consejo para la Transparencia

OFICIO N° 000675

MAT: Comunica información relativa al debido cumplimiento de las disposiciones comprendidas en la Ley N°19.628, sobre Protección de la Vida Privada, en las operaciones de tratamiento de datos personales y datos sensibles que tienen lugar en el marco de la aplicación "CoronApp".

ANT: No hay.

Santiago, 07 MAY 2020

A: **SR. FELIPE WARD EDWARDS**
MINISTRO SECRETARIO GENERAL DE LA PRESIDENCIA

SR. JAIME MAÑALICH MUXI
MINISTRO DE SALUD

DE: **ANDREA RUIZ ROSAS**
DIRECTORA GENERAL
CONSEJO PARA LA TRANSPARENCIA

1. El Consejo de la Transparencia ha tomado conocimiento del desarrollo por parte del Ministerio de Salud (en adelante, indistintamente, "MINSAL"), en el contexto de la emergencia sanitaria generada por la propagación en la población del brote de COVID-19 y con apoyo del Ministerio Secretaría General de la Presidencia (en adelante, indistintamente, "SEGPRES"), de la aplicación para dispositivos móviles "CoronApp". Esta herramienta ha sido puesta a disposición del público general, para ser descargada en dispositivos iOS y Android, a través de un enlace contenido en el sitio web https://coronapp.gob.cl/ y en las tiendas de aplicaciones de ambas plataformas.
2. Según se informa en la página de inicio del referido sitio web, la aplicación tendría los siguientes objetivos: (i) permitir a los usuarios reportar y controlar sus síntomas relacionados con el COVID-19, así como también, monitorear los síntomas de hasta 8 personas ("familiares, convivientes u otros que no puedan usar la aplicación"); (ii) obtener información oficial sobre la pandemia, recibiendo notificaciones del Gobierno e información a través del WhatsApp informativo del MINSAL; (iii)

indicar el lugar donde una persona residirá durante la cuarentena; y, (iv) colaborar con la prevención de contagios, informando sobre situaciones que ponen en riesgo a más personas.

3. En este sentido, **la aplicación CoronApp requiere, para la ejecución de sus funcionalidades, la recopilación, almacenamiento y procesamiento de una gran cantidad de datos personales, en especial, datos de carácter sensible, tanto de sus usuarios enrolados como de terceros.** A este respecto, suscita especial preocupación el adecuado tratamiento de los datos suministrados por los usuarios o que sean recabados a partir de su actividad o interacción con esta herramienta digital, el que debe ajustarse en todo momento a los principios, derechos y deberes contemplados en nuestra normativa sobre protección de datos personales.

4. En consecuencia, el Consejo Directivo de esta Corporación, en virtud de la facultad establecida en la letra m) del artículo 33 de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285, en sesión ordinaria N°1091, de fecha 23 de abril de 2020, acordó remitir a usted el presente Oficio, mediante el cual se formulan algunas prevenciones tendientes a garantizar que las operaciones de tratamiento de datos asociadas al funcionamiento de la aplicación CoronApp cumplan estrictamente con lo dispuesto en el artículo 19 N°4 de la Constitución Política de la República y las normas pertinentes de la Ley N°19.628, sobre Protección de la Vida Privada (LPVP), y sus modificaciones posteriores.

5. Esta Corporación, remite la presente comunicación en el mejor ánimo de colaborar con los órganos de la Administración del Estado responsables de la debida gestión y administración de las bases de datos personales y sensibles, que se generen con ocasión de la aplicación Coronapp, y con el exclusivo objeto de dar a conocer los mecanismos de resguardo que resulta adecuado implementar para dar cumplimiento a la Ley N°19.628, sobre Protección de la Vida Privada.

6. Las observaciones que se presentan a continuación se basan en las declaraciones contenidas en las Políticas de Privacidad de CoronApp, disponibles en el enlace web https://coronapp.gob.cl/politicas.html, así como también, en lo señalado en los Términos y Condiciones aplicables al acceso y uso de dicha aplicación, disponibles en https://coronapp.gob.cl/terminos.html.

