[1]Decreto Ejecutivo N° 285

(de 28 mayo de 2021)

Que reglamenta la Ley 81 de 2019 sobre Protección de Datos Personales

EL PRESIDENTE DE LA REPÚBLICA
en uso de sus facultades constitucionales y legales,

CONSIDERANDO:

Que la Constitución Política de la República de Panamá reconoce entre sus garantías fundamentales la inviolabilidad de las comunicaciones privadas y el derecho que tiene toda persona de acceder a su información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley;

Que mediante la Ley 81 de 2019 se promulgó el régimen general de protección de datos personales con el objeto de establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales de las personas naturales en la República de Panamá y en la misma se estableció, además, una prórroga para su entrada en vigor, efectiva a partir del 29 de marzo de 2021;

Que corresponde al Órgano Ejecutivo, a través del Ministerio de la Presidencia y en coordinación con Autoridad Nacional de Transparencia y Acceso a la Información, reglamentar la citada Ley para facilitar su implementación y cumplimiento por los responsables del tratamiento y custodios de las bases de datos;

Que la Ley 81 de 2019 constituye el marco general de defensa del derecho a la protección de datos personales en la República de Panamá y, por tanto, debe ser considerada como el estándar mínimo de cumplimiento en relación con la protección de datos personales por cualquier ley especial en la materia y por cualquier entidad reguladora;

Que observando los estándares internacionales en materia de protección de datos personales y, en particular, por orden cronológico de aprobación: las Directrices de privacidad de la OCDE de 1981, los principios de Protección de Datos para Iberoamérica de la OEA de 1996, el Reglamento Europeo de Protección de Datos de 2016 y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, aprobados el 20 de junio de 2017, entre otros, el presente decreto desarrolla la Ley 81 de 2019, siguiendo estos lineamientos;

Que, teniendo en cuenta el aumento de flujos transfronterizos de datos y operaciones comerciales, la República de Panamá requiere un régimen fuerte en materia de protección de datos personales y una autoridad de control reconocible a nivel nacional;

Que la Constitución Política dispone que es atribución del Presidente de la República, con la participación del ministro respectivo, reglamentar las leyes que lo requieran sin apartarse de su texto ni de su espíritu,

DECRETA:

Capítulo I
Disposiciones generales

Art. 1. Objeto. Este decreto ejecutivo tiene por objeto desarrollar las disposiciones que regulan el régimen general de protección de datos personales para la República de Panamá previstos en la Ley 81 de 26 de marzo de 2019.

Las disposiciones y postulados sobre protección de datos personales contenidos en la Ley 81 de 2019 y el presente decreto, son mínimas y no excluyentes de otras leyes especiales sobre la materia, especialmente en lo relativo al tratamiento y custodia de datos.

Este decreto constituye el régimen de aplicación general a cualquier tratamiento de datos personales sin perjuicio de tener que observar, además, los requisitos añadidos que puedan establecerse en leyes especiales que resulten aplicables al tratamiento de datos que se llevan a cabo por el responsable del tratamiento o por el custodio de la base de datos y especialmente en el caso de actividades reguladas.

En el caso de sujetos regulados por la ley especial, siempre que esta ley contenga reglas relativas al tratamiento de datos personales, se tendrá la Ley 81 de 2019 y el presente decreto como régimen general y estándar mínimo de cumplimiento para garantizar la correcta protección de los datos personales. La ley especial debe regular aquellos requisitos especiales que exijan los tratamientos de datos que en ella se señalan y de esta forma complementar y ampliar las previsiones de la Ley 81 de 2019, con la finalidad de que los datos personales que sean objeto de tratamiento de esa actividad queden debidamente protegidos.

[1] Publicado en la Gaceta Oficial 29.296-A de 28 de mayo de 2021.

Cuando así lo exija el sector regulado, los requerimientos de las políticas de privacidad, protocolos, procesos y procedimientos de tratamiento y transferencia segura establecidos por la Ley 81 de 2019 y este decreto, deberán ser completados para adaptarse a las exigencias de sus tratamientos de datos.

