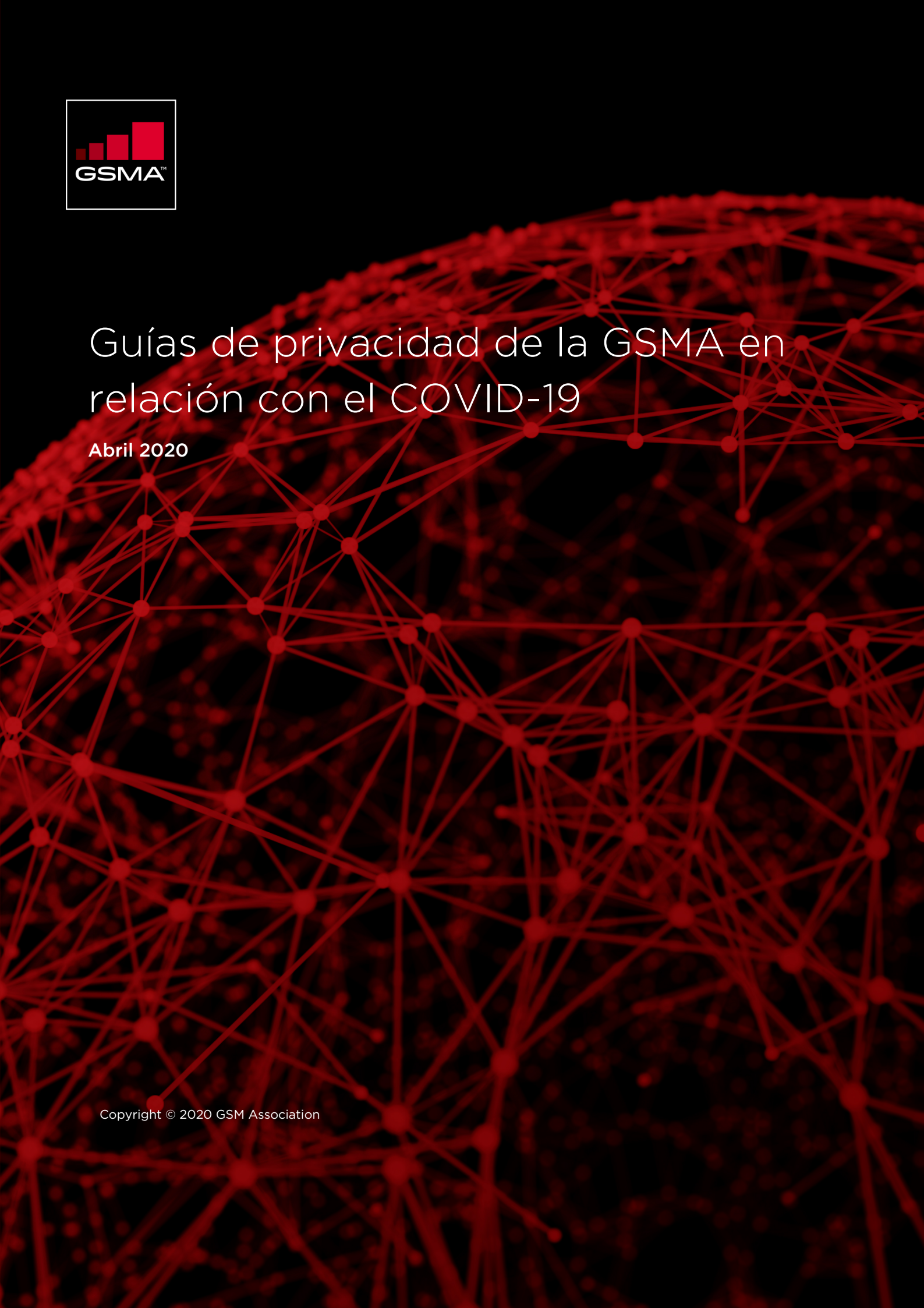

Guías de privacidad de la GSMA en relación con el COVID-19

Abril 2020

Introducción

El brote coronavirus (COVID-19) sigue extendiéndose rápidamente en muchas partes del mundo. Como consecuencia, algunos gobiernos y otros organismos están solicitando los datos o la información procesada que están en manos de operadores móviles y de otras compañías.

Los datos y la información procesada de los operadores móviles y de Internet pueden ser importantes porque la movilidad de las personas es uno de los factores críticos que contribuyen a la propagación de virus infecciosos de transmisión humana. La información precisa y actualizada sobre patrones agregados de movilidad podría ser crucial para el monitoreo, la predicción de brotes y la planificación de las necesidades futuras de recursos, como tests, camas de hospital, personal o equipos sanitarios. También se podría utilizar para la identificación de individuos que puedan haber estado en contacto con casos de contagio confirmados, o para informar a las personas cuando entran en zonas afectadas, siempre de conformidad con la ley.

