions dans l'Apple Store

Les transactions en magasin sont des transactions effectuées en espèces, par carte bancaire ou cartes cadeaux dans un Apple Store. Pour les demandes portant sur les dossiers d'un magasin, le numéro complet de la carte bancaire utilisée et toute information supplémentaire comme la date et l'heure de la transaction, le montant et les articles achetés doivent être communiqués. Les informations sur le type de carte associé à un achat particulier, le nom de l'acheteur, son adresse e-mail, la date et l'heure de la transaction, son montant et l'adresse du magasin, le cas échéant, peuvent être obtenues sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Les demandes de duplicatas de reçus doivent inclure le numéro de transaction du magasin associé à l'achat et, le cas échéant, peuvent être obtenues sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Remarque : pour préserver la sécurité des données, si une demande juridique contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (fichier PDF et autres formats modifiables, par exemple, un document Numbers, Excel, Pages ou Word). Le mot de passe doit être envoyé dans un e-mail séparé. En outre, en raison des normes de sécurité du système, Apple ne téléchargera aucun document associé à une demande juridique à partir d'un lien envoyé par e-mail.

E. Commandes passées sur apple.com

Apple conserve les informations relatives aux commandes passées sur apple.com, y compris le nom de l'acheteur, l'adresse d'expédition, le numéro de téléphone, l'adresse e-mail, le produit acheté, le montant de l'achat et l'adresse IP de l'achat. Pour les demandes d'informations concernant des commandes passées sur apple.com, un numéro de carte bancaire complet, un numéro de commande ou le numéro de série de l'article acheté doivent être communiqués. Le nom du client associé à ces paramètres peut être également fourni, mais le nom seul ne suffit pas pour obtenir ces informations. Les demandes d'informations concernant des commandes passées sur apple.com peuvent également

inclure l'identifiant Apple/l'adresse e-mail du compte. Si l'identifiant Apple ou l'adresse e-mail du compte ne sont pas connus, Apple exige des informations sur la personne comme son nom complet **et** son numéro de téléphone et/ou son nom complet **et** son adresse postale afin d'identifier le compte Apple concerné. Les informations concernant des commandes passées sur apple.com, le cas échéant, peuvent être obtenues sur présentation d'une demande juridiquement valide pour le pays du demandeur.

Remarque : pour préserver la sécurité des données, si une demande juridique contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (fichier PDF et autres formats modifiables, par exemple, un document Numbers, Excel, Pages ou Word). Le mot de passe doit être envoyé dans un e-mail séparé. En outre, en raison des normes de sécurité du système, Apple ne téléchargera aucun document associé à une demande juridique à partir d'un lien envoyé par e-mail.

F. Cartes cadeaux

Les cartes cadeaux Apple Store, App Store et iTunes ont un numéro de série. Le format de ces numéros de série varie selon des variables, comme la conception et/ou la date de délivrance. Apple peut fournir les informations disponibles relatives aux cartes cadeaux Apple Store, App Store et iTunes en réponse à toute demande juridiquement valide pour le pays de la personne qui en est à l'origine. Si une demande juridique comprend cinq numéros de série de cartes cadeaux ou plus, Apple demande à ce qu'ils soient envoyés par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (par exemple, un document Numbers, Excel, Pages ou Word).

i. Cartes cadeaux Apple Store

Les cartes cadeaux Apple Store peuvent servir à effectuer des achats dans un Apple Store ou sur apple.com. Les informations disponibles peuvent inclure des données sur la personne ayant acheté la carte cadeau (si elle a été achetée auprès d'Apple et non d'un vendeur tiers), les transactions d'achat associées et les articles achetés. Dans certains cas, Apple peut être en mesure d'annuler ou de suspendre une carte cadeau Apple Store, en fonction de l'état de la carte en question. Les informations d'une carte cadeau Apple Store, le cas échéant, peuvent être obtenues sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Remarque : pour préserver la sécurité des données, si une demande juridique contient des informations complètes de carte cadeau Apple Store, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (fichier PDF et autres formats modifiables, par exemple, un document Numbers, Excel, Pages ou Word). Le mot de passe doit être envoyé dans un e-mail séparé. En outre, en raison des normes de sécurité du système, Apple ne téléchargera aucun document associé à une demande juridique à partir d'un lien envoyé par e-mail.

ii. Cartes cadeaux App Store et iTunes

Les cartes cadeaux App Store et iTunes sont valables pour Apple Music, Apple Books, ainsi que sur l'App Store et le Mac App Store. Grâce au numéro de série, Apple peut déterminer si la carte cadeau App Store et iTunes a été activée (achetée dans un point de vente) ou utilisée

(ajoutée au solde de crédit d'un compte Apple).

