Protección de Datos
y su incidencia en época del coronavirus

FUNDACIÓN ProBono COLOMBIA

Contenido

FUNDACIÓN ProBono COLOMBIA

Introducción

La creación de una cartilla sobre la protección de los datos en el Estado de Emergencia decretado en Colombia con ocasión de la pandemia provocada por el Coronavirus, se constituye como un documento es especial interés por los desafíos que presenta el tratamiento de los datos como herramienta principal de prevención y manejo de la crisis, la permanencia laboral, control sanitario, emisión de ayudas humanitarias, y hasta para la reactivación económica con aislamiento, estos tópicos acompasados con las normas que hacen parte del régimen normativo de protección de datos, y las que se han expedido de forma temporal, hacen del presente documento un instrumento de consulta para el enriquecimiento del conocimiento de los titulares de los datos sobre el adecuado manejo de su información por parte de terceros públicos o privados.

Cristian Fernando Barrera Cerón

Tópicos de Investigación

- Régimen Colombiano de Protección de Datos
- Clasificación de los Datos y la Información
- Derechos de la Protección de Datos
- Mecanismos y Autoridades para la Protección de Datos
- Principios para la Protección de Datos
- Habeas Data Financiero y Obligaciones Legales
- Protección de Datos - Salud y Subsidios - Covid19
- Protección de Datos - Comercio - Covid19

1. Régimen Colombiano de Protección de Datos

¿Existen en Colombia disposiciones en la Constitución Politica Nacional que reglamenten o amparen la protección de mis datos?

En el artículo 15 de la Constitución Política de la República de Colombia se consagra la protección de los datos, como un derecho fundamental, en el cual el titular, ostenta la calidad de propietario de sus datos. Es de resaltar que la Protección de los Datos, ha tenido un gran desarrollo jurisprudencial por La Corte Constitucional Colombiana, quien desde 1992 hasta la actualidad, se ha pronunciado con más de 180 sentencias, las cuales van de la mano con los principios internacionales de la protección de datos personales, que han sido incorporados en los textos y documentos de la Organización de las Naciones Unidas y la Unión Europea.

¿Existe en Colombia un marco normativo en materia de protección de datos?

Colombia cuenta con una mixtura de normas, que regulan la materia objeto de la presente cartilla, dentro de las importantes, encontramos, la **Ley 1266 de 2008** sobre el habeas data financiero y comercial destinado a calcular el nivel de riesgo crediticio; la **Ley 1273 de 2009**, destinada a proteger a título de bien jurídico la información y los datos personales; la **Ley 1581 de 2012** la cual tiene por objeto la protección de los datos personales de forma general y completa; y la **Ley 1712 de 2014** sobre transparencia de la información por parte de entidades públicas y privadas con función pública.

¿Si la mayoría de Países en el Mundo tienen una sola norma en materia de protección de datos porqué en Colombia existen dos?

En los sistemas normativos en materia de protección de datos existen dos modelos de protección de datos, uno completo en un solo cuerpo normativo y otro en el que confluyen dos o más sistemas de protección, teniendo en cuenta la interacción con la intimidad y privacidad. En Colombia se pensó en un sistema único y que este sería en la Ley 1266 de 2008, sin embargo en ésta se establecieron principios de protección para los datos financieros, siendo una regulación sectorial, por lo que con la Ley 1581 de 2012 se buscó la protección de todos los datos personales. Así las cosas, con el sistema híbrido colombiano, las disposiciones generales y sectoriales deben interpretarse según la ley general, y la complejidad de cada tipo de dato especial.

¿Qué materias de protección de datos se reglamentan en la Ley 1273 de 2009?

Es importante hacer claridad, la Ley 1273 de 2009 tal como su título lo indica, modifica el Código Penal, y crea un nuevo bien jurídico tutelado denominado "*De la protección de la información y de los datos*", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Igualmente sobre la protección de datos, crea tipo penales tales como "*Violación de datos personales y suplantación de sitios web para capturar datos personales*".

