GUÍA DE ORIENTACIÓN JURÍDICA POR AFECTACIONES DERIVADAS DEL COVID-19

CAPÍTULO 07

Protección de Datos Personales y Comercio Electrónico

#GuíaJurídicaCOVID19mx

MÉXICO 2020

La enfermedad infecciosa identificada como COVID-19 que estalló el pasado mes de diciembre de 2019 en Wuhan (China) y que posteriormente se propagó a nivel mundial, ha obligado a los países y organizaciones internacionales a tomar las precauciones adecuadas para evitar su contagio. El presente escrito tiene como finalidad establecer claridad respecto a las cuestiones relacionadas con la protección de datos personales y en particular los datos personales sensibles frente a organismos públicos y privados que pudieran tratar estos datos durante la pandemia del COVID-19, y algunas consideraciones de comercio electrónico. Previendo que muchas de las operaciones que tradicionalmente se hacían en físico, ahora serán a través de medios electrónicos.

Sector Salud

¿Que tipo de datos trata el sector salud?

Los hospitales y centros de atención médica tratan datos personales con la finalidad de identificar a una persona y poder registrarla en su sistema, sin embargo, estas instituciones tratan en su mayoría datos personales sensibles, los cuales son aquellos datos que afecten a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En este sentido, es muy importante que tanto los hospitales como cualquier organización que recabe datos personales sensibles realice el tratamiento con apego a los principios de protección de datos personales, los cuales establecen el eje rector sobre el cual los responsables deberán tutelar los datos personales bajo su protección.

¿Qué son los datos personales sensibles?

Dividiremos en dos rubros la respuesta:

En términos de lo señalado por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.- Son los que requieren una especial protección en virtud de su naturaleza y de las consecuencias que puede tener el mal manejo de éstos en su titular. La fracción X del artículo 3 de la LGPDPSSO los define como: aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como:

a) Origen racial o étnico;
b) Estado de salud presente o futuro;
c) Información genética;
d) Creencias religiosas, filosóficas y morales;
e) Opiniones políticas, y
f) Preferencia sexual.

Ahora bien, lo que refiere la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en su Artículo 3, fracción VI, los Datos Personales Sensibles son: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

¿Que datos personales pueden recabar estos organismos?

Para determinar los datos personales que podrían recabar los organismos públicos y privados durante esta pandemia, debemos precisar que, con base en el principio de proporcionalidad, previsto en el artículo 13 de la Ley, los datos que recaben deberán ser los necesarios, adecuados y relevantes en relación con las finalidades previstas en su Aviso de Privacidad.

En este sentido, solo podrán ser objeto del tratamiento por parte del responsable aquellos datos que resulten necesarios para efecto de determinar las medidas necesarias en caso de que una persona tenga síntomas del virus o sea positivo. Entre los datos que son relevantes podemos mencionar los siguientes: presencia de síntomas de COVID-19, saber si la persona tiene la enfermedad infecciosa, saber si la persona viajó recientemente a un país en donde haya un alto número de casos de infectados de COVID-19 o en su defecto, si alguna persona físicamente cercana a él ha realizado un viaje con esas características.

¿Qué tipo de datos me deben solicitar en una institución de salud (pública o privada) con relación a COVID-19?

Únicamente aquellos que sean adecuados, relevantes y estrictamente necesarios para cumplir con la finalidad del tratamiento, es decir, detectar si padeces del virus, entre ellos se pueden mencionar: saber si has viajado recientemente, ya sea dentro o fuera del país, si padeces algunos de los síntomas de COVID-19, así como alguna de las condiciones preexistentes que hacen más riesgosa la presencia del virus o si has tenido contacto con alguna persona que esté en alguna de estas situaciones, entre otras.

Además, es necesario que la institución haga todos sus esfuerzos para limitar el período del tiempo del tratamiento para que sea el menor posible.

Esto de conformidad con los artículos 25 y 13 de la LGPDPPSO y de la LFPDPPP, respectivamente.

