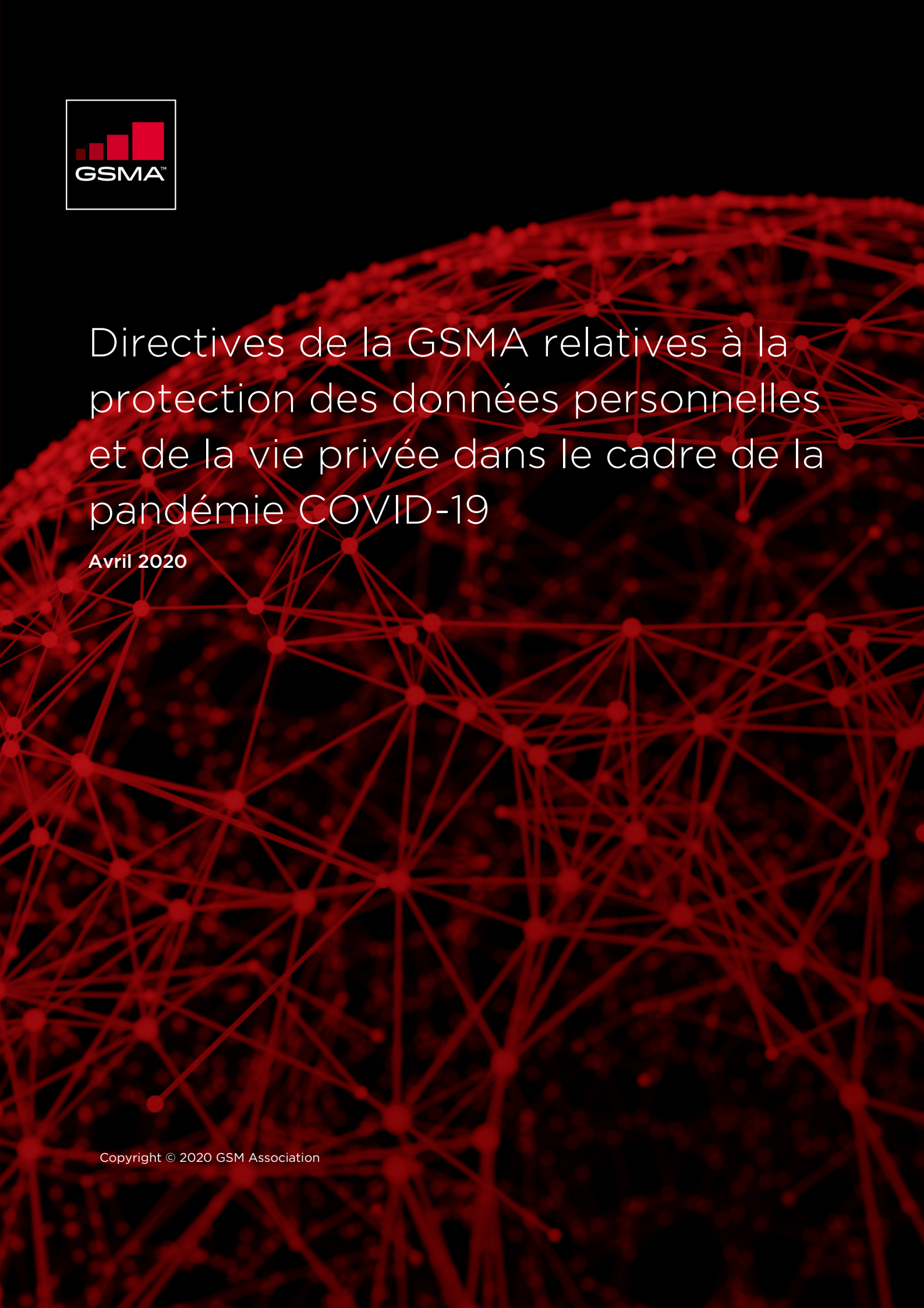

Directives de la GSMA relatives à la protection des données personnelles et de la vie privée dans le cadre de la pandémie COVID-19

Avril 2020

Introduction

Alors que la pandémie de COVID-19 continue de se propager rapidement dans de nombreuses régions du monde, des gouvernements et des organismes publics demandent à avoir accès aux données ou aux informations analytiques détenues par les opérateurs de réseau mobile (ORM) et d'autres entreprises.