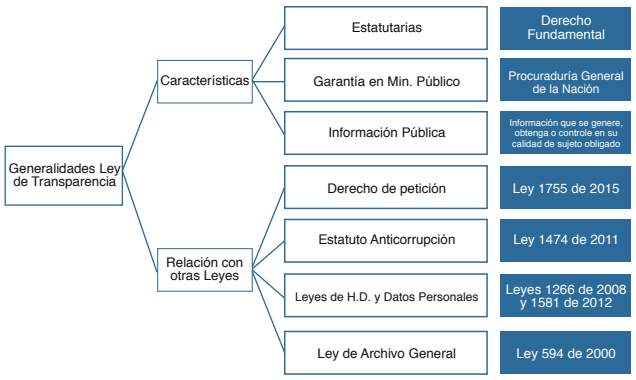
REGIMEN COLOMBIANO DE PD: Constitución Nacional Artículo 15, Ley 1266 de 2008, Ley 1273 de 2009, Ley 1581 de 2012, Ley 1712 de 2014, Decreto 1377 de 2013 (Decreto Único 1085 de 2015), Decreto 620 de 2020.

¿Qué materias se reglamentan a través de los Decretos 2952 de 2010 y 1377 de 2013?

El Decreto 2952 de 2010, reglamenta el tratamiento que se le debe brindar a los titulares de los datos, cuando los mismos hayan sido expuestos a situaciones de fuerza mayor, tales como, secuestro, desaparición forzada y secuestro, toda vez que por su estado de debilidad manifiesta, merecen contar con un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial, y consagra el tope máximo del reporte basado en la duración de la mora.

En cuanto al decreto 1377 de 2013, reglamentó parcialmente la Ley 1581 de 2012, y estableció aspectos relacionados con la autorización del titular de información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas.

¿A qué personas o entidades le son aplicables las normas de la Ley de Transparencia y del Derecho de Acceso a la Información Pública 1712 de 2014?



La también denominada Ley de transparencia aplica entre otras a: (i) Todas las entidades públicas de todas las Ramas del Poder Público, del Orden Nacional, Departamental, Municipal y Distrital; (ii) Los órganos, organismos y entidades independientes o autónomos y de Control; (iii) Las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos; (iv) Los partidos o movimientos políticos y los grupos significativos de ciudadanos. Estos sujetos están obligados al principio de máxima divulgación sobre la información que tratan de forma interna.

¿Qué disposiciones en materia de protección de datos presenta el Decreto 620 de 2020 sobre el uso y operación de los servicios ciudadanos digitales?

El Decreto establece que los Servicios Ciudadanos Digitales son el conjunto de soluciones y procesos que brinde el Estado para su transformación digital y lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante la administración pública. A su vez, el capítulo quinto del Decreto, consagra que, los Prestadores de Servicios Ciudadanos Digitales, son responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente, y deberán evaluar el impacto de las operaciones de dichos servicios en el tratamiento de datos, incluyendo:

- Una descripción detallada de las operaciones de tratamiento de datos y sus fines en la prestación de los servicios ciudadanos digitales.
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
- Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, aplicando la privacidad por diseño y por defecto.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, tecnologías y mecanismos que garanticen la protección de datos.

2. Clasificación de los Datos y la Información

Datos Personales: Son los datos asociados a una persona y que permiten su identificación.

Datos Públicos: Son los que obedecen a un interés general o público, como los documentos y registros públicos, tales como las sentencias o el número de su cédula.

Datos Privados: Son los datos que tienen un interés íntimo, reservado y que su conocimiento interesa al titular, tales como fotografías, videos, etc.

Datos Semiprivados: Son los datos que su conocimiento presentan relevancia o importancia para el titular y un cierto sector o grupo de personas, tales como datos financieros.

Datos Sensibles: Son los datos que su inadecuado tratamiento afecta la intimidad del titular o puede generar su discriminación, tales como datos de salud u orientación sexual.

Información Pública Clasificada: Es aquella información que pertenece al ámbito privado o semiprivado de una persona natural o jurídica y que su acceso es clasificado por poder vulnerar derechos como la intimidad, la salud, los secretos comerciales, etc.

Información Pública Reservada: Es aquella información que legalmente está prohibida su revelación a terceros no autorizados, como la información de defensa y seguridad nacional.

Información Protegida por la Reserva Bancaria: Es la información respecto de la cual las entidades vigiladas por la Superintendencia Financiera de Colombia deben guardar reserva y discreción sobre los datos de sus clientes, tales como los datos de movimientos financieros, etc.

3. Derechos de la Protección de Datos

¿Qué derechos se traducen en el denominado "ARCO"?