Lorsqu'une carte cadeau App Store et iTunes est activée, les informations disponibles peuvent inclure le nom et l'adresse du magasin, ainsi que la date et l'heure. Lorsqu'une carte cadeau App Store et iTunes est utilisée, les informations disponibles peuvent inclure les informations sur le compte Apple concerné, la date et l'heure de l'activation et/ou de l'utilisation, et l'adresse IP d'utilisation. Dans certains cas, Apple peut être en mesure de désactiver une carte cadeau App Store et iTunes, en fonction de l'état de la carte en question. Les informations d'une carte cadeau App Store et iTunes, le cas échéant, peuvent être obtenues sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Remarque : pour préserver la sécurité des données, si une demande juridique contient les informations complètes d'une carte cadeau App Store et iTunes, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (fichier PDF et autres formats modifiables, par exemple, un document Numbers, Excel, Pages ou Word). Le mot de passe doit être envoyé dans un e-mail séparé. En outre, en raison des normes de sécurité du système, Apple ne téléchargera aucun document associé à une demande juridique à partir d'un lien envoyé par e-mail.

G. Apple Pay

Les transactions Apple Pay effectuées en magasin (par exemple pour les communications NFC/sans contact) et dans des apps ou points de vente en ligne font l'objet d'une authentification sécurisée depuis l'appareil de la personne et sont envoyées dans un format chiffré au commerçant ou à son organisme de paiement. Bien que la sécurité des transactions soit assurée par un serveur Apple, Apple ne traite pas les paiements et ne stocke ni ces transactions ni les numéros de cartes de crédit/débit associés aux achats effectués à l'aide d'Apple Pay. Ces informations peuvent être mises à disposition par l'établissement émetteur, le réseau de paiement ou le commerçant.

Pour connaître les pays et régions compatibles avec Apple Pay, consultez l'article suivant: support.apple.com/fr-fr/HT207957.

Pour demander des données transactionnelles liées à des achats effectués dans des Apple Store ou sur apple.com, Apple a besoin du numéro de compte principal de l'appareil (DPAN, Device Primary Account Number) utilisé dans le cadre de la transaction. Le DPAN comporte 16 chiffres et peut être fourni par la banque émettrice. Remarque : le DPAN est utilisé dans les transactions de paiement sans contact effectuées auprès des commerçants, à la place du numéro de carte de crédit/débit (FPAN ou « Funding PAN », numéro de compte principal de financement). Le DPAN est converti en FPAN correspondant par l'organisme de paiement. Le numéro DPAN permettra à Apple de rechercher les informations demandées via son système de gestion des points de vente. Ces informations peuvent être obtenues, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

En plus des informations sur la personne concernée par la demande, Apple peut également fournir des renseignements sur le type de carte(s) de crédit/débit qu'elle a ajoutée(s) à Apple Pay. Ces informations peuvent être obtenues, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine. Pour demander ces informations, Apple a besoin d'un identifiant d'appareil (numéro de série Apple, SEID, IMEI ou MEID), d'un identifiant Apple ou de l'adresse e-mail d'un compte Apple.

Remarque : pour préserver la sécurité des données, si une demande juridique contient un DPAN, celui-ci doit être envoyé par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (fichier PDF et autres formats modifiables, par exemple, un document Numbers, Excel, Pages ou Word). Le mot de passe doit être envoyé dans un e-mail séparé. En outre, en raison des normes de sécurité du système, Apple ne téléchargera aucun document associé à une demande juridique à partir d'un lien envoyé par e-mail.