¿Pueden hacer públicos mis datos en caso de ser positivo al COVID-19?

Es muy importante para el titular de los datos personales leer el Aviso de Privacidad de la persona o institución a la cual dará sus datos personales ya que este es el documento en donde el responsable da a conocer que datos recaba, para que finalidades y si realiza transferencia de sus datos personales a un tercero.

Ahora bien, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, establece no se requerirá el consentimiento del titular para realizar una transferencia de datos personales cuando sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios. Asimismo, tampoco se requerirá el consentimiento del titular cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.

En este sentido, se puede afirmar que los hospitales sí pueden transferir la información ya que está previsto en La Ley y se entiende que la finalidad es para salvaguardar un interés público, que en el presente caso es dar a cono-

cer a la sociedad el número de casos confirmados por cada entidad estatal del país. Las medidas de seguridad para la protección de los datos personales sensibles y el respeto a los principios rectores de protección son sumamente importantes.

En caso de ser positivo de COVID-19, ¿la institución de salud (pública o privada) puede usar mis datos personales sin mi consentimiento?

En principio no, por ser datos personales sensibles requiere de tu consentimiento expreso y por escrito, sin embargo, hay excepciones a este principio establecidas en el artículo 22 de la LGPDPPSO y en el artículo 10 de la LFPDPPP, en donde se dice que no se requerirá de tu consentimiento cuando el tratamiento de los datos sea indispensable para atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras no estés en condiciones de otorgar el consentimiento o cuando exista una situación de emergencia que potencialmente pueda dañarte en tu persona.

En caso de ser positivo de COVID-19, ¿a quién le debo compartir yo esta información?

Recuerda que tú eres el dueño de tus datos personales, así que tú eres quien decide a quien le compartes esta información (sin tomar en cuenta a la institución de salud que te realice la prueba y te diagnostique), sin embargo, esta es información que involucra a todas las personas con las que has tenido contacto y/o frecuentas con regularidad, por eso es importante que se los hagas saber a ellos, con el propósito de que puedan tomar las medidas necesarias para cuidar de su salud.

Es importante hacer mención que, en caso de ser positivo de COVID-19, si lo compartes por tu propia cuenta en fuentes de acceso público, por ejemplo, en redes sociales, no se necesitará de tu consentimiento para tratar tus datos personales, pues estás decidiendo compartirlos y únicamente tú serás el responsable del tratamiento que se le dé a esta información y las consecuencias que pueda tener.

¿Qué son las fuentes de acceso público?

La LFPDPPPP en su artículo 3 fracción X las define como aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación.

¿Puedo saber en qué forma y para qué usarán mis datos personales las instituciones de salud (pública o privada)?

Sí, la institución de salud (pública o privada) debe informarte a través de su aviso de privacidad, la forma, la finalidad, las características principales y que datos personales recaba, de conformidad con el artículo 26 de la LGPDPPSO y del 15 de la LFPDPPP.

¿A qué tipos de riesgos se pueden enfrentar mis datos personales en vista de COVID-19?

Las personas frente a la pandemia estamos en la constante necesidad

de buscar información cierta, actual e inmediata, sobre las medidas y técnicas adoptadas por las autoridades en relación con COVID-19, así como información veraz sobre el mismo, esto genera una oportunidad para los ciberdelincuentes de realizar acciones para tratar de robarse los datos personales de los ciudadanos, vulnerando los mismos.