7. En este sentido, a juicio de este Consejo, las operaciones de tratamiento de datos personales que tienen lugar en el marco de la aplicación CoronApp debiesen considerar, al menos, los siguientes elementos:

a) **Necesidad y proporcionalidad de las actividades de tratamiento de datos, en vista al cumplimiento de las finalidades declaradas por la aplicación.**

   i. La Política de Privacidad da cuenta que **CoronApp recopila**, además de información de carácter personal no comprendida dentro de alguna de las categorías especiales de datos (tales como el RUN o pasaporte del usuario,

correo electrónico, número telefónico, nombre y apellido, edad, comuna y ciudad de residencia), **datos sensibles de salud** (esto es, los medicamentos que toma o han sido prescritos al usuario, preexistencia de enfermedades y datos de seguimiento de la enfermedad, tales como síntomas, contacto con personas contagiadas confirmadas) y **datos sensibles relativos a hábitos personales**, concretamente, la geolocalización del usuario.

ii. En vista a que las operaciones de tratamiento de datos sensibles involucran un mayor riesgo de lesionar los derechos fundamentales de su titular, especialmente la protección de su vida privada, su intimidad y el derecho a no ser objeto de discriminaciones arbitrarias, se recomienda siempre ponderar la necesidad de tratar categorías de datos que requieren altos niveles de resguardo.

iii. Por consiguiente, corresponde **evaluar si la recopilación de cada uno de los datos solicitados puede resultar excesiva y desproporcionada de cara al cumplimiento de los fines lícitos que justificarían su procesamiento.**

iv. Asimismo, debiese **explicitarse en las mismas políticas los fines u objetivos específicos y precisos que se persigue con el tratamiento de cada uno de los datos personales obtenidos, evitando el empleo de fórmulas abiertas e indeterminadas que impidan alcanzar niveles apropiados de transparencia en el manejo de los datos.**

b) <u>Identificación del responsable del tratamiento.</u>

i. **La Política de Privacidad afirma que la aplicación CoronApp ha sido desarrollada por MINSAL,** refiriéndose expresamente al hecho que dicho ministerio y sus organismos relacionados se encuentran facultados por ley para requerir, recolectar, ceder o procesar información de salud, junto con los deberes de confidencialidad asociados a dichas atribuciones. Por su parte, los Términos y Condiciones señalan, adicionalmente, que "*[e]l registro de la cuenta de usuario requiere que comunique a la Subsecretaría de Redes Asistenciales determinados datos personales que se indican en nuestras Políticas de Privacidad.*".

ii. Al respecto, **se debe individualizar con claridad en la Política de Privacidad, en un apartado especial, el organismo público que reviste la calidad de responsable del tratamiento de los datos recopilados a través de la aplicación CoronApp**, indicando además un punto de contacto específico para estos efectos. Esta circunstancia tiene particular relevancia en lo que respecta al ejercicio expedito por parte de los titulares de datos de los derechos reconocidos por la LPVP.

iii. Por otra parte, según señala el propio sitio web <u>https://coronapp.gob.cl/</u>, así como también la información técnica publicada en la Apple Store y Google Play, la aplicación fue desarrollada por la División de Gobierno Digital de SEGPRES.

iv. En vista a ello, **se debe especificar el rol de dicho organismo en el funcionamiento de la aplicación y, eventualmente, en el procesamiento de los datos recabados a partir de la misma, por ejemplo, en calidad de mandatario o encargado del tratamiento, en virtud a lo dispuesto en el artículo 8° de la LPVP.**

v. Finalmente, en este marco, en cuanto a la posibilidad que los datos recabados puedan utilizarse para fines científicos e investigaciones, en los términos señalados en el numeral 8 de la política, se recomienda especificar si dichos tratamientos de datos serán efectuados por terceros, públicos o privados, en calidad de encargados del tratamiento.

c) **Base de licitud para el tratamiento de los datos.**

i. En lo que respecta a las condiciones de licitud para recabar datos personales sensibles, conforme dispone el artículo 10 de la LPVP, existe una prohibición general de tratamiento de esta categoría de datos, salvo cuando una disposición legal lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

ii. Sobre la base de lo anterior, **la Política de Privacidad debe indicar con claridad la fuente habilitante para el tratamiento de los datos recopilados a partir de la aplicación CoronApp.**

iii. En esta materia, el texto de la Política de Privacidad hace referencia, indistintamente, tanto a la existencia de una autorización legal que permitiría los referidos tratamientos, como al eventual otorgamiento del consentimiento de los titulares de datos. La identificación explícita del título habilitante es importante para determinar con precisión el estatuto aplicable a dichas operaciones, por ejemplo, en lo que respecta al ejercicio de los denominados derechos ARCO.