H. iCloud

iCloud est un service dans le cloud d'Apple qui permet aux clients d'accéder à leurs photos, leurs documents et plus encore à partir de tous leurs appareils. Ils peuvent également sauvegarder le contenu de leurs appareils iOS et iPadOS sur iCloud et configurer un compte de messagerie iCloud.com. Les noms de domaine de la messagerie iCloud peuvent être @icloud.com, @me.com et @mac.com. Toutes les données iCloud stockées par Apple sont chiffrées à l'emplacement du serveur. En ce qui concerne les données qu'Apple peut déchiffrer, Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis. Apple ne reçoit ni ne conserve les clés de chiffrement des données chiffrées de bout en bout de la clientèle.

iCloud est un service basé sur la clientèle. Les demandes de données iCloud doivent inclure l'identifiant Apple/l'adresse e-mail du compte. Si l'identifiant Apple ou l'adresse e-mail du compte ne sont pas connus, Apple exige des informations sur la personne comme son nom complet **et** son numéro de téléphone, et/ou son nom complet **et** son adresse postale afin d'identifier le compte Apple concerné. Si seul un numéro de téléphone, un identifiant Apple ou l'adresse e-mail d'un compte est renseigné(e), les informations disponibles pour les comptes vérifiés associés à ces critères peuvent être mises à disposition.

I. Les informations suivantes peuvent être disponibles sur iCloud :

I. Informations client

Lorsqu'un compte iCloud est créé, des informations de base sur la personne comme son nom, son adresse postale, son adresse e-mail et son numéro de téléphone peuvent être communiquées à Apple. De plus, des données concernant les connexions aux fonctionnalités iCloud peuvent aussi être mises à disposition. Les informations sur les clients iCloud et les historiques de connexion avec les adresses IP peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine. Les historiques de connexion sont conservés pendant une durée allant jusqu'à 25 jours.

II. Historiques de la messagerie

Les historiques de la messagerie comprennent des enregistrements de données telles que la date et l'heure des communications entrantes et sortantes, ainsi que les adresses e-mail des expéditeurs et des destinataires. Les historiques de la messagerie d'iCloud sont conservés pendant une durée allant jusqu'à 25 jours et, le cas échéant, peuvent être obtenus sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

III. Sauvegardes des contenus liés aux e-mails et à iCloud, de Mon flux de photos, de la photothèque iCloud, d'iCloud Drive, des contacts, des calendriers, des signets, de l'historique de navigation Safari, de l'historique des recherches de Plans, des messages, des appareils iOS

iCloud stocke le contenu des services que la personne a décidé de conserver sur son compte lorsque celui-ci est actif. Apple ne conserve pas le contenu supprimé une fois qu'il a été effacé de ses serveurs. Le contenu iCloud peut inclure des sauvegardes d'e-mails, de photos stockées, de documents, de contacts, de calendriers, de signets, de l'historique de navigation Safari, de l'historique des recherches de Plans, des messages et des appareils iOS. La sauvegarde d'un appareil iOS peut inclure les photos et vidéos contenues dans la pellicule de l'appareil photo, les réglages de l'appareil, les données des apps, les iMessages, les messages Business Chat, les SMS, les MMS et la messagerie vocale. Toutes les données iCloud stockées par Apple sont chiffrées à l'emplacement du serveur. En ce qui concerne les données qu'Apple peut déchiffrer, Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis. Apple ne reçoit ni ne conserve les clés de chiffrement des données chiffrées de bout en bout de la clientèle.

Toutes les demandes émanant des autorités chargées de l'application de la loi et autres autorités publiques en dehors des États-Unis concernant du contenu, à l'exception des situations d'urgence (définies ci-dessus dans la section Demandes urgentes), doivent être conformes aux lois applicables, y compris à la loi ECPA (Electronic Communications Privacy Act) des États-Unis. Une demande effectuée en vertu d'un Traité d'entraide judiciaire mutuelle ou un Accord exécutif en vertu de la loi fédérale des États-Unis « Clarifying Lawful Overseas Use of Data Act » (CLOUD Act) est conforme à la loi ECPA. Apple fournit le contenu du client, tel qu'il existe sur son compte, uniquement en réponse à une demande valide juridiquement.

II. Protection avancée des données

La fonctionnalité Protection avancée des données pour iCloud utilise le chiffrement de bout en bout pour protéger les données iCloud avec le niveau le plus élevé de sécurité des données d'Apple. Pour les utilisateurs qui activent la fonctionnalité Protection avancée des données pour iCloud, Apple ne conserve que des données iCloud limitées. Pour en savoir plus sur la fonctionnalité Protection avancée des données, consultez les pages support.apple.com/fr-fr/guide/security/advanced-data-protection-for-icloud-sec973254c5f/ et support.apple.com/fr-fr/HT212520.

