Recommandations concernant les procédures judiciaires

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 la filiale 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, à l'Apple Store en ligne et à Apple Media Services peuvent également être contrôlées par des entités juridiques en dehors des États-Unis, tel que spécifié dans les conditions générales de chaque service dans une juridiction spécifique. En général, les entités légales 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 les clients d'Apple, y compris les questions de la clientèle sur la divulgation d'informations, doivent être formulées sur la page https://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 ou de la cliente, 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.

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, un portefeuille d'applications logicielles pour les particuliers et les professionnels, les systèmes d'exploitation iOS et Mac OS 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 écrire 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 légales reçues par Apple visent à obtenir des informations sur un client ou une cliente 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 ou de la cliente, 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 légales à 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 légalement 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 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 (Numbers, Pages, etc.). Les identifiants de ce type sont généralement requis afin de rechercher des informations relatives aux appareils, aux comptes ou aux transactions financières.

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 légitimes : ordonnances de production (Australie, Canada, Nouvelle-Zélande), lettres de réquisition ou commissions rogatoires (France), demande de données (Espagne), Ordre judiciaire (Brésil), demande d'informations (Allemagne), demande de divulgation de renseignements personnels (個人情報の開示依頼, Japon), demande de données personnelles, ordonnances, mandats et autorisations des données des communications (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 légale 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 légale 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 première 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 de bonne foi 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 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 dans le cadre d'une telle demande, le ou la responsable de l'agent·e 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·e et invité·e 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 Global Security Operations Centre (GSOC) d'Apple au 001 408 974-2095. Ce numéro est pris en charge 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 que l'ordonnance du tribunal ne démontre pas que le compte 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 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 et clientes quand les informations de leur compte Apple sont recherchées en réponse à une demande légale 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 légale 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 et clientes 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 juridique 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 enregistrent un appareil sous une version antérieure à iOS 8 et Mac OS Sierra 10.12 transmettent à Apple des informations d'inscription de base ou personnelles, y compris 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 sous Mac OS 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 mises à disposition sur présentation d'une demande juridiquement valide pour le pays du demandeur.

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.

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 les clients 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 du demandeur.

C. Services Apple Media

App Store, Apple Music, l'app Apple TV, Apple Podcasts et Apple Books (« Apple Media Services ») sont des applications logicielles permettant d'organiser et de lire des apps, de la musique et des vidéos numériques et du contenu en streaming. Apple Media Services fournit également du contenu à télécharger depuis un ordinateur ou appareil iOS. Lorsqu'une personne crée un compte Apple, elle peut communiquer des informations de base comme ses nom, adresse postale, adresse e-mail et numéro de téléphone. De plus, des données sur les transactions et connexions liées aux achats/téléchargements sur Apple Media Services, ainsi que les connexions liées à des mises à jour/nouveaux téléchargements et les connexions Apple Media Services, peuvent aussi être mises à disposition. Les informations sur les clients et clientes Apple Media Services et les journaux de leurs

connexions avec les adresses IP 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.

Les demandes de données Apple Media Services 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 Apple Media Services concerné. L'autorité publique ou l'autorité chargée de l'application de la loi peut également fournir un numéro de commande Apple Media Services valide, ou un numéro de carte bancaire complet associé aux achats Apple Media Services. Le nom du client associé à ces paramètres peut être également fourni, mais le nom du client seul ne suffit pas pour obtenir ces informations.

Remarque : pour préserver la sécurité des données, si une demande légale contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un fichier/document chiffré/protégé par un mot de passe. Le mot de passe doit être envoyé dans un e-mail séparé.

D. Transactions dans un magasin de vente Apple Store

Les transactions en magasin sont des transactions effectuées en espèces, par carte bancaire ou cartes cadeaux dans un magasin de vente 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 du demandeur.

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 du demandeur.

Remarque : pour préserver la sécurité des données, si une demande légale contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un fichier/document chiffré/protégé par un mot de passe. Le mot de passe doit être envoyé dans un e-mail séparé.

E. Achats sur l'Apple Store en ligne

Apple conserve les informations relatives aux achats dans l'Apple Store en ligne, 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 sur l'Apple Store en ligne, 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 du client seul ne suffit pas pour obtenir ces informations. Les demandes d'informations concernant des commandes sur l'Apple Store en ligne 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 achats sur l'Apple Store en ligne, 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 légale contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un fichier/document chiffré/protégé par un mot de passe. Le mot de passe doit être envoyé dans un e-mail séparé.

