C/M/S/
Law.Tax

Protección de datos y COVID-19

Obligaciones y cuestiones a tener en cuenta sobre protección de datos y ciberseguridad cuando se desarrollan apps relacionadas con el COVID-19

CMS España

Abril 2020

Obligaciones y cuestiones a tener en cuenta sobre protección de datos y ciberseguridad cuando se desarrollan apps relacionadas con el COVID-19

Introducción

Las aplicaciones ("apps"), que pueden tener diversas finalidades, y el uso de datos tanto personales como anonimizados en relación con el COVID-19, son actualmente el centro de atención para los desarrolladores de apps. Estas apps, que sin duda conllevan importantes beneficios para la salud pública y la protección de las personas físicas frente al COVID-19, tienen que cumplir con requisitos en materia de protección de datos personales y ciberseguridad.

La primera cuestión que se plantea en el desarrollo de una app es si se van a tratar datos personales, ya que de ser así esta tendrá que cumplir con la normativa sobre protección de datos, que para un desarrollador establecido en España es tanto el Reglamento General de Protección de Datos (RGPD) como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD).

Si se tratan datos personales, el desarrollador de la app debería tener en cuenta las recomendaciones, derivadas del cumplimiento de la normativa ya mencionada, que se indican a continuación.

Responsabilidad proactiva ("*accountability*")

El desarrollador de la app tiene que asegurarse de que adopta las medidas adecuadas para cumplir y ser capaz de demostrar el cumplimiento, incluida la aplicación de políticas de protección de datos cuando resulte oportuno.

Protección de datos desde el diseño y por defecto

Debe aplicarse desde el momento mismo de planteamiento del desarrollo de la app, ya que se trata de adoptar medidas técnicas y organizativas adecuadas para cumplir y demostrar el cumplimiento.

En este sentido pueden ser relevantes la Guía de Privacidad desde el Diseño, publicada por la Agencia Española de Protección de Datos; los aspectos relativos a la intimidad y protección de datos indicados por la Comisión Europea en la Recomendación (UE) 2020/518 de la Comisión, de 8 de abril de 2020, o las recomendaciones sobre privacidad y protección de datos de en aplicaciones móviles de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés).

Analizar el riesgo del tratamiento

Lo que debe partir de conocer qué datos personales se van a tratar y, en su caso, si existe un riesgo alto que requiera llevar a cabo una evaluación de impacto relativa a la protección de datos (EIPD), así como la consulta previa a la autoridad de protección de datos si fuera necesario. Documentar esta EIPD es importante y puede ayudar a ofrecer transparencia sobre el uso de datos por la app.

Minimización de los datos y de los plazos de conservación

En particular, tratar únicamente los datos que sean necesarios y conservarlos durante el tiempo estrictamente necesarios para la finalidad o finalidades correspondientes es clave para cumplir con los principios que legitiman el tratamiento de datos personales, junto con otros principios de protección de datos y la base de legitimación aplicable.

Ingeniería de privacidad ("*privacy engineering*")

Se trata de un proceso sistemático que tiene por objeto que la protección de datos se aplique a lo largo del ciclo de vida de la app utilizada para tratar datos personales.

Almacenamiento de datos en el dispositivo móvil

De manera que se pueda controlar mejor el acceso a los datos, restringiendo dicho acceso a la app, así como facilitando la posibilidad de que los datos sean anonimizados.

Ciberseguridad

La seguridad desde el diseño es también necesaria para asegurar el derecho fundamental a la protección de datos, ya que, a lo largo del tratamiento de los datos personales, se trata de evitar accesos no autorizados (confidencialidad), modificaciones no autorizadas (integridad) o la supresión

accidental o ilícita (disponibilidad). Y también aplicando otras medidas, tales como la pseudonimización, para evitar riesgos para los interesados si un tercero no autorizado tuviera acceso a los datos.

Anonimización

Si se tratan datos personales o se usan datos anonimizados, el desarrollador de la app debe considerar las técnicas de pseudonimización y anonimización disponibles, en particular por lo que se refiere a la evolución tecnológica y a la necesidad de aplicar técnicas que sean robustas para evitar la re-identificación de las personas físicas.

El desarrollo de apps para combatir el COVID-19 es una necesidad y esta actividad, cuando implique o pueda implicar un tratamiento de datos personales, tiene que hacerse respetando el derecho fundamental a la protección de datos personales, así como otros derechos fundamentales, tales como el derecho a la intimidad en el uso de apps. En relación con esta cuestión, el Comité Europeo de Protección de Datos publicó el 14 de abril de 2020 una carta dirigida a la Comisión Europea en la que, por lo que se refería al entonces borrador de Comunicación sobre las orientaciones sobre apps móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos, ya indicaba que estas debían desarrollarse de manera responsable (*accountable*), a partir de los principios de protección de datos desde el diseño y por defecto y de documentar una evaluación de impacto relativa a la protección de datos.

Por lo que se refiere a la utilización de datos de movilidad, las apps, cuando cumplan con garantías adecuadas, podrían proporcionar información relevante para comprender la evolución y propagación del COVID-19. Esto no quiere decir que tengan que tratarse datos personales o que se geolocalice a la persona, debiendo considerar que su función es descubrir eventos, tales como casos de positivos en COVID-19, de manera que el tratamiento de datos personales podría vulnerar derechos fundamentales.

Y así lo contempla la Comisión Europea, en la Comunicación ya indicada que fue publicada el 17 de abril de 2020. Esta Comunicación constituye en buena medida una guía dirigida a los desarrolladores de apps a efectos de cumplir con la normativa europea sobre protección de datos personales.

En definitiva, quien desarrolle una app debe asegurarse de cumplir con los requisitos aplicables tanto en materia de protección de datos como de ciberseguridad, asesorándose previamente en lo que fuera oportuno, para evitar vulneraciones de derechos fundamentales. Además, considerar los requisitos legales y regulatorios aplicables ayudará a cualquier app a generar confianza entre sus usuarios.

Para más información, puede contactar con el equipo de TMC de CMS Albiñana & Suárez de Lezo: Javier Torre de Silva, socio; Miguel Recio, asociado.

La presente publicación no constituye asesoramiento jurídico de sus autores.

cms-asl@cms-asl.com | **cms.law**