Les informations suivantes peuvent être disponibles sur iCloud si un utilisateur a activé la fonctionnalité Protection avancée des données pour iCloud :

a. Informations client

Lorsqu'un compte iCloud est créé, des informations de base sur la personne comme son nom, son adresse postale, son adresse e-mail et son numéro de téléphone peuvent être communiquées à Apple. De plus, des données concernant les connexions aux fonctionnalités iCloud peuvent aussi être mises à disposition. Les informations sur les clients iCloud et les historiques de connexion avec les adresses IP peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine. Les historiques de connexion sont conservés pendant une durée allant jusqu'à 25 jours.

b. Historiques de la messagerie

Les historiques de la messagerie comprennent des enregistrements de données telles que la date et l'heure des communications entrantes et sortantes, ainsi que les adresses e-mail des expéditeurs et des destinataires. Les historiques de la messagerie d'iCloud sont conservés pendant une durée allant jusqu'à 25 jours et, le cas échéant, peuvent être obtenus sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

c. Contenu des e-mails et autres contenus iCloud

Si la fonctionnalité Protection avancée des données est activée, iCloud stocke le contenu de la messagerie, des contacts et du calendrier que le client a décidé de conserver sur son compte lorsque celui-ci est actif. Ces données peuvent être fournies, tel qu'elles existent sur le compte du client, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Ces données limitées sont stockées par Apple et chiffrées à l'emplacement du serveur. En ce qui concerne les données qu'Apple peut déchiffrer, Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis. Apple ne reçoit ni ne conserve les clés de chiffrement des données chiffrées de bout en bout de la clientèle. Étant donné que la fonctionnalité Protection avancée des données utilise le chiffrement de bout en bout, Apple ne peut pas déchiffrer certains contenus iCloud, notamment les fichiers des services Photos, iCloud Drive, Sauvegarde, Notes et Signets Safari. Dans certaines circonstances, Apple peut conserver des informations limitées relatives à ces services iCloud. Ces informations peuvent être obtenues, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

III. Relais privé iCloud

Le relais privé iCloud est un service de confidentialité sur Internet inclus dans l'abonnement iCloud+. Le relais privé protège la navigation web des utilisateurs dans Safari, les requêtes de résolution DNS (« Domain Name Space », espace de noms de domaine) ainsi que le trafic non chiffré au sein des apps utilisant le protocole HTTP. L'utilisation du relais privé iCloud nécessite un abonnement à iCloud+ ainsi qu'un appareil doté d'iOS 15, d'iPadOS 15 ou de macOS Monterey (macOS 12) ou version ultérieure. Pour en savoir plus sur le relais privé, consultez l'article support.apple.com/fr-fr/HT212614 et le document www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF.

Lorsque le relais privé est activé, les requêtes de navigation web des utilisateurs sont envoyées via deux relais Internet distincts et sécurisés. L'adresse IP de l'utilisateur est détectable par le fournisseur réseau de celui-ci et le premier relais, qui est géré par Apple. Les enregistrements DNS de la personne, pour leur part, sont chiffrés afin qu'aucune partie ne puisse identifier l'adresse du site web sur lequel elle souhaite se rendre. Le deuxième relais, qui est géré par un fournisseur de contenu tiers, génère une adresse IP temporaire, déchiffre le nom du site web demandé et connecte l'utilisateur à ce dernier. Le relais privé vérifie que le client qui se connecte est un iPhone, un iPad ou un Mac. Le relais privé remplace l'adresse IP d'origine par une autre comprise dans la plage d'adresses IP utilisée par le service. L'adresse IP de relais attribuée peut être partagée par plusieurs utilisateurs du relais privé se trouvant dans la même zone.

Lorsque les requêtes de navigation web passent par le relais privé, Apple ne peut pas identifier l'adresse IP de l'utilisateur ni le compte utilisateur correspondant à partir des adresses IP du relais privé. Apple n'a aucune information à fournir concernant l'identifiant Apple associé à l'adresse IP du relais privé.

Remarque : le relais privé iCloud n'est pas disponible dans tous les pays ni toutes les régions. Si une personne ayant activé le relais privé se rend dans un pays ou une région où ce service n'est pas disponible, celui-ci se désactivera et se réactivera automatiquement une fois que la personne sera dans un pays ou une région où il est pris en charge.