Art. 2. Ámbito de aplicación. La Ley 81 de 2019 y el presente decreto, resultarán aplicables cuando:

1. Las bases de datos se encuentren en el territorio de la República de Panamá y almacenen o conserven datos personales de nacionales o extranjeros;
2. El responsable del tratamiento de los datos personales esté domiciliado en la república de Panamá.
3. Los tratamientos de datos cuyo origen o almacenamiento sea el territorio de la República de Panamá, con las excepciones previstas en la Ley 81 de 2019; y
4. Los tratamientos de datos realizados en el marco de una actividad comercial, por Internet o cualquier otro medio de comunicación electrónica o digital, conforme a la Ley 51 de 2008, para organizar la protección de los datos personales en las actividades dirigidas al mercado panameño.

Art. 3. Sujetos protegidos. Quedan sujetos a protección los tratamientos de datos personales de las personas naturales, siempre que estos datos los identifiquen o los hagan identificables. Los derechos de las personas fallecidas en relación con sus datos personales se rigen por las reglas generales del Código Civil.

En el caso de tratamiento de datos personales de menores de edad, se dará prioridad al interés superior del menor conforme a las normas de la República de Panamá y a los tratados internacionales existentes en la materia.

Art. 4. Definiciones. Para los efectos de este decreto, además de los términos contenidos en la Ley 81 de 2019, también regirán los siguientes:

1. Autoridad de control. La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), es el organismo de la administración pública responsable de supervisar, implementar y controlar el cumplimiento de la Ley 81 de 2019 y el presente decreto, en todo el territorio nacional.
2. Datos biométricos. Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen la identificación única de dicha persona.
3. Datos genéticos. Datos personales relativos a las características genéticas heredadas o adquiridas de una persona natural que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
4. Datos relativos a la salud. Datos personales relativos a la condición física o mental de una persona natural, que revelen información sobre su estado de salud.
5. Derechos ARCO. Derechos irrenunciables básicos de los titulares de datos personales, e identificados como: derechos de acceso, rectificación, cancelación y oposición.
6. Destinatario: La persona natural o jurídica, autoridad pública, servicio u organismo al que se transfieran datos personales.
7. Elaboración de perfiles. Toda forma de tratamiento automatizado que utilice datos personales para evaluar determinados aspectos de una persona natural, y en particular para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos.
8. Exportador. Persona natural o jurídica de carácter público o privado, domiciliado en el país, que efectúe transferencias de datos personales extrafronterizos, conforme a lo dispuesto en la Ley 81 de 2019 y el presente decreto.
9. Evaluación de impacto en protección de datos. Documentación del responsable del tratamiento que contiene la descripción de los procesos con datos personales que pueden generar riesgos para los derechos y deberes individuales y sociales, así como medidas, salvaguardas y mecanismos de mitigación de riesgos.
10. Oficial de Protección de Datos Personales. Funcionario designado para atender la unidad de enlace.
11. Regulador: Entidad del Estado encargada de fiscalizar a los sujetos de sectores regulados por leyes especiales.
12. Violación de la seguridad de los datos personales. Toda infracción a la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Sección primera
Principios generales para el tratamiento

Art. 5. Principios. La protección de datos personales se rige por los principios de lealtad, finalidad, proporcionalidad, veracidad y exactitud, seguridad de los datos, transparencia, confidencialidad, licitud y portabilidad.

Art. 6. Principio de lealtad. Los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos.

Art. 7. Principio de finalidad. Los responsables del tratamiento deberán recolectar datos con fines determinados y legítimos.

Los datos no podrán utilizarse posteriormente de manera incompatible o diferente con dichos fines. El tratamiento ulterior de los datos personales con fines de investigación, estudios, encuestas o conocimientos de interés público, no se considerará incompatible con los fines que motivaron la recogida.

Los fines del tratamiento de los datos determinarán el plazo de conservación de estos, transcurrido el cual el responsable del tratamiento los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización. Para determinar el plazo de conservación de los datos se acudirá a las leyes aplicables en cada caso y a las responsabilidades de todo orden que deban ser atendidas por el responsable del tratamiento o custodio de la base de datos.

En el caso de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias se atenderá a lo dispuesto en el artículo 30 de la Ley 81 de 2019.

Art. 8. Principio de proporcionalidad. Para conocer qué datos son adecuados, pertinentes y mínimos necesarios para la finalidad perseguida con el tratamiento de los datos, los responsables del tratamiento y, en su caso, los custodios de la base de datos, tomarán en cuenta el estado de la tecnología, la naturaleza, ámbito, contexto y fines de tratamiento.