La industria móvil es consciente de la urgencia con la que deben actuar los gobiernos para ralentizar la propagación de la COVID-19 y del deseo de algunos gobiernos de solicitar ayuda en este sentido. Al mismo tiempo, la industria móvil sabe que el uso de los datos de los operadores móviles por parte de los gobiernos u organismos plantea serias inquietudes en relación con la privacidad. Estas guías ofrecen recomendaciones para que la industria móvil pueda conservar la confianza del público y, al mismo tiempo, dar respuesta a los gobiernos y organismos de salud pública que soliciten ayuda para luchar contra la pandemia del coronavirus.

Términos clave utilizados en estas Guías:

Metadatos los datos sobre tráfico, como los registros de detalles de llamadas[1] desde redes móviles, incluidos aquellos en los que identificadores clave, como el número del teléfono móvil y la información del suscriptor, se han reemplazado con un pseudónimo[2].

Datos Agregados No Identificables son Metadatos agregados con límites apropiados (por ejemplo, en cuanto al número de personas, el tiempo y/o el espacio) diseñados para evitar la posibilidad de que se pueda re-identificar a los individuos. Normalmente incluyen matrices origen-destino o información sobre el flujo del tráfico de personas generada a partir de Metadatos. Aunque al diseñar estos conjuntos de datos se realizan grandes esfuerzos para evitar la posibilidad de re-identificación, subsiste un riesgo residual y teórico que dificulta cumplir el requisito legal de anonimato auténtico que imponen algunas jurisdicciones.

Insights o "Información procesada" es el producto, la representación o visualización del análisis realizados con Datos Agregados No Identificables.

[1] Registros de Detalles de Llamadas (CDR, por sus siglas en inglés): registros de una llamada de voz o de otra transacción, por ejemplo, un mensaje de texto (SMS) generado por un operador móvil que incluye tanto el número de teléfono de la persona que hace la llamada como el de la que la recibe, la fecha, la hora y la duración de la llamada, e información de baja resolución sobre la ubicación (torre celular más cercana).
[2] Nota: la mayoría de la legislación sobre protección de datos se aplica a datos a partir de los cuales un individuo es identificado o puede ser identificable. En los casos en que sea posible identificar a personas a partir de datos pseudoanonimizados, normalmente se aplican las leyes de protección de datos, pero estas también reconocen que la pseudoanonimización es una buena medida de seguridad.

Datos de Operadores Móviles se refiere a cualquiera o todas las definiciones anteriores de Metadatos, Datos Agregados No Identificables e Insights.

Gobiernos u Organismos Internacionales incluye a los gobiernos, autoridades de la salud pública y otros organismos tales como la Organización de Naciones Unidas, organizaciones internacionales e intergubernamentales u organismos regionales que desean acceder a Datos de Operadores Móviles para que les ayuden a contener, ralentizar o investigar la propagación del virus o mitigar su impacto en la salud pública.

Investigadores incluye a instituciones académicas que desean acceder a Datos de Operadores Móviles adquiridos por los Gobiernos u Organismos Internacionales.

Guías de privacidad de la GSMA en relación con el COVID-19

A continuación se exponen las recomendaciones de la GSMA que deberían seguir los operadores móviles al estudiar las solicitudes de acceso a Datos de Operadores Móviles relacionadas con el brote de COVID-19:

Cumplimiento de la ley y aspectos éticos

- Cumplir con todos los requisitos legales y condiciones aplicables de acuerdo a las licencias otorgadas.
- Tomar medidas proactivas para implementar buenas prácticas de privacidad, como los Principios de Privacidad Móvil de la GSMA[3], y tener en cuenta los aspectos éticos relacionados con la cesión lícita de Datos de Operadores Móviles para ayudar a los gobiernos u organismos a contener, ralentizar o investigar la propagación del virus o mitigar su impacto en la salud pública.
- Trabajar conjuntamente con los gobiernos, organismos y, si es necesario, tribunales, para buscar claridad cuando la base legal de una solicitud resulte incierta o poco clara, o cuando se requieran poderes adicionales de urgencia para respaldar la solicitud.