iv. Así, mientras el encabezado de la Política de Privacidad señala que el Ministerio de Salud y sus organismos relacionados *"se encuentran facultados por ley para requerir, recolectar, ceder o procesar información de salud, conforme a las competencias explícitas e implícitas que les han sido conferidas"*, en el numeral 4, sobre responsabilidad del MINSAL, se señala que el consentimiento expreso de su titular *"ha sido entregado de manera libre expresa y por escrito por el usuario de la aplicación"*.

Adicionalmente, respecto al tratamiento de los datos de geolocalización, se señala en el numeral 6 que *"su acceso se basa en el consentimiento entregado en la descarga de la aplicación"*. Por lo demás, la propia Política de Privacidad señala que la descarga de la aplicación es "voluntaria", por personas mayores de 18 años.

v. En vista a lo anterior, es recomendable **establecer expresamente en las referidas políticas que el tratamiento de datos, si bien se inserta en el ámbito competencial del MINSAL (artículo 20 de la LPVD en coherencia con lo dispuesto en ley orgánica del Ministerio de Salud), encuentra su fundamento en la autorización expresa otorgada por el titular de los mismos.**

Lo anterior, teniendo presente el hecho que la aplicación debe ser descargada voluntariamente por el usuario a través de las plataformas Google Play o Apple Store, la categoría especial de datos que son recopilados por CoronApp y las finalidades de su procesamiento, es posible estimar que la concurrencia del consentimiento autónomo e informado del titular de datos permite tutelar de mejor forma en este caso la autodeterminación informativa de los individuos.

vi. **Un tratamiento de datos basado en el consentimiento de sus titulares implica, entre otros aspectos, permitir a éstos la posibilidad que puedan revocar su consentimiento, en los términos señalados en el artículo 4°, inciso 4, de la LPVP, así como también, garantizarles el ejercicio de los derechos de acceso, rectificación, cancelación y bloqueo, de conformidad a las reglas contenidas en los artículos 12 y siguientes del mismo cuerpo legal.**

d) Ejercicio de los derechos ARCO.

i. En primer término, es fundamental que se especifique claramente el estatuto de derechos que los usuarios de la aplicación en cuestión podrán ejercer. En especial, adoptando los resguardos que se describen a continuación:

ii. La aplicación deberá permitir siempre el acceso a los datos entregados para dichos efectos, la modificación o rectificación cuando éstos sean inexactos o erróneos y así se acredite.

iii. Además, deberá contemplar la posibilidad de cancelar los datos, toda vez que éstos han sido entregados voluntariamente por sus titulares.

iv. Finalmente, resulta importante que **la misma aplicación disponga de herramientas que facilite a los usuarios titulares de datos el ejercicio expedito de sus derechos, junto con disponer para estos efectos de canales especiales de información o consulta.**

e) Tratamiento de datos de "usuarios dependientes".

i. La Política de Privacidad señala, en su numeral 2, que *"[l]os usuarios podrán agregar otros usuarios dependientes, familiares o personas que no tengan acceso a un dispositivo móvil propio. Estos usuarios dependen de la cuenta del usuario principal registrado en la aplicación. El usuario registrado en la aplicación es responsable de la veracidad, actualización, precisión y completitud de los datos de terceros que ingresa."*.