Con este fin podrán realizar y documentar evaluaciones de impacto en protección de datos personales con el objeto de minimizar los datos objeto de tratamiento, conocer los riesgos que impliquen los tratamientos y adoptar las medidas y garantías necesarias para mitigarlos.

La autoridad de control podrá definir aquellos supuestos en los que es recomendable realizar una evaluación de impacto y establecer las pautas o estándares a seguir en su desarrollo.

Los responsables del tratamiento y los custodios de las bases de datos, adoptarán medidas organizativas que regulen el acceso a los datos personales en su entidad, conforme a este principio permitiendo el acceso a ellos únicamente a los empleados o funcionarios públicos que lo necesiten para el desarrollo de sus funciones y limitando el mismo a la cantidad de datos y al tiempo necesario para ello.

Art. 9. Principio de veracidad y exactitud. Los responsables del tratamiento adoptarán las medidas necesarias para mantener exactos y puestos al día los datos personales en su posesión, de tal manera que no se altere la realidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

Art. 10. Principio de transparencia. Toda información o comunicación al titular de los datos personales relativa al tratamiento de éstos deberá ser en lenguaje sencillo y claro, y mantenerlo informado de todos los derechos que le amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO.

Art. 11. Principio de confidencialidad. Todas las personas que intervengan en el tratamiento de datos personales están obligadas a guardar secreto o reserva respecto de estos, incluso cuando hayan finalizado su relación con el titular o responsables del tratamiento de los datos, impidiendo el acceso o uso no autorizado.

Art. 12. Principio de licitud. Para que el tratamiento de un dato personal sea lícito, deberá ser recolectado y tratado con base en algunas de las condiciones de licitud que reconoce la Ley 81 de 2019 y conforme a lo que se describe en la Sección tercera de este Capítulo.

Art. 13. Principio de portabilidad. El titular de los datos tiene derecho a obtener de parte del responsable del tratamiento una copia de los datos personales de manera estructurada en un formato genérico de uso común.

Sección segunda
Requisitos de la información

Art. 14. Contenido de la información. Cuando los datos se obtengan directamente del titular, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

1. La identidad y datos de contacto del responsable del tratamiento.
2. La finalidad o finalidades del tratamiento a que se destinarán los datos personales; cuando el responsable del tratamiento proyecte el tratamiento posterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento posterior, información sobre ese otro fin y cualquier información adicional pertinente.
3. La condición que legitima el tratamiento conforme a los artículos 6, 8 y 33 de la Ley 81 de 2019. Cuando el tratamiento esté basado en el consentimiento del interesado, se le debe informar de su derecho a revocar el consentimiento en cualquier momento, sin que ello tenga efectos retroactivos; cuando el tratamiento de datos personales sea un requisito legal o un requisito necesario para suscribir un contrato, así se indicará y cuando el

tratamiento se base en los intereses legítimos del responsable del tratamiento o de un tercero, conforme al artículo 8 de la Ley 81 de 2019, se detallará cuáles son estos intereses.
4. Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
5. La intención del responsable del tratamiento de transferir datos personales a un tercer país, así como la condición prevista en el artículo 33 de la Ley 81 de 2019 que resulta aplicable.
6. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
7. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.
8. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 19 de la Ley 81 de 2019, y, al menos en tales casos, la información significativa sobre la lógica aplicada, como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
9. Los datos de contacto del oficial de protección de datos personales.

Cuando los datos personales no se hayan obtenido de su titular, el responsable del tratamiento le facilitará, además de la información a que se refiere este artículo, la referente a la categoría de los datos de que se trate y la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

Art. 15. Plazos para facilitar la información. Cuando los datos sean proporcionados por el titular, la información se facilitará en el momento de la recogida de los datos.

Cuando los datos se obtengan de otra fuente, la información se facilitará:
1. Si los datos personales se utilizan para comunicarse con el titular, a más tardar en el momento de la primera comunicación.
2. Si se comunica a otro destinatario, éste deberá informar al titular en la primera comunicación que le dirija.

Art. 16. Forma para facilitar la información. El responsable del tratamiento podrá elegir la forma en la que va a proporcionar la información al titular de los datos siempre que ésta le permita demostrar que cumplió con la obligación de informar.

La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de menores de edad. Podrá utilizarse recursos audiovisuales, cuando sea apropiado, con el fin de proporcionar la información necesaria.