La cesión de Insights o de Datos Agregados No Identificables a Gobiernos u Organismos Internacionales normalmente está fuera del ámbito de las leyes generales de protección de datos en la medida en que esa información o esos datos sean verdaderamente anónimos. Cuando las leyes de protección de datos no sean aplicables al uso de Datos Agregados No Identificables, normalmente dicho uso se permite sobre la base de que son de interés público, aunque los operadores móviles deberán, por supuesto, revisar y cumplir los requisitos legales locales.

En casos excepcionales, los Gobiernos y Organismos Internacionales podrían solicitar Metadatos relacionados con individuos concretos, por ejemplo, para la identificación de personas que puedan haber estado en contacto con casos confirmados, o para informar a personas cuando entran en zonas afectadas. Estos datos solo se deben ceder con una base legal válida para su tratamiento como por

[3] Informe de la GSMA: Mobile Privacy Principles Promoting consumer privacy in the mobile ecosystem

ejemplo, dependiendo de la legislación local, la obtención del consentimiento del individuo, la actuación para defender intereses vitales del individuo en una emergencia, o el cumplimiento de una ley específica que requiera la cesión de los datos. Dicha ley específica sería requisito ineludible para fines de seguridad pública, y absolutamente necesaria y proporcionada para alcanzar una finalidad concreta y legítima que sea coherente con estándares de privacidad reconocidos internacionalmente, los derechos humanos y otras leyes pertinentes.

Transparencia

- Ofrecer al público transparencia en relación con la cesión de Datos de Operadores Móviles a Gobiernos u Organismos Internacionales, a menos que la ley lo prohíba.
- Ayudar a los gobiernos u organismos a combatir la desinformación y concientizar sobre la necesidad de compartir datos para luchar contra la COVID-19.

La transparencia es clave para mantener la confianza del público y evitar que circulen rumores infundados. Es esencial que los operadores móviles, así como los gobiernos u organismos, sean transparentes con el público acerca del alcance y la naturaleza de la cesión de datos en el contexto del COVID-19.

Insights y Datos Agregados no Identificables

- Prohibir la re-identificación de individuos a partir de información procesada y Datos Agregados No Identificables dentro de sus respectivas organizaciones.
- Llevar a cabo la transformación de Metadatos en Insights o en Datos Agregados No Identificables antes de su cesión a gobiernos u organismos. Para evitar la cesión de datos subyacentes,

El proceso de transformación de Metadatos en Datos Agregados No Identificables para uso de los responsables de políticas públicas debería ser realizado por los operadores móviles, a fin de reducir la cantidad y sensibilidad de los datos cedidos a gobiernos u organismos.

Al realizar la desidentificación, bien sea por medio de la agregación o de otras técnicas, los operadores móviles deberían evaluar el riesgo de re-identificación, en particular en relación con el entorno externo y los otros conjuntos de datos disponibles sobre el COVID-19. Cuando ya se haya realizado la desidentificación, debería llevarse a cabo también una Evaluación del Impacto sobre la Privacidad (conocida como Data Privacy Impact Assessment, o DPIA por sus siglas en inglés).

El formato requerido por los gobiernos para la información procesada o los Datos Agregados No Identificables varía de país en país, lo que dificulta establecer comparaciones útiles. Los operadores móviles pueden trabajar con Gobiernos u Organismos Internacionales para mejorar su comprensión sobre lo que es posible, reducir la cantidad de información solicitada y cedida, e intentar ajustar sus solicitudes en el futuro, teniendo en cuenta las diferencias en el ámbito regulador y otros factores pertinentes.

Metadatos

- Ceder Metadatos a Gobiernos u Organismos Internacionales solo cuando sea lícito hacerlo, por ejemplo, en muchas jurisdicciones, si es para defender los intereses vitales de las personas, o si se hace sobre la base del consentimiento válido, o porque una ley concreta lo requiere. Dicha ley tendría que ser absolutamente necesaria y proporcionada para alcanzar una finalidad concreta y legítima que sea coherente con estándares de privacidad reconocidos internacionalmente, los derechos humanos y otras leyes pertinentes.

En casos excepcionales, algunos gobiernos u organismos podrían solicitar Metadatos relacionados con una o más personas. Una solicitud legal de este tipo puede hacerse para proteger a personas involucradas, por ejemplo, cuando se trata de identificar a contactos de casos conocidos de COVID-19 o de avisar a las personas cuando hayan entrado o entren en un área afectada.

Las leyes generales de protección de datos, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, normalmente permiten el tratamiento de datos personales si se realiza para proteger los intereses vitales del individuo o cuando se ha otorgado un consentimiento válido. No obstante, su legalidad en un caso particular dependerá de las circunstancias concretas y de la jurisdicción.