De forma coincidente ende la Ley 1266 de 2008 y 1581 de 2012, se establecen como derechos de los titulares de los datos los denominados derechos **ARCO: Acceso, Rectificación, Cancelación y Oposición.**

- **Acceder:** Todos los titulares de los datos tienen el derecho a obtener información sobre el origen y tratamiento de sus datos, así como ser informado de tratamientos específicos.

- **Rectificar:** Todos los titulares de los datos tienen el derecho a que sus datos se traten con veracidad, por lo que es posible solicitar que se modifiquen o rectifiquen cuando no sean correctos o estén incompletos.

- **Conocer:** El también denominado derecho al olvido consiste en la posibilidad de los titulares de los datos de solicitar se excluyan los datos que no son óptimos o que no son proporcionales para el tratamiento.

- **Oponerse:** Los titulares de los datos tienen derecho a presentar oposición a que sus datos sean tratados para fines específicos o que no sean tratados en absoluto.

¿Cómo se desarrolla el derecho de supresión del dato?

De forma adicional a los derechos de habeas data denominados ARCO, la legislación colombiana en la materia establecen otros derechos como el de supresión de los datos, el cual consiste en la posibilidad de los titulares de los datos por diversas razones, incluso personales, soliciten la exclusión de su información de una base de datos, aduciendo voluntad propia o por uso indebido de los datos, salvo que exista una obligación legal o contractual que impida que se realice la supresión del dato y demande su permanencia. **El ejemplo más común es la solicitud de eliminación de los datos para entrega de información comercial o publicidad.**

¿Cómo se debe entender el derecho de revocación de la autorización?

Consiste en la posibilidad de manifestar la revocación de la autorización del tratamiento de los datos, con este derecho se priva de la legitimación para realizar tratamientos de datos, procede también el derecho cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento se ha incurrido en conductas contrarias a la ley. Sin embargo no procederá cuando se tenga un deber legal, o convencional de permanecer.

¿En qué consiste el derecho de actualización de los datos?

En virtud del principio de veracidad de la información, al titular de los datos le asiste el derecho a actualizar sus datos personales frente a los responsables, encargados, operadores, fuentes o usuarios de la información cuando estos datos sean parciales, desactualizados, inexactos, incomprensibles, fraccionados o incompletos.

¿Es posible solicitar prueba de la autorización de tratamiento de datos e información del uso de los mismos?

De acuerdo con los principios de libertad, transparencia y finalidad, el titular de los datos tiene el derecho a solicitar a los responsables, encargados, operadores, fuentes o usuarios de la información, copia o prueba de la autorización otorgada, salvo los casos en los que por disposición legal se encuentre exceptuada la obligación de realizar tratamiento de datos con autorización o consentimiento del titular de la información.

4. Mecanismos y Autoridades para la PD

¿Con qué garantías constitucionales goza la protección de los datos en Colombia?
Según lo dispuesto en el artículo sexto de la Ley 1266 de 2008 y el artículo octavo la Ley 1581 de 2012, los derechos que se derivan del Derecho de "habeas data" se pueden ejercer a través de las garantías del **Derecho de Petición** y la de **Acción de Tutela**, consagrados en los artículos 23 y 86 de la Constitución Nacional.

¿Ante que entidades me puedo quejar por un inadecuado tratamiento de datos financieros?
Atendiendo lo señalado en el artículo 17 de la Ley 1266 de 2008 existen dos autoridades de vigilancia en materia de datos financieros, por un lado la **Superintendencia de Industria y Comercio** como Autoridad de Protección de Protección de Datos; y la **Superintendencia Financiera de Colombia**, cuando el infractor sea una entidad vigilada por ésta última autoridad. Igualmente, respecto de entidades financieras es posible acudir al **Defensor del Consumidor Financiero**, según lo dispuesto en el artículo 5º de la Ley 1328 de 2009.

¿Es posible realizar una actuación judicial para la protección de los datos?
A través del **proceso declarativo** consagrado en el Código General del Proceso – CGP, es posible ventilar las controversias que se presenten en materia de protección de datos, acciones que serán del conocimiento del Juez Civil; en los casos de entidades financieras es igualmente posible adelantar la **acción de protección al consumidor financiero** consagrado en el artículo 24 del CGP.