F. Cartes cadeaux

Les cartes cadeaux Apple Store et les cartes cadeaux Apple Store et iTunes ont un numéro de série et un code PIN (ou code PIN d'utilisation). Les cartes cadeaux Apple Store et les cartes cadeaux Apple Store et iTunes ont plusieurs formats de numéro de série qui dépendent de variables telles que le design et/ou la date d'émission. Les codes PIN d'utilisation permettent à la personne qui détient la carte cadeau d'accéder aux fonds crédités sur la carte cadeau. Le code PIN de la carte cadeau est le paramètre le plus fiable permettant à Apple de rechercher des informations relatives à la carte cadeau. Apple peut fournir les informations disponibles relatives aux cartes cadeaux App Store et aux cartes cadeaux 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 légale comprend cinq codes PIN de cartes cadeaux ou plus, Apple demande à ce que ces codes PIN de cartes cadeaux soient également soumis dans un format électronique modifiable.

i. Cartes cadeaux Apple Store

Les cartes cadeaux Apple Store peuvent être utilisées pour effectuer des achats dans un magasin de vente Apple Store ou sur l'Apple Store en ligne. Le code PIN figurant sur une carte cadeau Apple Store commence par la lettre « Y ». Dans certains cas, des cartes cadeaux Apple Store plus anciennes peuvent avoir un code PIN à huit chiffres. 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 du demandeur.

Remarque : pour préserver la sécurité des données, si une demande légale 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 fichier/document chiffré/protégé par un mot de passe. Le mot de passe doit être envoyé dans un e-mail séparé.

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. Le code PIN figurant sur une carte cadeau App Store et iTunes commence par la lettre « X ». Grâce au code PIN, 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 iTunes Store est utilisée, les informations disponibles peuvent inclure les informations sur le compte Apple concerné, la date et l'heure de l'activation et/ou 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 légale 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 fichier/document chiffré/protégé par un mot de passe. Le mot de passe doit être envoyé dans un e-mail séparé.

G. Apple Pay

Les transactions Apple Pay effectuées en magasin (par exemple pour les communications NFC/sans contact) et sur 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 crypté 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, consulter : https://support.apple.com/fr-fr/HT207957.

Pour demander les données de transactions des achats effectués dans les magasins Apple Store, Apple a besoin du numéro du compte principal de l'appareil (DPAN) et d'un identifiant haché (le plus souvent à 64 chiffres) pouvant être obtenu auprès de l'établissement émetteur. Pour connaître le numéro DPAN associé à une transaction Apple, il faut s'adresser à la banque ou à l'établissement émetteur de la carte bancaire. Le numéro DPAN permettra à Apple de rechercher les informations demandées à travers 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 du demandeur.

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 du demandeur. 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 légale contient un numéro DPAN, celui-ci doit être envoyé par e-mail à l'adresse lawenforcement@apple.com dans un fichier/

document chiffré/protégé par un mot de passe. Le mot de passe doit être envoyé dans un e-mail séparé.

H. iCloud

iCloud est un service d'Apple qui permet à la clientèle d'accéder à sa musique, ses photos, ses documents et plus encore à partir de tous ses appareils. Elle peut également sauvegarder le contenu de ses appareils iOS sur iCloud. Avec le service iCloud, il est possible de créer 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. Lorsqu'il est fait appel à des revendeurs tiers pour stocker des données, Apple ne leur donne jamais les clés de chiffrement. Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis.

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.

Les informations ci-dessous peuvent être mises à disposition à partir d'iCloud :

i. Informations sur la clientèle

Lorsqu'un compte iCloud est créé, des informations de base sur la personne comme ses nom, adresse postale, adresse e-mail et 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 et clientes iCloud et les journaux de leurs connexions avec les adresses IP 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. Les journaux des connexions sont conservés pendant une durée allant jusqu'à 25 jours.

ii. Journaux d'e-mails

Les journaux d'e-mails 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 journaux d'e-mails 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 du demandeur.

iii. Contenu des e-mails et autres contenus iCloud. Sauvegardes des 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 paramètres de l'appareil, les données des apps, les iMessage, 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. Lorsqu'il est fait appel à des revendeurs tiers pour stocker des données, Apple ne leur donne jamais les clés de chiffrement. Apple conserve les clés de chiffrement dans ses centres de données aux États-Unis.

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 ou de la cliente, tel qu'il existe sur son compte, uniquement en réponse à une demande valide juridiquement.