Entre los datos que pueden comunicarse en relación con los usuarios dependientes, se incluyen datos sensibles, como el estado de salud y las afecciones médicas.

ii. A este respecto, cabe advertir que **la referida política no específica la base de licitud en virtud del cual se obtienen datos de personas distintas del usuario principal, esto es, información que concierne a terceros.**

iii. De ahí que, salvo en lo relativo a los datos de personas respecto de las cuales el usuario principal tiene la calidad de representante legal, se plantean reparos al tratamiento de esta categoría de datos, desde el punto de vista de la autodeterminación informativa, puesto que se advierte que no concurre efectivamente el consentimiento del tercero que es titular de los datos en cuestión, además de la dificultad de asegurar la exactitud y veracidad de dicha información.

iv. A consecuencia de lo anterior, cabe señalar que no se advierte cómo los **usuarios dependientes, quienes no tienen una relación directa con la aplicación, podrán ejercer efectivamente ante el responsable del tratamiento los derechos reconocidos por la LPVP.**

v. Estas circunstancias deben ser revisadas y perfeccionadas, con el objeto de garantizar la debida protección de los datos personales y sensibles de todas las personas.

f) Almacenamiento de los datos.

i. El numeral 5 de la Política de Privacidad señala que *"[p]ara fines históricos, estadísticos, científicos y de estudios o investigaciones, se podrán almacenar y utilizar los datos por un período de 15 años, con las debidas medidas de seguridad y garantías de anonimización."*.

Sin embargo, luego, el numeral 8 de las referidas políticas, sobre uso de la información para fines científicos e investigaciones, informa la aplicación de medidas de anonimización de los datos recabados, sólo al momento de publicar los resultados y análisis obtenidos de los estudios científicos.

ii. Sobre el particular, si bien los procesos de anonimización o disociación constituyen medidas de seguridad robustas, por cuanto impiden que un dato sea asociado a una persona determinada o determinable, el hecho de requerir su aplicación únicamente en la etapa de publicación de resultados implica que estas medidas de seguridad, en definitiva, tendrán un alcance restringido.

iii. Por consiguiente, debe **evaluarse la necesidad de establecer períodos extensos de conservación de los datos, teniendo especialmente presentes los riesgos que trae aparejado el procesamiento de datos sensibles, así como las finalidades extraordinarias que motivaron su recopilación y comunicación**

voluntaria por parte de sus propios titulares de la información, esto es, hacer frente a la emergencia sanitaria consecuencia del brote de COVID-19.

iv. Además, deberán establecerse mecanismos efectivos de seudonimización o anonimización, según corresponda, que aseguren la irreversibilidad de dichos procedimientos, impidiendo con ello que se pueda identificar a los titulares de los mismos.

v. Respecto a los datos de geolocalización, si bien el numeral 6 de la Política de Privacidad señala que este dato *"será utilizado exclusivamente y con el único fin de realizar acciones útiles de seguimiento de pacientes para la protección de la salud pública, durante la vigencia de la emergencia sanitaria"*, **dicha declaración debiese ser explícita y clara en cuanto a establecer que estos datos no serán tratados para fines científicos e investigaciones, estando, por consiguiente, exceptuados de las reglas especiales de almacenamiento informadas en el numeral 5 de la política.**

vi. Por otra parte, se **deben tener presente los riesgos de seguridad que pueden derivarse del hecho que los datos recabados y procesados por CoronApp no sean almacenados en servidores locales propios de MINSAL, sino que en servidores externos, localizados fuera del territorio nacional, lo que requiere operaciones de transferencia internacional de datos personales.**

Según se afirma en el numeral 5 de la política, la información registrada en la aplicación será *"almacenada y replicada en una nube privada bajo la completa administración del MINSAL, en Amazon Web Services (AWS) correspondiente a la región 'us-east region' el cual se encuentra físicamente en Estados Unidos de América en el estado de Virginia"*.

vii. Teniendo presente que, en este caso, los datos objeto de tratamiento abarcan información sensible de diversa índole, es necesario la implementación de una serie de medidas destinadas a garantizar el debido resguardo de los datos objeto del tratamiento por la aplicación en cuestión.

Entre otros, se sugiere **la existencia de un contrato con el encargado del tratamiento situado en el extranjero, que contenga cláusulas estrictas de reserva, asegurando en todo momento el cumplimiento de las normas y obligaciones contempladas en la ley chilena.**

Dichas disposiciones debiesen, a lo menos, especificar: **(i)** las instrucciones del responsable y limitación del tratamiento del encargado (esto es, que el mandatario no podrá aplicar los datos a otra finalidad); **(ii)** el detalle de las medidas de seguridad exigidas, sobre la base de los especiales riesgos asociados al tratamiento de datos sensibles; **(iii)** el cumplimiento de deberes reforzados de confidencialidad; **(iv)** la prohibición de retransmitir los datos a un tercero; y **(v)** el deber del encargado de devolverlos al responsable, al terminar la relación contractual, eliminando toda copia de los mismos.

g) **Seguridad de la información.**

i. En esta materia, la Política de Privacidad se limita a redirigir al enlace web https://www.minsal.cl/seguridad_de_la_informacion/, donde se informa sobre un sistema de seguridad de carácter general, aplicable al "conjunto de activos de información institucional".