¿Existen medidas administrativas que se puedan iniciar por vulneración de datos personales?
La Superintendencia de Industria y Comercio en el marco de las facultades otorgadas en los artículos 17 y 19, de las Leyes 1266 de 2008 y 1581 de 2012, respectivamente, puede conocer de las **denuncias que por violación de tratamiento de datos** que presenten los titulares; la Superintendencia Financiera de Colombia – SFC podrá conocer de las infracciones al habeas data financiero, respecto de sus entidades vigiladas.

¿En el marco de la Ley 1273 de 2009 existen acciones judiciales que puedan ser adelantadas, como y ante que autoridades se pueden realizar?
En el ámbito penal por infracciones a la protección de la información, al amparo del tipo penal consagrado en el artículo 269F de la Ley 1273 de 2009, sobre la violación de los datos personales, es posible presentar **denuncia penal ante la Fiscalía General de la Nación.**

¿Cuáles son las autoridades colombiana que velan por la protección de los datos?
La **Superintendencia de Industria y Comercio** (Autoridad de Protección de Datos); la **Procuraduría General de la Nación** sobre los tratamientos inadecuados de datos por parte de autoridades públicas; la Superintendencia Financiera de Colombia sobre las infracciones en materia de habeas data financiero que realicen sus vigiladas; el **Juez Civil** respecto de los procesos judiciales que se adelanten en la materia; y el **Juez Penal Municipal** respecto de los delitos de violación de datos personales.

¿Qué medidas pueden emitir las autoridades de protección de datos en Colombia?
Dentro de las medidas posibles que pueden adoptar están: (i) **Ley 1266 de 2008:** Multas de carácter personal e institucional hasta por el equivalente a 1.500 Salarios Mínimos Mensuales Legales Vigentes – SMMLV (Año 2020 $1.470.985.500), suspensión de actividades, cierre temporal o inmediato de la operación; (ii) **Ley 1581 de 2012:** Multas de carácter personal e institucional hasta por el equivalente a 2.000 SMMLV (Año 2020 $1.961.314.000), suspensión de actividades, cierre temporal o inmediato; (iii) **Ley 1273 de 2009:** Pena de prisión de (48) a (96) meses y en multa de 100 a 1000 SMMLV (Año 2020 máximo $ 980.657.000.

5. Principios para la Protección de los Datos

PRINCIPIO DE FINALIDAD: El tratamiento de los datos debe realizarse para una finalidad legítima de acuerdo con la ley, e informada al Titular.

PRINCIPIO DE LIBERTAD: El tratamiento de datos solo puede ejercerse con el consentimiento, previo, expreso e informado del Titular.

PRINCIPIO DE LEGALIDAD: El tratamiento de los datos debe desarrollarse conforme con la ley y las demás disposiciones en la materia.

PRINCIPIO DE VERACIDAD: Los datos objeto de tratamiento deben ser veraces, exactos, comprensibles, completos, no pueden ser parciales, incompletos, o que induzcan a error.

PRINCIPIO DE CONFIDENCIALIDAD: Se debe garantizar la reserva de la información, se prohíbe el acceso o comunicación de datos a terceros no autorizados.

PRINCIPIO DE SEGURIDAD: Los datos se deben tratar con las medidas técnicas o humanas necesarias para otorgar seguridad, evitando su adulteración pérdida, uso o acceso no autorizado.

PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA: El tratamiento de los datos se debe sujetar a los límites establecidos en la Ley, y solo podrá realizarse por personas autorizadas.

PRINCIPIO DE TRANSPARENCIA: En el tratamiento de datos se debe garantizar los derechos de habeas data e información del titular, podrán ejercerse en todo momento y sin restricciones.

RAZONABILIDAD: Solo podrán recolectarse, almacenar, usar o circular los datos durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades de tratamiento.

Interpretación integral de derechos constitucionales: Las normas deben interpretarse en el sentido de que se amparen adecuadamente los derechos al habeas data, y a la información.

6. Habeas Data Financiero y Obligaciones Legales

¿Qué obligaciones tienen las entidades antes de realizar el reporte negativo de una obligación ante los operadores de bancos de datos?

De acuerdo con lo dispuesto en la Ley 1266 de 2008 de forma previa a que una fuente de información, como un establecimiento de crédito, realice el reporte negativo de una obligación ante los operadores de información financiera debe acreditar: (i) Contar con la autorización para llevar a cabo el reporte, (ii) Contar con los soportes de contratación y comportamiento de la obligación a reportar, (iii) realizar una comunicación previa al titular del datos con no menos de (20) días calendario previo al reporte.