I. Localiser

Localiser mon est une fonction activée par l'utilisateur qui permet à un client ou une cliente iCloud de localiser son iPhone, iPad, iPod touch, Apple Watch, AirPods ou Mac lorsqu'il ou elle l'a perdu 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 https://www.apple.com/fr/icloud/find-my/.

Pour que la fonctionnalité Localiser mon fonctionne en cas de perte d'un appareil, celle-ci doit avoir été activée sur cet appareil avant sa perte. La fonctionnalité Localiser mon 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 mon étant destinées aux clients et clientes, Apple ne dispose pas de dossiers sur les plans ou les alertes fournis par le biais de ce service. Le lien d'assistance suivant fournit des informations et la procédure à suivre en cas de perte ou de vol d'un appareil iOS : https://support.apple.com/fr-fr/HT201472.

Les journaux de connexion de Localiser mon sont conservés pendant une durée pouvant aller jusqu'à 25 jours et, le cas échéant, peuvent être obtenus sur présentation d'une demande juridiquement valide pour le pays du demandeur. L'activité Localiser mon 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 du demandeur.

J. 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 ultérieurs sont dotés d'iOS 8.0 ou 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.

K. 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, avec une demande juridiquement valide pour le pays de la personne qui en est à l'origine en fournissant à Apple un numéro de série (ou dans le cas d'un appareil iOS, un numéro IMEI, MEID ou UDID).

L. Demandes de données de vidéosurveillance d'un magasin de vente 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 concernant 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.

M. 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 journaux des connexions avec les adresses IP et l'historique des transactions peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays du demandeur.

N. Activation d'appareils iOS

Quand un client ou une cliente 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'événement. Les adresses IP de l'événement, 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 du demandeur.

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 doivent 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 correspondant à l'adresse http://support.apple.com/fr-fr/HT209044. En Chine continentale, à Hong Kong et à Macao, l'iPhone 11, l'iPhone 11 Pro, l'iPhone 11 Pro Max et l'iPhone XR sont dotés de la double SIM, avec deux cartes nano-SIM.

O. 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 journaux des connexions 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.

P. Mon identifiant Apple et journaux iForgot

Les journaux 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 journaux des connexions avec les adresses IP peuvent être obtenus, le cas échéant, sur présentation d'une demande juridiquement valide pour le pays du demandeur.

Q. 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 journaux des invitations à un appel FaceTime lorsqu'elles sont initiées. Ces journaux n'indiquent pas que des communications entre les personnes ont réellement eu lieu. Les journaux 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.

R. 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 de journaux des communications iMessage. Apple ne possède pas de journaux des requêtes iMessage. Ces journaux 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 journaux 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 se basant sur les journaux des requêtes iMessage. Apple ne peut pas non plus identifier l'application ayant initié la requête. Les journaux des requêtes iMessage ne confirment pas qu'un événement iMessage a réellement fait l'objet d'une tentative. Les journaux 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.

S. 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+, Apple TV Channels et 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 du client seul ne suffit pas pour obtenir ces informations.

Remarque : pour préserver la sécurité des données, si une demande légale contient des informations complètes de carte bancaire, celles-ci doivent être envoyées par e-mail à l'adresse lawenforcement@apple.com dans un fichier/document chiffré/protégé par un mot de passe. Le mot de passe doit être envoyé dans un e-mail séparé.

T. Connexion avec Apple

Connexion 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 Connexion avec Apple sur un site Web ou 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 réseau social, de remplir des formulaires ou de choisir un nouveau mot de passe, il suffit de toucher le bouton Connexion avec Apple, puis de passer en revue ses informations pour se connecter rapidement et en toute sécurité avec Face ID, Touch ID ou le mot de passe de son appareil. Pour obtenir plus d'informations à ce sujet, consultez l'article correspondant à l'adresse https://support.apple.com/fr-fr/HT210318.

Masquer mon adresse e-mail est une fonctionnalité de Connexion 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 ou d'une cliente, 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 et réponses

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 en justice 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 utilisateurs.

Q : Pouvez-vous m'aider à restituer un appareil perdu ou volé à son propriétaire légitime ?
R : Si ces situations se présentent, contactez lawenforcement@apple.com. Veillez à préciser l'IMEI ou le numéro de série de l'appareil, ainsi que toute autre information pertinente. Si des informations sur la personne client sont disponibles, nous la contacterons et lui conseillerons de s'adresser 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 légale 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 clientes 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'un membre du public, dans les cas de mise en danger d'enfants, ou si la notification n'est pas applicable aux faits en cause dans l'affaire.