Por su parte, los Términos y Condiciones, establecen que "*[l]a Subsecretaría de Redes Asistenciales declara que ha tomado las medidas técnicas necesarias para velar por la confidencialidad y por la protección de los datos personales ingresados por el Usuario en la aplicación o los registrados por ella.*".

ii. Sin embargo, no se informan las medidas de seguridad particulares y específicas aplicables a la aplicación CoronApp, que garanticen la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros, con la finalidad de evitar la alteración, pérdida y acceso no autorizado de los mismos.

iii. Sobre el particular, **es de fundamental importancia la comunicación de información específica y relevante sobre las condiciones de seguridad técnicas y organizativas propias de CoronApp, teniendo especialmente presente la especial entidad de los datos personales que son objeto de tratamiento, así como la constante interacción de esta aplicación con dispositivos externos a la institución (equipos de telefonía móvil donde CoronApp ha sido descargada), lo que implica mayores riesgos de seguridad informática.**

iv. Por otra parte, incide en estos riesgos el uso de infraestructura o servidores externos al MINSAL para el almacenamiento de los datos recabados y procesados por la aplicación, más aún si estos se encuentran localizados fuera del ámbito territorial donde resulta aplicable la normativa chilena de tratamiento de datos.

v. Para estos efectos, se sugiere tener presente las recomendaciones sobre medidas de seguridad en las operaciones de tratamiento de datos sensibles remitidas a los órganos de la Administración del Estado, por este Consejo para la Transparencia, mediante Oficio N°501, de 21 de abril de 2020.

h) **Denuncia de conductas o eventos de alto riesgo.**

i. Dentro de las opciones que brinda CoronApp, destaca el hecho que permite a los usuarios notificar o informar ciertos eventos, tales como eventuales incumplimientos de cuarentenas.

ii. En este punto, **debemos advertir el riesgo que la aplicación opere como un sistema de denuncias que promueva -indirectamente- entre los usuarios, conductas tendientes a recabar información reservada de terceras personas, pudiendo afectar el derecho de éstas a la privacidad y la intimidad, junto con**

aumentar el riesgo de estigmatización social y discriminación por COVID-19.

iii. De ahí que deberá asegurarse que las herramientas facilitadas a la ciudadanía mediante la aplicación se transformen en un mecanismo de denuncia entre los ciudadanos, y se resguarden los derechos recién mencionados.

i) **Inscripción de bases de datos.**

i. Teniendo presente que los órganos o servicios deberán inscribir los bancos de datos personales que administren en el registro que para estos efectos lleva el Servicio de Registro Civil e Identificación, de conformidad con lo dispuesto en el artículo 22 de la LPVP, **el responsable de la base de datos que se genere con ocasión de la aplicación CoronApp deberá proceder en dicho sentido.**

ii. Adicionalmente, **la Política de Privacidad deberá dar cuenta de la circunstancia de haberse efectuado dicha inscripción.**

8. Por último, este Consejo reitera su voluntad de colaborar, en el marco de sus competencias legales, en los esfuerzos estatales desplegados para hacer frente a esta pandemia mundial que nos afecta y, en particular, para el adecuado tratamiento de los datos personales que supone su control y gestión.

Sin otro particular, saluda atentamente a usted,

REPÚBLICA DE CHILE ★ CONSEJO PARA LA TRANSPARENCIA ★ Directora General

ANDREA RUIZ ROSAS
DIRECTORA GENERAL
Consejo para la Transparencia

DISTRIBUCIÓN:
1. Sr. Felipe Ward Edwards, Ministro Secretario General de la Presidencia.
2. Sr. Jaime Mañalich Muxi, Ministro de Salud.
3. Sr. Arturo Zúñiga Jory, Subsecretario de Redes Asistenciales.
4. Archivo.