Cuando la información vaya a facilitarse a través de Internet o a través de dispositivos de pantalla reducida, y siempre que así lo considere el responsable del tratamiento, se podrá dar cumplimiento al deber de información mediante un sistema de información dividida en capas. De esta forma la política de privacidad y/o las condiciones de servicios accesibles, a las que se refiere la Ley 81 de 2019, se podrán dividir en capas. En la primera capa se facilitará al afectado la información básica referente a la identidad del responsable del tratamiento, finalidad del tratamiento y posibilidad de ejercer los derechos que le reconoce la Ley 81 de 2019 y se le indicará una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Sección tercera
Condiciones de licitud para el tratamiento

Art. 17. Condiciones de licitud para el tratamiento. Se podrá proceder el tratamiento de los datos cuando se cumplan, al menos, una de las condiciones siguientes:
1. Cuando el titular de los datos haya otorgado su consentimiento previo, inequívoco e informado por un medio que permita al responsable del tratamiento probar la trazabilidad de dicho consentimiento.
2. Cuando el tratamiento tenga lugar en el marco de una relación contractual en la que el titular de datos sea parte o se celebre en su interés.
3. Cuando el tratamiento sea necesario para el cumplimiento de una obligación legal por parte del responsable del tratamiento. En estos casos, la ley que recoja la obligación debe disponer:
   a. La finalidad del tratamiento.
   b. La determinación del responsable o responsables del tratamiento.
   c. Las limitaciones que rigen la licitud del tratamiento por parte del responsable.
   d. Las categorías de datos objeto de tratamiento.
   e. Los titulares de los datos afectados.
   f. Las entidades a las que se pueden comunicar los datos y los fines de la comunicación;
   g. Los plazos de conservación de los datos.

4. Cuando el tratamiento este autorizado en una ley especial o las normativas que las desarrollen. Estas leyes podrán imponer condiciones especiales al tratamiento respetando lo previsto en la Ley 81 de 2019 y el presente decreto.
5. Cuando el tratamiento sea necesario para proteger intereses vitales del titular de los datos o de otra persona natural.
6. Cuando sea requerido por una entidad pública en el ejercicio de sus funciones legales, para la salvaguarda de un interés público o por orden judicial.
7. Cuando el tratamiento sea necesario para satisfacer el interés legítimo perseguido por el responsable del tratamiento o por un tercero, siempre que prevalezcan los intereses o los derechos y libertades fundamentales del titular de los datos, en especial cuando sea un menor de edad. Para justificar el interés legítimo el responsable del tratamiento deberá demostrar que evaluó y ponderó los intereses o derechos involucrados y que adoptó las medidas necesarias para mitigar los riesgos derivados del tratamiento.

   Esta condición de licitud no será aplicable al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.
8. Cuando se trate de datos sensibles, se atenderá a las condiciones previstas en el artículo 13 de la Ley 81 de 2019 para proceder a su transferencia a terceros.

Art. 18. Condiciones para el consentimiento. El consentimiento deberá ir precedido de la información prevista en el artículo 10 del presente decreto, para cumplir las exigencias de ser informado e inequívoco.

El consentimiento deberá obtenerse de forma que permita su trazabilidad. Esto es, cuando el tratamiento se base en el consentimiento del interesado, el responsable del tratamiento deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. Se considera válida la documentación del consentimiento, incluso por vía electrónica o por cualquier otro mecanismo, conforme al medio que se utilice en cada caso para la recogida de los datos, siempre que éste permita demostrar al responsable del tratamiento que el consentimiento fue otorgado.

Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos.

El consentimiento para el tratamiento de datos de salud, así como otros datos sensibles, cuando la ley que los regule lo exija, deberá ser irrefutable y expreso.

En el caso de tratamiento de datos de menores de edad e incapaces, el tratamiento deberá llevarse a cabo con la autorización previa del acudiente, tutor o quien ejerza la guardia y crianza o tutela del menor o incapaz. En estos casos, el responsable del tratamiento deberá demostrar que hizo todos los esfuerzos razonables para verificar esta autorización, teniendo en cuenta el estado de la tecnología disponible en cada momento.

Los datos personales de los menores de edad e incapaces se pueden recopilar sin consentimiento cuando el tratamiento sea necesario para contactar con los padres, acudiente, tutor o quien ejerza la guarda y crianza o tutela del menor o incapaz y únicamente con esta finalidad.