¿Cuál es el tiempo de permanencia de los reportes negativos de las obligaciones?

Teniendo en cuenta lo dispuesto en la Ley 1266 de 2008, las normas reglamentarias y la Jurisprudencia colombiana en la materia, se deben diferencias diversos eventos sobre la permanencia del dato negativo:

1. **El escenario de pago de la obligación o de sus cuotas vencidas:** El máximo tiempo de permanencia será el doble del tiempo que se ha permanecido en mora, hasta el término de 4 años, es decir que así permanezca en mora por más de 2 años, el tiempo del reporte no podrá ser por más de 4 años.

2. **El escenario de terminación de la obligación por modo diferente al pago:** Teniendo en cuenta que dentro de las formas de extinción de las obligaciones diferentes al pago se encuentran entre otras la novación, la condonación, la compensación, la prescripción, el término de permanencia del dato negativo será de 4 años contados a partir desde la ocurrencia de uno de estos eventos.

3. **El escenario que ha operado la prescripción liberatoria:** Debido al vacío legal que se establece en la norma sobre la caducidad del dato negativo por ausencia de pago o de alguno de los diversos modos de extinción de las obligaciones, la Corte Constitucional ha establecido que el dato negativo no puede permanecer de forma indefinida, por lo que la caducidad del dato negativo es de 14 años, computados así: (i) 10 años que se deben contar desde el momento en que se hizo exigible la obligación (la ocurrencia de este término es denominado prescripción liberatoria) y (ii) 4 años después de verificar que pasaron los 10 años de la prescripción liberatoria, para un total de 14 años.

* La Corte Constitucional igualmente he mencionado que la verificación de la caducidad del dato negativo, de ninguna manera implica la declaratoria judicial sobre la prescripción de la obligación.

¿Si inicio un proceso de Insolvencia de Persona Natural no Comerciante como opera el tiempo de permanencia del dato negativo?

La ley 1564 de 2012 en materia de insolvencia de persona natural no comerciante establece que en el caso en que el conciliador o el juez acepten la solicitud de negociación de deudas deben comunicarlo de forma inmediata ante los operadores de información financiera para que realicen el registro en el reporte de las obligaciones financieras. Ahora bien, en caso de liquidación patrimonial, el término de caducidad del dato negativo de los (4) años, debe empezarse a contar (1) años después de la fecha de la apertura de la liquidación.

¿Cómo opera la permanencia de los datos negativos en los procesos concursales?

Según las disposiciones de la Ley 1116 de 2006, y la Doctrina de la Superintendencia de Sociedades, es posible concluir que el reporte negativo antes las centrales de información financiera según lo señalado en la Ley 1266 de 2008, es posible desarrollarse en tres situaciones así: (i) el reporte de las obligaciones antes del acuerdo de reorganización, (ii) el reporte de obligaciones una vez se ha logrado un acuerdo de reorganización, y (iii) el reporte de obligaciones que se adquieren con posterioridad al acuerdo de reorganización.

En el primer y tercer escenario el reporte negativo de las obligaciones impagas antes del acuerdo de reorganización o las que se adquieran con posterioridad al acuerdo, seguirán los términos de permanencia ordinarios de la **Ley 1266 de 2008** teniendo en cuenta que en éstos dos casos las obligaciones conservan las **condiciones iniciales pactadas.**

Caso contrario sucede con el segundo de los eventos planteados, pues las obligaciones impagas en el proceso de reorganización con acuerdo aprobado, les son aplicables las disposiciones normativas de los artículos 20 y 40 de la Ley 1116 de 2006, en el sentido que las obligaciones incluidas en el acuerdo de reorganización **se modifican con el acuerdo**, y la mora en el pago se entenderá terminada. Se podrá entonces reportar en estado de **acuerdo de reorganización.**

¿Qué obligaciones documentales tienen las entidades que realizan tratamiento de datos?