I. Localiser

Localiser est une fonction qui permet à un client iCloud de localiser ses appareils (iPhone, iPad, iPod touch, Apple Watch, AirPods, Mac ou AirTag) lorsqu'il les a perdus, et/ou de prendre certaines mesures comme mettre l'appareil en mode Perdu, le verrouiller ou en effacer le contenu. Des informations supplémentaires sur ce service sont disponibles à l'adresse www.apple.com/fr/icloud/find-my/.

Pour que la fonctionnalité Localiser fonctionne en cas de perte d'un appareil, celle-ci doit avoir été activée sur cet appareil avant sa perte. La fonctionnalité Localiser ne peut pas être activée sur un appareil à distance, après la perte de celui-ci, ou à la demande d'une autorité publique ou d'une autorité chargée de l'application de la loi. Les informations sur les services de localisation d'un appareil sont stockées sur chaque appareil individuel, et Apple ne peut en aucun cas récupérer ces informations depuis un appareil quel qu'il soit. Les informations sur les services de localisation d'un appareil localisé par la fonctionnalité Localiser étant destinées aux clients, Apple ne dispose pas de dossiers sur les plans ou les alertes fournis par le biais de ce service. L'article suivant fournit des informations et indique la marche à suivre en cas de perte ou de vol d'un appareil iOS : support.apple.com/fr-fr/ HT201472.

Les historiques de connexion de Localiser sont conservés pendant une durée allant jusqu'à 25 jours et, le cas échéant, peuvent être obtenus sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine. L'activité Localiser liée aux demandes de verrouillage ou d'effacement à distance d'un appareil, le cas échéant, peut être obtenue sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

J. AirTag et programme pour accessoires du réseau Localiser

Avec l'app Localiser sur iPhone, iPad, iPod touch et Mac, les clients peuvent facilement localiser des objets personnels en attachant un AirTag ou en utilisant un produit qui fait partie du programme pour accessoires du réseau Localiser.

Grâce à un AirTag, iOS 14.5 et macOS 11.3 (ou versions ultérieures), la clientèle peut recevoir de l'aide en cas de perte d'objets personnels (clés, sacs à dos, bagages, etc.) à l'aide de l'app Localiser. Pour sonner ou pour utiliser la fonctionnalité Localisation précise avec les modèles d'iPhone compatibles, l'AirTag doit être à portée du signal Bluetooth de l'iPhone, de l'iPad ou de l'iPod touch jumelé. Lorsqu'un AirTag n'est pas à proximité de son propriétaire, il est possible d'obtenir son emplacement approximatif s'il se trouve à portée d'un appareil du réseau Localiser, qui comporte des centaines de millions d'appareils Apple dans le monde entier. Pour plus d'informations, consultez les articles support.apple.com/fr-fr/HT212227 et support.apple.com/fr-fr/HT210967.

Le programme pour accessoires du réseau Localiser autorise les produits d'un fabricant d'appareils tiers (vélos, casques, etc.) à utiliser le service pour que les clients puissent localiser leurs produits tiers compatibles avec l'app Localiser sous iOS 14.3 et macOS 11.1 (ou versions ultérieures).

Pour ajouter l'AirTag ou les produits tiers pris en charge dans l'onglet Objets de l'app Localiser, les clients doivent disposer d'un identifiant Apple, se connecter à leur compte iCloud en ayant activé la fonctionnalité Localiser, et associer leur AirTag ou produit tiers pris en charge à leur identifiant Apple. L'interaction est chiffrée de bout en bout, et Apple ne peut pas accéder à l'emplacement d'un AirTag ou autre produit tiers pris en charge. Pour obtenir plus d'informations à ce sujet, consultez l'article support.apple.com/fr-fr/HT211331.

Avec un numéro de série, Apple peut être en mesure de fournir les informations du compte associé en réponse à la demande juridiquement valide pour le pays de la personne qui en est à l'origine. L'historique de jumelage d'un AirTag est disponible pendant une durée allant jusqu'à 25 jours. L'article suivant explique comment trouver le numéro de série d'un AirTag : support.apple.com/fr-fr/HT211658.