Les données et les informations analytiques provenant des réseaux mobiles et d'autres sociétés Internet peuvent s'avérer très utiles, dans la mesure où la mobilité des personnes est l'un des facteurs essentiels qui contribuent à la propagation de virus infectieux transmis par l'homme. Des informations précises et à jour sur des schémas de mobilité agrégés pourraient potentiellement être vitales à des fins de surveillance, pour prévoir les flambées de la maladie et planifier les besoins de ressources futurs, notamment en matière de kits de dépistage, de lits, de personnel médical ou de matériel. D'autres utilisations pourraient inclure l'identification de personnes susceptibles d'avoir été en contact avec des cas confirmés ou informer les gens s'ils sont entrés dans une zone affectée, à condition que cela soit conforme à la loi.

Le secteur de la téléphonie mobile reconnaît l'urgence avec laquelle les gouvernements doivent agir pour ralentir la propagation du COVID-19, et la volonté de certains d'entre eux de chercher de l'aide à cet égard. Pour autant, le secteur de la téléphonie mobile reconnaît que l'utilisation des données des opérateurs de réseau mobile par des gouvernements ou des organismes publics soulève de graves préoccupations en matière de protection des données et de la vie privée. Ces directives reflètent les recommandations sur la façon dont le secteur de la téléphonie mobile peut préserver la confiance du public tout en répondant aux demandes d'aide que lui adressent les gouvernements et les organismes de santé publique dans la lutte contre le COVID-19.

Termes clés utilisés dans ces directives :

« Métadonnées » désigne les données de trafic comprenant les enregistrements détaillés des appels[1] provenant de réseaux mobiles, y compris les cas où les identifiants clés, tels que le numéro de téléphone mobile et les informations sur les abonnés, ont été remplacés par un pseudonyme[2].

« Données Non Identifiables Agrégées » désigne les métadonnées sous une forme agrégée et selon des seuils appropriés (par exemple, quant au nombre d'individus, en matière de temps et/ou d'espace), qui sont conçus pour empêcher la possibilité de réidentifier des individus. Sont généralement incluses les matrices d'origine et de destination ou les informations sur les lieux fréquentés générées à partir des Métadonnées. Bien que tous les efforts soient déployés pour concevoir des ensembles de données qui empêchent une possible réidentification, le risque résiduel et théorique qui subsiste résiste difficilement à « l'épreuve du droit » du véritable anonymat qui est imposé dans certains pays

[1] Données CDR (« Call Detail Records » : enregistrements détaillés des appels) : enregistrement d'un appel vocal ou d'une autre opération, par exemple : SMS généré par un opérateur de réseau mobile, qui comporte les numéros de téléphone mobile de la personne qui passe l'appel et aussi de celle qui le reçoit, l'heure et la durée de l'appel, ainsi que des informations de localisation de basse résolution (tour cellulaire la plus proche).
[2] Il y a lieu de noter que la plupart des lois sur la protection des données s'appliquent aux données permettant d'identifier un individu. Lorsqu'il est possible d'identifier des individus à partir de données pseudonymes, les lois sur la protection des données s'appliquent généralement, tout en reconnaissant aussi que la pseudonymisation est une mesure de précaution précieuse.

« Informations analytiques » désigne le produit, le tableau de bord ou la visualisation des analyses effectuées sur des Données Non Identifiables Agrégées.

« Données des Opérateurs Mobiles » désigne l'une ou l'ensemble des définitions ci-dessus pour les Métadonnées, les Données Non Identifiables Agrégées et les Informations analytiques.