Algunas leyes y condiciones de licencias móviles dirigidas a proveedores de datos de comunicaciones electrónicas prohíben el uso de Metadatos para tales fines, a menos que se haya otorgado consentimiento o que esté permitido por una ley promulgada específicamente para proteger la seguridad pública

Garantías de gobiernos u organismos

- Si bien en ningún caso deberían cederse datos salvo cuando sea compatible con la ley, los operadores móviles deben solicitar a los Gobiernos u Organismos Internacionales ciertas garantías:

Uso legítimo y justo

Confirmar que el uso de los Metadatos y Datos Agregados No Identificables es legítimo y justo en relación con las personas involucradas y que se tienen en cuenta todas las circunstancias y posibles efectos. Si la solicitud se basa en una ley específica para la protección de la seguridad pública, deben garantizar que dicha ley es necesaria y proporcionada para alcanzar una finalidad concreta y legítima que sea coherente con estándares de privacidad reconocidos internacionalmente, los derechos humanos y otras leyes pertinentes.

Se insta a los Gobiernos u Organismos Internacionales a solicitar la opinión de la Autoridad de Protección de Datos y/o de la autoridad nacional reguladora de las telecomunicaciones en el país pertinente, y a que comunique esas opiniones a los operadores móviles.

Además, los Gobiernos u Organismos Internacionales deben abordar las limitaciones de responsabilidad pertinentes o indemnizar a operadores móviles por cualquier acción judicial que resulte de haber dado respuesta a las solicitudes y las obligaciones relativas a la retención, cesión e interceptación de las comunicaciones y los datos.

Transparencia

Ofrecer al público general la mayor transparencia posible en relación con el uso de los Datos de Operadores Móviles y el marco jurídico aplicable.

Limitación de los fines

Describir con claridad la finalidad para la cual se están cediendo los Metadatos o los Datos Agregados No Identificables y evitar que se reutilicen para otros fines, en particular para aquellos no relacionados con la prevención de la propagación del COVID-19. En caso de que un Gobiernos u Organismos Internacionales permita a Investigadores acceder a Datos Agregados No Identificables, deberá examinar, supervisar y, si es necesario, impedir que se propongan temas de investigación que no se ajusten a los fines originales.

Prohibición de re-identificación

Imponer una norma estricta que prohíba la re-identificación de Metadatos o de Datos Agregados No Identificables por parte de empleados o Investigadores, salvo cuando lo permita la ley y siempre que se notifique a las personas identificadas.

Seguridad

Contar con medidas tecnológicas y organizacionales adecuadas para proteger la seguridad de todos los Datos de Operadores Móviles, tanto durante la transmisión como cuando no se están tratando. Esto incluye protocolos apropiados de acceso y autorización.

Evaluación de impacto de privacidad de datos (DPIA)

Llevar a cabo una evaluación de impacto de privacidad de los datos con respecto a todos los Metadatos o Datos Agregados No Identificables recibidos.

Evitar la discriminación y respetar los derechos fundamentales

Respetar los derechos de igual protección ante la ley y no utilizar los Datos de Operadores Móviles ni sus insights para discriminar indebidamente a personas o grupos, ni para violar derechos humanos fundamentales.

Investigadores

Someter a examen Auditar a los Investigadores y a sus proyectos a los fines de que los mismos se encuentren alineados con los principios contenidos en estas guías. Esto debe incluir la supervisión sobre quiénes se encuentran autorizados a acceder a estos datos y la obligación de borrar todos los Datos de Operadores Móviles cuando finalice el proyecto.

Retención de los datos

Borrar todos los Datos de Operadores Móviles al finalizar el periodo establecido o cuando ya no sean necesarios para los fines acordados y relacionados con la salud.

Rendición de cuentas

Proporcionar pruebas de que han actuado conforme a las garantías otorgadas. Procurar que una autoridad de supervisión independiente controle el cumplimiento de estos principios.

Los materiales que se enumeran a continuación forman parte de una colección más amplia de iniciativas y recursos de la GSMA sobre privacidad, que se describen detalladamente en los siguientes enlaces:

- GSMA Mobile Privacy and Big Data Analytics
- Informe de la GSMA: Safety, privacy and security across the mobile ecosystem
- Informe de la GSMA: Consumer research insights and considerations for policymakers
- Informe de la GSMA: Mobile Privacy Principles Promoting consumer privacy in the mobile ecosystem
- Informe de la GSMA: Privacy Design Guidelines for Mobile Application Development
- Manual de políticas públicas de comunicaciones móviles de la GSMA

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