Veuillez noter que les numéros de série des appareils Apple ne contiennent ni la lettre « O », ni la lettre « I », mais qu'Apple utilise les chiffres 0 (zéro) et 1 (un) dans ces numéros de série. Les demandes avec des numéros de série contenant les lettres « O » ou « I » ne donneront aucun résultat. Si une demande juridique comprend cinq numéros de série ou plus, Apple demande à ce qu'ils soient également soumis dans un format électronique modifiable (par exemple, un document Numbers, Excel, Pages ou Word).

K. Extraction de données d'appareils iOS verrouillés par un code d'accès

Pour tous les appareils sous iOS 8.0 ou versions ultérieures, Apple ne pourra pas procéder à des extractions de données iOS, car les données qui font généralement l'objet d'une demande des autorités chargées de l'application de la loi sont chiffrées, et Apple ne possède pas la clé de chiffrement. Tous les modèles d'iPhone 6 et modèles ultérieurs sont dotés d'iOS 8.0 ou d'une version ultérieure d'iOS.

Pour les appareils sous iOS 4 à iOS 7, Apple peut, en fonction de l'état de l'appareil, procéder à des extractions de données iOS, conformément à la loi ECPA de Californie (Electronic Communications Privacy Act) (CalECPA, code pénal de Californie, 1546-1546.4). Pour qu'Apple procède à une extraction des données iOS d'un appareil qui répond à ces critères, l'autorité chargée de l'application de la loi doit se procurer un mandat de perquisition émis pour un motif raisonnable en vertu de la loi CalECPA. À l'exception de la loi CalECPA, Apple n'a identifié aucune autorité juridique compétente pouvant contraindre Apple à procéder à des extractions de données en tant que tiers dans le cadre d'une enquête judiciaire.

L. Demande d'adresse IP

Avant de communiquer une adresse IP comme information d'identification dans le cadre d'une procédure judiciaire, Apple demande aux autorités chargées de l'application de la loi de déterminer que l'adresse IP en question n'est pas une adresse IP publique ou de routeur, qu'elle n'utilise pas le NAT de classe transporteur (CGNAT), et de confirmer lors de la procédure judiciaire qu'il s'agit bien d'une adresse IP non publique. En outre, une restriction de date ne dépassant pas trois jours doit être appliquée à ce type de demande. En réponse à une telle demande, Apple peut être en mesure de produire des historiques de connexion (voir ci-dessous, section III.Q), à partir desquels les autorités chargées de l'application de la loi pourront tenter d'identifier un compte Apple ou un identifiant Apple particulier qui servira d'information d'identification dans le cadre d'une demande de procédure judiciaire ultérieure. Les données d'un client Apple fondées sur une adresse IP, le cas échéant, peuvent être obtenues sur présentation d'une

demande juridiquement valide pour le pays de la personne qui en est à l'origine.

M. Autres informations disponibles sur l'appareil

Adresse MAC : une adresse MAC (Media Access Control) est un identifiant unique attribué à des interfaces réseau pour les communications sur le segment du réseau physique. Un produit Apple avec des interfaces réseau aura une ou plusieurs adresses MAC, y compris Bluetooth, Ethernet, Wi-Fi ou FireWire. Cette information peut être obtenue, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine et en fournissant à Apple un numéro de série (ou dans le cas d'un appareil iOS, un numéro IMEI, MEID ou UDID).

N. Demandes de données de vidéosurveillance d'un magasin Apple Store

Les données de vidéosurveillance peuvent varier d'un magasin à l'autre. Elles sont généralement conservées par l'Apple Store pendant une durée maximale de 30 jours. Dans nombre de juridictions, cette durée peut être limitée à seulement vingt-quatre (24) heures en raison des législations locales. Une fois ce délai expiré, les données ne sont plus disponibles. Les demandes qui concernent uniquement les données de vidéosurveillance peuvent être envoyées à lawenforcement@apple.com. S'agissant des données demandées, l'autorité publique ou l'autorité chargée de l'application de la loi doit fournir une date et une heure spécifiques et les informations concernant la transaction.