« Gouvernements ou Organismes publics » inclut les gouvernements nationaux, les autorités de santé publique et d'autres organismes publics tels que les agences des Nations Unies, des organisations internationales et intergouvernementales ou des organismes publics régionaux qui cherchent à avoir accès aux Données des Opérateurs Mobiles afin de les aider à contenir, retarder la propagation du virus, ou à mener des recherches là-dessus, ou à en atténuer les effets sur la santé publique.

« Chercheurs » inclut les établissements universitaires qui cherchent à accéder aux Données des Opérateurs Mobiles acquises par les Gouvernements ou les Organismes publics.

Directives de la GSMA relatives à la protection des données personnelles et de la vie privée dans le cadre de la pandémie COVID-19

La GSMA recommande aux opérateurs de réseau mobile « ORM » d'adopter les approches suivantes en réponse aux demandes d'accès aux Données des Opérateurs Mobiles dans la lutte contre la propagation du COVID-19 :

Respect de la loi et la considération de l'éthique

- Respecter toutes les obligations légales et les conditions de licence en vigueur.
- Adopter en amont de bonnes pratiques relatives à la protection des données personnelles et de la vie privée, comme les Principes de protection des données personnelles et de la vie privée dans le cadre des communications mobiles de la GSMA[3] et envisager les implications éthiques du partage légal des Données des Opérateurs Mobiles dans le but d'aider des Gouvernements ou des Organismes publics à contenir ou à retarder la propagation du virus, à faire des recherches dessus ou à en atténuer l'impact sur la santé publique.
- Entamer le dialogue avec les Gouvernements ou les Organismes publics et, s'il y a lieu, les juridictions concernées, pour demander des précisions lorsque le fondement juridique d'une demande est vague ou incertain ou lorsque des pouvoirs d'urgence supplémentaires peuvent être nécessaires pour étayer une demande.

Le partage d'Informations analytiques ou de Données Non Identifiables Agrégées à des Gouvernements ou à des Organismes publics échappe généralement au champ d'application plus général des lois de protection des données, dès lors que ces données sont véritablement anonymes. Lorsque les lois sur la protection des données s'appliquent bien à l'utilisation de Données Non Identifiables Agrégées, ce

[3] Rapport de la GSMA : Principes du respect de la vie privée dans le secteur du mobile - Promouvoir le respect de la vie privée du consommateur dans l'écosystème du mobile

partage est généralement autorisé pour des raisons d'intérêt public, même si, bien entendu, les ORM doivent examiner les exigences juridiques locales et s'y conformer.

Dans des cas exceptionnels, il est possible que des Gouvernements ou des Organismes publics soient amenés à demander des Métadonnées se rapportant à des individus spécifiques, par exemple pour identifier ceux susceptibles d'avoir été en contact avec des cas confirmés ou pour informer les personnes qui sont entrées dans une zone affectée. Ces données ne doivent être partagées que sous réserve d'un fondement juridique valable à leur traitement, telle que, selon la législation locale en vigueur, l'obtention avérée du consentement de l'individu, pour agir dans l'intérêt vital de l'individu en cas d'urgence ou conformément à une loi spécifique exigeant le partage des données. Une pareille loi spécifique devrait être nécessaire pour la sécurité publique et absolument vitale et proportionnée pour atteindre un objectif précis et légitime qui doit être conforme aux normes reconnues sur le plan international en matière de protection de la vie privée, des droits de l'homme et les autre lois applicables..

Transparence

- Faire preuve de transparence avec le public au sujet du partage des Données des Opérateurs Mobiles avec des Gouvernements ou des Organismes publics, sauf si la loi l'interdit
- Aider les Gouvernements ou les Organismes publics à lutter contre la désinformation et sensibiliser le public au partage des données pour contribuer à lutter contre le COVID-19

La transparence est essentielle au maintien de la confiance et à la prévention de la circulation de rumeurs infondées. Il est essentiel que les ORM ainsi que les Gouvernements ou les Organismes publics soient francs avec le public quant à l'étendue et à la nature du partage des données dans le contexte de la lutte contre la pandémie de COVID-19.