ESET, una compañía de seguridad informática, el pasado 16 de marzo, compartió un artículo llamado "Engaños que explotan el miedo por el Coronavirus" en donde enumeran las tácticas que han estado usando los cibercriminales, a continuación, se mencionan algunas de éstas:

a) A través de correos electrónicos spam, se incluyen comunicados engañosos en los que suplantan páginas oficiales para distribuir sitios web infectados haciendo uso de títulos llamativos.

b) Se envían correos de spam en búsqueda de que los ciudadanos crean que pueden ordenar máscaras de protección respiratoria para mantenerse a salvo del COVID-19, cuando en realidad lo que se está haciendo es revelar información sensible, personal y financiera.

c) Como la Organización Mundial de la Salud -OMS, es la principal fuente de información sobre el brote de Coronavirus, se encuentra entre las autoridades cuya identidad se ha visto más suplantada en las últimas campañas de engaños. La forma de operar de los atacantes ha sido ofrecer información relevante acerca del virus, en un intento por lograr que potenciales víctimas hagan clic en los enlaces maliciosos. Comúnmente, dichos enlaces pueden instalar malware, robar información personal, o intentar obtener credenciales de ingreso y contraseñas.

Estos son algunos ejemplos de las vulneraciones a las que los ciudadanos están expuestos.

¿Qué puedo hacer para proteger mis datos personales y no caer en este tipo de prácticas?

Es importante estar muy alerta y ser extremadamente cuidadoso al momento de buscar cualquier tipo de información relacionada con la pandemia, así como con la que tú difundes. También es importante no caer en pánico, pues, lo que los criminales están haciendo es aprovecharse de la incertidumbre y del miedo de los ciudadanos.

El INAI (Instituto Nacional de Acceso a la Información y Protección de Datos Personales) ha emitido las siguientes recomendaciones:

- Evitar hacer clic en cualquiera de los enlaces adjuntos o descargar archivos anexos a correos no solicitados o textos de fuentes no reconocidas, o incluso de fuentes confiables a no ser que esté absolutamente seguro de que dicho mensaje sea auténtico;

- Ignorar las comunicaciones que le solicitan su información personal. De ser necesario, verifique los contenidos del mensaje con el emisor o la organización que dicen represen-

tar, y hágalo a través de otro medio que no sea el mensaje recibido;

- Mantenerse especialmente atento a los correos que añaden un sentido de alerta y lo urgen a tomar una acción inmediata u ofrecen vacunas o curas contra el COVID-19;
- Estar atento ante donaciones fraudulentas o campañas de financiación compartida de proyectos;
- Utilizar software de seguridad en múltiples capas que incluya protección contra el phishing;
- Introducir el nombre de usuario y contraseña solo cuando la conexión sea segura;
- Lo mismo ocurre en correos de organizaciones oficiales, como bancos, agencias de impuestos, tiendas online, agencias de viajes, aerolíneas, etc. Incluso de su propia oficina.
- Es muy importante tomarse el tiempo necesario para leer los términos y condiciones de todas las aplicaciones que se descarguen.

Home office

¿Que pasa si estoy tratando datos personales mientras hago home office?

Durante la pandemia COVID-19, una de las medidas más importantes para evitar la propagación del virus es el distanciamiento social, por consiguiente, muchas empresas a nivel nacional se encuentran trabajando desde casa. En este sentido, es muy importante para todas las personas que tienen acceso o manipulan información sensible o confidencial desde sus casas que mantengan toda información personal y sensible en áreas restringidas y cumplir con los controles de privacidad básicos.

Por consiguiente, es fundamental resguardar las computadoras portátiles, tabletas y cualquier dispositivo que cuente con acceso a información sensible o confidencial con controles de seguridad como contraseña para acceder a estos dispositivos y un respaldo digital para evitar cualquier pérdida de información personal.

Es importante tener en cuenta que los datos personales y/o los datos personales sensibles que sean recabados durante el trabajo en casa, no deberán ser almacenados en un sistema que no sea los de la empresa, lo anterior con la finalidad de cumplir con el principio de responsabilidad el cual establece que el responsable deberá velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión.

Educación

¿Que implicaciones hay en materia de protección de datos y la educación?