Conforme con lo dispuesto en la ley 1581 de 2012 y el Decreto 1733 de 2013 es una obligación de quien realiza tratamiento de datos, elaborar, publicar y cumplir con lo siguiente: (i) Contar y conservar copia de la **Autorización** otorgada por los titulares de los datos, (ii) Contar con una **Política de Tratamiento de Datos** la cual debe estar disponible para los titulares y (iii) Cuando no sea posible poner a disposición de los titulares de los datos la Política de Tratamiento se deberá contar con un **Aviso de Privacidad.**

OBLIGACIONES LEGALES

AUTORIZACIÓN

- Informar de forma clara si el tratamiento será manual o automatizado.
- Informar que es facultativo contestar preguntas sobre datos sensibles.
- Informar las finalidades del tratamiento.
- Informar de forma clara y explícita cuáles datos a tratar son sensibles.
- Informar de forma completa los derechos de habeas data que le asisten al titular.
- Informar los canales para ejercer los derechos de habeas data.
- Informar los datos de identificación y contacto del responsable del tratamiento.
- Dejar constancia que el consentimiento fue informado.

POLÍTICA DE TRATAMIENTO DE DATOS

- Constar en medio físico o electrónico.
- Redactarse en lenguaje claro.
- Establecer un medio físico o electrónico de divulgación.
- Nombre, razón social, datos de contacto físicos y electrónicos.
- Informar los principios aplicables para el tratamiento de los datos.
- Indicar el tipo de tratamiento manual o automatizado.
- Informar las finalidades del tratamiento.
- Informar de forma completa los derechos y forma de ejercerlos.
- Informar el procedimiento para procesar los derechos de habeas data.
- Informar la publicación de la Política y su vigencia.

AVISO DE PRIVACIDAD

- Informar el nombre o razón social del responsable del tratamiento.
- Informar los datos de contacto del responsable del tratamiento.
- Informar el tipo de tratamiento manual o automatizado.
- Informar las finalidades del tratamiento.
- Informar de forma completa los derechos de habeas data que le asisten al titular.
- Informar los mecanismos de comunicación y disposición de la Política de Tratamiento de Datos.
- Informar que es facultativo contestar preguntas sobre datos sensibles.

7. Registro de Bases y Transferencia

¿Qué obligaciones tienen las entidades antes de realizar el reporte negativo de una obligación ante los operadores de bancos de datos?
De acuerdo con lo dispuesto en la Ley 1266 de 2008 de forma previa a que una fuente de información, En la ley 1581 de 2012 se estableció como obligación a cargo de los responsables del tratamiento de los datos, realizar el registro de las bases de datos de datos personales ante la Superintendencia de Industria y Comercio- SIC, autoridad que tiene a cargo el Registro Nacional de Bases de Datos – RNBD, denominado el directorio público de las bases de datos sujetas a tratamiento que operan en el país.

Después de una serie de prórrogas sobre el registro de bases datos, a través de la Circular 003 de 2018 la SIC, estableció los obligados a llevar a cabo el RNBD, las entidades públicas, sociedades o entidades sin ánimo de lucro que tengan activos fijos totales superiores a 100.000 Unidades de Valor Tributario – UVT (Año 2020 $3.560.700.000).

El RNBD consiste en la identificación de la base de datos, el registro de la cantidad de datos almacenados, las medidas de seguridad empleadas, la procedencia de los datos, la transferencia o transmisión nacional o internacional de los datos, la cantidad de reclamos presentados por los titulares, y los incidentes de seguridad. El RNBD debe ser actualizado según las siguientes periodicidades: (i) Dentro de los primeros (10) hábiles de cada mes cuando se realicen cambios sustanciales en la información registrada, (ii) anualmente, entre el 2 de enero y el 31 de marzo, (iii) dentro de los primeros (15) días de los meses de febrero y agosto de cada año se deberá actualizar los reclamos, (iv) las bases nuevas se deben registrar (2) meses después de su creación.

¿Por las operaciones de mi empresa debemos realizar transferencias de datos a terceros países, para custodia o tratamiento de los datos, cómo se deben realizar esas transferencias?
Según lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, existen los conceptos de transmisión y transferencia de datos, consistiendo la transmisión de los datos en el envío de la información personal a una persona natural o jurídica ubicada localmente en el exterior, quién realizará el tratamiento de datos personales bajo las instrucciones de un responsable; y la transferencia entendida como el envío de información personal a una persona natural o jurídica ubicada localmente o en el exterior, quien decidirá autónomamente sobre el tratamiento de la información. La siguiente imagen explica la transferencia internacional de datos.