Informations analytiques et Données Non Identifiables Agrégées

- Interdire la ré-identification des individus à partir d'Informations analytiques et de Données Non Identifiables Agrégées au sein de leurs organisations respectives
- Procéder à la conversion des Métadonnées en Informations analytiques et en Données Non Identifiables Agrégées avant de les communiquer à des Gouvernements ou à des Organismes publics, et afin d'éviter de partager les données sous-jacentes originales

Il appartient aux ORM de procéder à la transformation des Métadonnées en des Informations analytiques et des Données Non Identifiables Agrégées pour les décideurs politiques avant leur communication à des Gouvernements ou à des Organismes publics afin de réduire la quantité et le caractère sensible des données partagées avec des Gouvernements ou des Organismes publics.

Lors du processus de désidentification des données, que ce soit par agrégation ou par d'autres techniques, il appartient aux ORM d'évaluer le risque de ré-identification, en particulier celui se rapportant à l'environnement externe et aux autres ensembles de données COVID-19 disponibles. Une évaluation de l'impact sur la protection des données et de la vie privée doit également être effectuée lors de la désidentification.

Le format dans lequel les Gouvernements demandent des Informations analytiques ou des Données Non Identifiables Agrégées varie d'un pays à l'autre, ce qui rend plus difficile l'établissement de comparaisons

utiles. Les ORM peuvent travailler avec les Gouvernements et les Organismes publics pour mieux comprendre ce qu'il est possible de faire, réduire au minimum les informations demandées et partagées et chercher à harmoniser leurs demandes à l'avenir, en gardant à l'esprit les différences qui existent en matière de réglementation et d'autres facteurs pertinents.

Métadonnées

- Le partage de Métadonnées avec des Gouvernements ou des Organismes publics n'est autorisé que s'il est légitime de le faire, par exemple, dans de nombreux territoires, s'il est dans l'intérêt vital de l'individu concerné, ou sur la base d'un consentement valide ou si une loi l'exige spécifiquement. Une telle loi devrait être absolument nécessaire et proportionnée pour atteindre un objectif précis et légitime conforme aux normes reconnues sur le plan international en matière de protection de la vie privée, des droits de l'homme et d'autres lois pertinentes.

Dans des cas exceptionnels, il est possible que des Gouvernements ou des Organismes publics demandent des Métadonnées concernant un ou plusieurs individus. Une demande légale de ce type peut être dans l'intérêt supérieur des personnes concernées, y compris, par exemple, lors de l'identification de personnes qui ont été en contact avec des cas connus de COVID-19 ou pour avertir des individus qu'ils sont peut-être entrés, ou sont sur le point d'entrer, dans une zone infectée.

Les lois générales sur la protection des données, comme le RGPD de l'Union européenne, autorisent généralement le traitement de données à caractère personnel s'il est dans l'intérêt vital de l'individu de le faire ou si un consentement valable a été donné. Cependant, sa légalité dans un cas particulier dépendra des circonstances précises et de la compétence juridique.

Certaines lois et conditions de licence mobile visant les fournisseurs de données de communications électroniques interdisent l'utilisation des Métadonnées à de telles fins à moins que le consentement n'ait été donné ou sur autorisation d'une loi adoptée spécifiquement dans le but de protéger la sécurité publique.

Garanties des Gouvernements ou des Organismes publics

- Même si, quoi qu'il en soit, tout partage de données ne peut se faire que dans le respect de la loi, les ORM doivent, le cas échéant, demander aux Gouvernements ou aux Organismes publics de prendre les engagements suivants :

  Légalité et équité

  Confirmer que l'utilisation de Métadonnées ou de Données Non Identifiables Agrégées est légale et équitable à l'égard de toute personne concernée en tenant compte de toutes les circonstances et des impacts potentiels. Dans la mesure où la demande repose sur une loi spécifique dans l'intérêt de la sécurité publique, que ces lois sont nécessaires et proportionnées pour atteindre un objectif précis et légitime conforme aux normes reconnues sur le plan international en matière de protection de la vie privée, des droits de l'homme et d'autres lois pertinentes.