En estos momentos, la educación en todos los niveles ha sido suspendida o se ha migrado a modalidad en línea, la mayoría de las universidades han optado por continuar con los cursos mediante videoconferencias con los alumnos. Ante este panorama, los datos personales de todos los alumnos deberán ser tratados y resguardados utilizando

medidas de seguridad administrativas, físicas y técnicas para evitar su alteración, pérdida o acceso no autorizado.

Asimismo, es importante definir las herramientas electrónicas que se deberán usar para la comunicación digital con los alumnos y el personal docente, procurando en todo momento que los datos personales que sean recabados por estos medios sean únicamente los necesarios para la finalidad de continuar con los cursos impartidos por las escuelas o universidades.

Algunas recomendaciones para las instituciones académicas que realicen la educación continua mediante clases virtuales sería apegarse estrictamente a las necesidades básicas para el desarrollo de la clase sin comprometer datos adicionales por parte de los alumnos, por ejemplo, realizar la clase utilizando los micrófonos de las plataformas más no el video si éste no es necesario. Es importante también verificar la configuración, Aviso de Privacidad y políticas de privacidad de las plataformas que se utilicen para dar las clases virtuales protejan los datos personales de los alumnos y profesores y no realicen transferencias a terceros que comprometan esta información personal.

Comercio electrónico

¿Se considera comercio electrónico vender mis productos u ofrecer mis servicios a través de plataformas electrónicas, aún cuando sean cuentas privadas?

Sí. Cuando se ofrecen productos o servicios de forma habitual al público, se considera comercio, y cuando se ofrezcan, comercialicen o venden bienes, productos o servicios, mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, se considera que es electrónico.

¿Qué condiciones tengo que cumplir para entregar los productos y/o prestar los servicios?

Tanto el Código de Comercio, como diversas leyes establecen los requisitos legales indispensables para realizar actos de comercio. Al menos, debe dejarse claro 1) el servicio o producto que se va a ofrecer, de forma veraz, sin engaños (para que sirve, qué funciones tiene, cómo opera) 2) las condiciones en que se realizará la operación (cuándo se entrega, cómo se entrega, quién paga los gastos si hay envío, si hay responsabilidad de entrega, etc.), 3) precio e impuestos generados y forma de pagarse, 4) condiciones para devolución y 5) mecanismos para hacer efectiva la garantía.

Aunque sea un pequeño negocio, ¿me aplican disposiciones de comercio electrónico?

Si, cualquier persona, física o moral, de cualquier tamaño debe cumplir con las disposiciones legales, dando seguridad jurídica a sus consumidores.

¿Cuáles son las recomendaciones básicas de seguridad para operaciones en línea?

Preferentemente utilizar pagos en línea a través de plataformas como PayPal, MoneyPool, etc. ya que éstas no revelan información del proveedor. Si no se utilizan éstas, es importante no reve-

lar información de tarjetas (no enviar fotografía por ambos lados, evitando compartir el número de seguridad), ni proporcionar información personal. Confirmar la recepción de transferencia de dinero, previo a entregar la mercancía o el servicio.

¿Tiene alguna consecuencia que ofrezca mis bienes y productos con fotografías que no sean reales?

Sí. La información y publicidad que se proporcione debe ser veraz, comprobable, clara y exenta de textos, diálogos, sonidos, imágenes o alguna otra figura que induzcan o puedan inducir a error o confusión al Usuario y Consumidor por ser engañosas o abusivas, de conformidad con las disposiciones jurídicas aplicables. Además, el uso de fotografías sin autorización de quién tiene derechos de autor sobre ellas, puede generar una sanción pecuniaria considerable.

¿Debo tener un aviso de privacidad aunque sea persona física?

Sí. Al tratar datos personales de sus clientes, y más tratándose de sensibles, debe generarse un aviso de privacidad y darse a conocer en los términos ya comentados. Debe en todo momento cuidarse los datos personales que estamos tratando: no se pueden trasmitir a terceras personas, deben cuidarse los dispositivos en que se resguarden, y destruirse cuando ya no se utilicen.