O. Game Center

Game Center est le réseau social de jeux d'Apple. Des informations sur les connexions d'une personne à Game Center peuvent être mises à disposition. Les historiques de connexion peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

P. Activation d'appareils iOS

Quand un client active un appareil iOS ou met à jour le logiciel, certaines informations sont fournies à Apple par le prestataire de services ou à partir de l'appareil, selon l'évènement. Les adresses IP de l'évènement, les numéros ICCID et autres identifiants peuvent être mis à disposition. Ces informations peuvent être obtenues, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

Double SIM : pour les appareils dotés de la double SIM, les informations sur l'opérateur de la nano-SIM et/ou de l'eSIM disponibles peuvent être obtenues sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine. L'eSIM est une carte SIM numérique qui permet d'activer un forfait mobile auprès d'un opérateur sans avoir à utiliser une nano-SIM physique. Pour obtenir plus d'informations à ce sujet, consultez l'article support.apple.com/fr-fr/HT209044. En Chine continentale, à Hong Kong et à Macao, l'iPhone 12, l'iPhone 12 Pro, l'iPhone 12 Pro Max, l'iPhone 11, l'iPhone 11 Pro, l'iPhone 11 Pro Max, l'iPhone XS Max et l'iPhone XR sont dotés de la double SIM, avec deux cartes nano-SIM.

Q. Historiques de connexion

L'activité de connexion d'une personne ou d'un appareil à des services Apple tels qu'Apple Music, Apple TV, Apple Podcasts, Apple Books, iCloud, Mon identifiant Apple et Apple Discussions, peut être

obtenue, le cas échéant, auprès d'Apple. Ces historiques de connexion avec les adresses IP peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

R. Historiques Mon identifiant Apple et iForgot

Les historiques iForgot et Mon identifiant Apple d'une personne peuvent être obtenus auprès d'Apple. Ceux-ci peuvent inclure des informations sur les réinitialisations de mot de passe. Les historiques de connexion avec les adresses IP peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

S. FaceTime

Les communications FaceTime sont chiffrées de bout en bout, et Apple n'a aucun moyen de déchiffrer les données FaceTime qui transitent entre les appareils. Apple ne peut intercepter des communications FaceTime. Apple dispose des historiques des invitations à un appel FaceTime lorsqu'elles sont initiées. Ces historiques n'indiquent pas que des communications entre les personnes ont réellement eu lieu. Les historiques des invitations à des appels FaceTime sont conservés pendant une durée allant jusqu'à 25 jours. Ces informations peuvent être obtenues, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

T. iMessage

Les communications iMessage sont chiffrées de bout en bout, et Apple n'a aucun moyen de déchiffrer les données iMessage qui transitent entre les appareils. Apple ne peut pas intercepter les communications iMessage et ne possède pas d'historiques des communications iMessage. Apple ne possède pas d'historiques des requêtes iMessage. Ces historiques indiquent qu'une requête a été initiée par l'application d'un appareil (Messages, Contacts, Téléphone ou une autre application) et envoyée aux serveurs d'Apple en vue d'une recherche (pouvant porter sur un numéro de téléphone, une adresse e-mail ou un identifiant Apple) afin de déterminer si la recherche est « compatible avec iMessage ». Les historiques des requêtes iMessage n'indiquent pas que des communications entre les personnes ont réellement eu lieu. Apple ne peut pas déterminer si une communication iMessage a vraiment eu lieu en s'appuyant sur les historiques des requêtes iMessage. Apple ne peut pas non plus identifier l'application ayant initié la requête. Les historiques des requêtes iMessage ne confirment pas qu'un évènement iMessage a réellement fait l'objet d'une tentative. Les historiques des requêtes iMessage sont conservés pendant une durée allant jusqu'à 25 jours. Ces informations peuvent être obtenues, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

U. App Apple TV

L'app Apple TV permet de parcourir, d'acheter, de s'abonner et de regarder des films et séries depuis Apple TV+, les chaînes Apple TV ainsi que des apps et services tiers. L'historique des téléchargements et des achats peut être mis à disposition.

Les demandes de données Apple TV doivent inclure l'identifiant de l'appareil Apple (numéro de série, IMEI, MEID ou GUID) ou l'identifiant Apple/l'adresse e-mail du compte. Si l'identifiant Apple ou l'adresse e-mail du compte ne sont pas connus, Apple exige des informations sur la personne comme

son nom complet et son numéro de téléphone, et/ou son nom complet et son adresse postale afin d'identifier le compte concerné. L'autorité publique ou l'autorité chargée de l'application de la loi peut également fournir un numéro de commande Apple valide, ou un numéro de carte bancaire complet associé aux achats Apple TV. Le nom du client associé à ces paramètres peut être également fourni, mais le nom seul ne suffit pas pour obtenir ces informations.