TRANSFERENCIA INTERNACIONAL DE DATOS

La transferencia internacional de datos es posible, siempre y cuando se cumpla con algunos de los siguientes requisitos:

1. Que el país al que se transfieren los datos sea catalogado por la Autoridad de Protección de Datos como un país con nivel adecuado de protección de datos.
2. Que la transferencia se trate de:
   a) Información respecto de la cual el titular haya otorgado su autorización para la transferencia;
   b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento por razones de salud o higiene pública;
   c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
   d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte;
   e) Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable;
   f) Transferencias para la salvaguardia del interés público, o para el reconocimiento de un derecho en un proceso judicial.

1. En los casos anteriormente no contemplados, corresponderá a la SIC proferir una declaración de conformidad relativa a la transferencia internacional de datos personales.
2. Se presume que la transferencia internacional cuenta con Declaración de Conformidad de la Autoridad de Protección de Datos, en el caso de que las partes hayan celebrado contrato donde establezcan las condiciones del tratamiento, se realicen con Responsabilidad Demostrada y con verificación del nivel adecuado de protección de datos.
3. Para llevar a cabo este último procedimiento se deberá remitir una comunicación a la SIC, informando sobre la operación a realizar y declarando que han suscrito el contrato de transferencia que garantice la protección de los datos objeto de transferencia, lo cual podrá ser verificado en cualquier momento.

8. Protección de Datos - Salud y Subsidios - Covid19

¿A los datos de la temperatura que se tomen durante el estado de emergencia por la pandemia originada por el Covid19, les aplican las normas de protección de datos?
Dentro de las medidas para combatir y mitigar los efectos de la pandemia provocada por el Covid-19, el Ministerio de Salud y Protección Social expidió la Resolución 666 del 24 de abril de 2020, mediante la cual se establece el protocolo de bioseguridad general para realizar el control y mitigación adecuados de la pandemia, siendo obligatorias tanto para el empleador como para el trabajador.

> Por ejemplo, en el apartado 5.1 de la mencionada resolución, en lo relacionado a "Prevención y manejo de situaciones de riesgo de contagio" se establecen dos situaciones de obligatorio cumplimiento en el lugar de trabajo: *"No se puede permitir el ingreso de y/o acompañamiento a las instalaciones de personas que presenten **síntomas de gripa ni cuadros de fiebre igual o mayor a 38°C**". "Establecer un protocolo de verificación de estado de salud y temperatura de proveedores y clientes cuando haya algún tipo de ingreso a las instalaciones".*

De lo anterior, se concluye que la toma de temperatura es un elemento esencial incluido en el protocolo de bioseguridad y de obligatorio cumplimiento, sin perjuicio de ello, teniendo en cuenta la calidad especial de los datos de salud como sensibles, a su recolección y autorización deben aplicarse la ley 1581 de 2012 en cuanto al tratamiento de datos sensibles y la excepción a su utilización por urgencia médica o sanitaria.

¿Qué medidas aplican en materia de protección de datos para el trabajo en casa, con ocasión del aislamiento decretado con ocasión de la pandemia originada por el Covid19?
La pandemia del Covid-19 origino la masiva implementación del trabajo en casa, de manera remota o virtual, tal y como se estableció en el protocolo de bioseguridad de la Resolución 666 del 2020. En tal sentido, y para garantizar el correcto uso de las herramientas tecnológicas con el fin de asegurar la protección y seguridad de datos personales se establecieron las siguientes recomendaciones de seguridad en ambientes digitales tales como: (i) Utilizar solo las herramientas corporativas para recibir, almacenar o compartir información; (ii) No utilizar ni enviar información a través de correos personales; (iii) No utilizar herramientas de almacenamiento, conversión de archivos o envío de información gratuita que no estén licenciadas por la empresa.

¿Existe una limitación en el uso de los datos personales y de los datos sensibles?
Los datos que se requieran recolectar para cumplir los protocolos de bioseguridad no puedan ser utilizados para otros fines, como publicidad y marketing. Los datos recabados deberán almacenarse durante un tiempo razonable para cumplir los protocolos o contestar requerimientos administrativos. Los datos recolectados deberán suprimirse de forma segura una vez cumplan la finalidad. Sobre La recolección y tratamiento de datos sensibles se deben implementar medidas reforzadas para garantizar la seguridad y confidencialidad de estos datos, No se puede condicionar ninguna actividad a que el titular suministre datos sensibles.