  Les Gouvernements et les Organismes publics sont priés de solliciter l'avis de l'autorité de contrôle de la protection des données et/ou du régulateur national des télécommunications dans le pays concerné et de partager ces avis avec les ORM.

En outre, il appartient aux Gouvernements ou aux Organismes publics de prévoir des limites de responsabilité adéquates ou d'indemniser les ORM contre les réclamations légales relatives au respect des requêtes et des obligations pour la conservation, la divulgation et l'interception des communications et des données.

Transparence

Faire preuve de la plus grande transparence possible avec le public quant à l'utilisation de Données des Opérateurs Mobiles et au cadre juridique applicable.

Limitation de la finalité

Indiquer clairement à quelle fin les Métadonnées ou les Données Non Identifiables Agrégées sont partagées et en empêcher la réutilisation à d'autres fins et, en particulier, à des fins non liées à la lutte contre la propagation du COVID-19. Dans le cas où un Gouvernement ou un Organisme autoriserait des Chercheurs à accéder aux Données Non Identifiables Agrégées, il devra vérifier, contrôler et, s'il y a lieu, bloquer tout sujet de recherche proposé qui ne serait pas conforme à la finalité initiale.

Interdiction de ré-identification

Appliquer une règle stricte interdisant la ré-identification de Métadonnées ou de Données Non Identifiables Agrégées par le personnel ou des Chercheurs, sauf dans la mesure autorisée par la loi et avec préavis aux individus identifiés.

Sécurité

Mettre en place des mesures technologiques et organisationnelles appropriées pour assurer la sécurité de toutes les Données des Opérateurs Mobiles lorsqu'elles sont « au repos » et « en transit ». Sont également concernés les protocoles d'accès et les autorisations appropriées.

Évaluation de l'impact sur la protection des données

Réaliser une évaluation de l'impact sur la protection des données en ce qui concerne les Métadonnées ou les Données Non Identifiables Agrégées qui ont été reçues.

Éviter toute discrimination et respecter les droits fondamentaux

Respecter les principes de l'égalité de la protection en vertu de la loi, et ne pas utiliser des Données d'Opérateurs Mobiles ou des Informations analytiques pour discriminer de manière inappropriée des individus ou des groupes, ou pour violer les droits fondamentaux.

Chercheurs

Contrôler correctement les Chercheurs et le champ d'application de leurs projets de recherche et les contraindre à une norme équivalente de respect de ces directives. Ces précautions doivent

inclure le contrôle de leur accès et l'obligation de supprimer toutes les Données d'Opérateurs Mobiles une fois les travaux de recherche terminés.

Conservation

Supprimer les Données d'Opérateurs Mobiles après une période définie ou une fois qu'elles ne sont plus nécessaires pour la finalité sanitaire convenue.

Responsabilité

Fournir la preuve qu'ils ont agi conformément aux garanties données. Mettre en place un conseil de surveillance indépendant pour contrôler le respect de ces principes.

Les documents ci-dessous font partie d'un large éventail de ressources et d'initiatives de la GSMA concernant le respect de la vie privée, qui sont décrites en détail dans les liens suivants :

- Protection de la vie privée sur mobile et big data
- Rapport de la GSMA : Sécurité, respect de la vie privée et sûreté dans l'ensemble de l'écosystème mobile
- Rapport de la GSMA : Connaissances approfondies issues des études sur les consommateurs et considérations pour les décideurs
- Rapport de la GSMA : Principes du respect de la vie privée dans le secteur du mobile - Promouvoir le respect de la vie privée du consommateur dans l'écosystème du mobile
- Rapport de la GSMA : Directives relatives à la protection de la vie privée pour le développement des applications mobiles
- Manuel des politiques de communications mobiles de la GSMA

Directives de la GSMA relatives à la protection des données personnelles et de la vie privée dans le cadre de la pandémie COVID-19 v0.1

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com