Remarque : pour préserver la sécurité des données, si une demande juridique contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un document chiffré/protégé par un mot de passe (fichier PDF et autres formats modifiables, par exemple, un document Numbers, Excel, Pages ou Word). Le mot de passe doit être envoyé dans un e-mail séparé. En outre, en raison des normes de sécurité du système, Apple ne téléchargera aucun document associé à une demande juridique à partir d'un lien envoyé par e-mail.

V. Se connecter avec Apple

Se connecter avec Apple offre un moyen plus confidentiel de se connecter aux apps et sites web tiers à l'aide de son identifiant Apple existant. Le bouton Se connecter avec Apple sur un site web ou dans une app partenaire permet de créer un compte et de se connecter à l'aide de son identifiant Apple. Au lieu d'utiliser un compte de média social, de remplir des formulaires ou de choisir un nouveau mot de passe, il suffit de toucher le bouton Se connecter avec Apple, puis de vérifier ses informations pour se connecter rapidement et en toute sécurité avec Face ID, Touch ID ou le code d'accès de son appareil. Pour obtenir plus d'informations à ce sujet, consultez l'article support.apple.com/fr-fr/HT210318.

Masquer mon adresse e-mail est une fonctionnalité de Se connecter avec Apple. Elle utilise le service de relais d'e-mails privés d'Apple pour créer et partager une adresse e-mail aléatoire unique transférant les e-mails depuis l'adresse personnelle d'un client, dont les informations de base peuvent être mises à disposition sur présentation d'une demande juridiquement valide pour le pays de la personne qui en est à l'origine.

IV.Questions fréquentes

Q : puis-je adresser des questions par e-mail à Apple dans le cadre de ma demande d'informations en tant qu'autorité chargée de l'application de la loi ?
R : oui, toute question ou demande concernant une procédure judiciaire peut être envoyée à lawenforcement@apple.com.

Q : un appareil doit-il être inscrit auprès d'Apple pour fonctionner ou être utilisé ?
R : non, un appareil ne doit pas être obligatoirement inscrit auprès d'Apple pour fonctionner ou être utilisé.

Q : Apple peut-elle me transmettre le code d'accès d'un appareil iOS actuellement verrouillé ?
R : non, Apple n'a pas accès au code d'accès des clients.

Q : pouvez-vous m'aider à restituer un appareil perdu ou volé à son propriétaire légitime ?
R : face à une telle situation, contactez lawenforcement@apple.com. Veuillez inclure le numéro de série de l'appareil (ou IMEI, le cas échéant) et toute autre information pertinente dans votre e-mail. Pour savoir comment trouver le numéro de série, consultez l'article support.apple.com/fr-fr/HT204308.

Si des informations sur la personne sont disponibles, nous la contacterons et fournirons des informations aux autorités chargées de l'application de la loi pour récupérer son appareil. Toutefois, s'il n'est pas possible de déterminer l'identité du client à partir des informations disponibles, vous devrez peut-être soumettre une demande juridique valide.

Q : Apple conserve-t-elle une liste des appareils perdus ou volés ?
R : non, Apple ne conserve pas de liste des appareils perdus ou volés.

Q : que convient-il de faire avec les informations fournies en réponse, lorsque l'autorité chargée de l'application de la loi a conclu l'enquête/l'affaire pénale ?
R : les informations et données contenant des informations personnellement identifiables (y compris toutes les copies effectuées), transmises à une autorité publique ou une autorité chargée de l'application de la loi, doivent être détruites après que l'enquête ou l'affaire pénale liée est conclue et que tous les appels sont épuisés.

Q : informez-vous les personnes concernées par des demandes d'informations des autorités chargées de l'application de la loi ?
R : oui, la politique de notification d'Apple s'applique aux demandes relatives aux comptes émanant des autorités chargées de l'application de la loi, des autorités publiques et des particuliers. Apple avertira les clients et les propriétaires de compte sauf en cas d'ordre de non-divulgation ou si la loi en vigueur l'interdit, ou si Apple, à sa seule discrétion, juge raisonnablement que cette mesure pourrait créer un risque de blessure ou de décès d'une personne, dans les cas de mise en danger d'enfants, ou si la notification n'est pas applicable aux faits en cause dans l'affaire.