¿Es necesaria la aplicación de normas de protección de datos, para el otorgamiento de subsidios previstos por el Gobierno con ocasión de la emergencia sanitaria por el Covid19?
Mediante los Decretos 639, 770 y 550 de 2020 se crearon una serie de subsidios Estatales, para los cuales las normas de creación establecieron que de forma temporal autoriza a las entidades públicas y privadas para recibir y suministrar los datos personales así como la información crediticia, comercial, que sea necesaria para la entrega del aporte estatal, de este modo, apelando a los principios de protección de los datos se debe recordar que el tratamiento debe obedecer a la finalidad de creación del programa, para identificar y certificar a los beneficiarios del programa, y garantizar la entrega efectiva de los aportes, igualmente se deben adoptar medidas para garantizar la seguridad, temporalidad, circulación restringida y confidencialidad de dichos datos.

9. Protección de Datos – Comercio - Covid19

¿En el contexto de la pandemia es posible realiza el uso de huelleros digitales?
A través de la Circular 002 de 2020 la SIC estableció la prohibición para entidades públicas o privadas de recolectar o tratar datos utilizando huelleros físicos o electrónicos. Sin perjuicio de lo anterior, en la Circular Externa 012 de 2020 de la SFC y la Resolución Nro. 4243 de la Superintendencia de Notariado y Registro – SNR, se estableció que para garantizar la prestación de servicios financieros, y trámites notariales, respectivamente, es posible usar los huelleros, aplicando protocolos de limpieza y desinfección.

¿Si una Autoridad Administrativa me solicita datos para la prevención y control del COVID-19, mi empresa está autorizada para entregarlos?
La SIC ha establecido en la Circular 01 de 2020 que los operadores de telefonía y entidades privadas, están autorizados para suministrar al Departamento de Planeación Nacional (DPN) y demás entidades públicas los datos que sean necesarios para la prevención, control y tratamiento de la propagación del Covid-19.

¿Para las medidas de reactivación económica como los días sin IVA, se deben aplicar normas de protección de datos?
Por medio de la Circular 05 de 2020 la SIC estableció que en ejecución de los días sin IVA decretados, no se suspende la aplicación de las normas de protección de datos teniendo que lo fundamental del derecho de habeas data, en este sentido instruye a los comercios que actúen en calidad de responsable de los datos de los consumidores para que realicen un tratamiento adecuado de los datos, como la recolección de datos ajustada a la autorización del titular, para la finalidad de la recolección, con seguridad, y circulación restringida. La autoridad reitera lo dispuesto en el Decreto 1733 de 2013 sobre el tratamiento de datos sensibles, su protección reforzada, así como que ninguna actividad puede condicionarse al suministro de datos sensibles.

¿El régimen de protección de datos rige en el contexto del COVID-19?
El pasado 18 de agosto de 2020 la SIC emitió la Circular 008 de 2020, en la que mencionó que con ocasión de la expedición de medidas excepcionales de salud emitidas por parte del Ministerio y Protección Social, no suspenden, o aplazan la aplicación de las disposiciones normativas en materia de protección de datos.

¿Existen deberes y medidas especiales en la recolección de datos?
Según las disposiciones normativas se prohíbe “utilizar medios engañosos o fraudulentos para recolectar datos”, de debe garantizar el debido otorgamiento de la autorización por parte del titular. Se deben recoger datos “pertinentes y adecuados para la finalidad para la cual fueron recogidos”, para el cumplimiento de la legislación en materia de salud, solo deben recogerse los datos exigidos por el Ministerio de Salud.

¿Se debe informar las finalidades del tratamiento y justificar la necesidad de recolección?
En la recolección de la información se deben comunicar las finalidades específicas del tratamiento de los datos y las normas de salud y salubridad, la recolección de los datos se debe realizar a través de medios idóneos, y se debe justificar la necesidad de recolección de los datos a la luz de las normas de excepción. Teniendo en cuenta el deber de información se recomienda disponer en el lugar de recolección de los datos el aviso de privacidad de la empresa, entidad o comercio que recolecta los datos.

¿Qué debo hacer con las bases de datos que he generado para cumplir con los protocolos?
Teniendo en cuenta que en cumplimiento de los protocolos de bioseguridad se puede generar la creación de nuevas bases de datos, si la empresa, entidad o comercio está obligada a llevar a cabo el Registro Nacional de Bases de Datos – RNBD ante la SIC, deberá realizar el registro de las nuevas bases de datos creadas.

Síguenos en nuestras redes sociales:

FUNDACIÓN ProBono COLOMBIA