Art. 19. Revocación del consentimiento. El consentimiento podrá ser revocado en cualquier momento. El retiro del consentimiento no afectará la licitud del tratamiento basada en el consentimiento previo a su revocación, salvo las excepciones contenidas en la ley 81 de 2019 y cualquier otra disposición legal aplicable.

Antes de dar su consentimiento, el interesado será informado de ello. Deberá ser tan fácil retirar el consentimiento como otorgarlo.

Art. 20. Fuentes de acceso público. A los efectos de la Ley 81 de 2019, sólo podrán ser consideradas fuentes de acceso público:

1. Las publicaciones estatales de carácter oficial publicadas en Gaceta Oficial.
2. Los medios de comunicación.
3. Los directorios telefónicos en los términos previstos por su normativa específica.
4. Las listas oficiales de profesionales mantenidas por las entidades que los agrupen en lo referente a nombre, título o profesión, actividad, dirección laboral o comercial y pertenencia a la entidad. Los colegios profesionales y demás entidades a las que corresponda elaborar estos listados estarán obligados a atender los derechos de los interesados en dejar constancia de su oposición al uso de sus datos con fines distintos al que responde la elaboración del citado listado.

Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista de profesionales en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su expedición.

Los interesados tendrán derecho a que la entidad responsable del mantenimiento de estos listados indique gratuitamente que se oponen a que sus datos personales puedan utilizarse para fines de mercadeo.

Capítulo II
Derechos de los titulares de datos personales

Art. 21. Disposiciones generales sobre ejercicio de los derechos. Los derechos de los titulares de datos personales podrán ejercerse directamente por el titular de los datos o por medio de representante legal. Será nulo cualquier acto o convenio entre los responsables del tratamiento o custodios de la base de datos y los titulares de los datos que limiten esos derechos.

El responsable del tratamiento establecerá protocolos sencillos, accesibles y gratuitos que permitan al titular de los datos ejercer sus derechos y al responsable del tratamiento dar respuesta en tiempo y forma.

El responsable del tratamiento informará al titular de los datos sobre los medios a su disposición para ejercer los derechos que le correspondan. Los medios deberán ser fácilmente accesibles y el responsable del tratamiento no podrá denegar el derecho por el solo motivo de optar el titular de los datos por otro medio, siempre que no suponga un coste desproporcionado para el responsable del tratamiento.

El solicitante deberá acreditar su identidad en el momento de la solicitud, así como los datos de contacto necesarios para enviarle la respuesta al ejercicio de su derecho. En el caso de ejercicio por medio de representante legal, deberá acompañarse a la solicitud la documentación que acredite la misma conforme al ordenamiento jurídico vigente.

El custodio de la base de datos podrá tramitar, por cuenta del responsable del tratamiento, las solicitudes de ejercicio a los derechos formuladas por los afectados, si así se establece en el contrato o acto jurídico que les vincule.

El responsable del tratamiento deberá dar respuesta al ejercicio de los derechos, incluso cuando no obrasen datos en sus bases de datos relacionados con el solicitante. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de los derechos formulado por el afectado recaerá sobre el responsable del tratamiento.

Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos, se atenderá lo dispuesto en aquellas, siempre que respeten los requisitos que se establecen en la Ley 81 de 2019 y en este decreto.

Cada derecho deberá ejercitarse separadamente sin que el ejercicio de uno excluya a los demás.

Art. 22. Ejercicio de derechos de menores e incapaces. Los padres, madres, acudientes, tutores o quienes ejerzan la guarda y crianza de menores o incapaces podrán ejercitar en su nombre y representación los derechos de acceso, rectificación, cancelación, oposición, portabilidad o cualesquiera otros que pudieran corresponderles en el contexto de la Ley 81 de 2019 y el presente decreto.

Art. 23. Gratuidad de las actuaciones. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, con las limitaciones que este decreto establece y las que dispongan leyes especiales en su caso.

Art. 24. Ejercicio del derecho de acceso del interesado. El titular de los datos tendrá derecho a obtener, del responsable del tratamiento, confirmación de si se están tratando o no datos personales que le conciernen. Si en efecto los datos están siendo tratados, el responsable del tratamiento le indicará lo siguiente:

1. Los fines del tratamiento.
2. Las categorías de datos personales de que se trate.
3. Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales.
4. El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.
5. El derecho al ejercicio de la rectificación o cancelación de datos personales, o a oponerse a dicho tratamiento, o a la portabilidad de los datos.
6. Si los datos personales no se han obtenido del interesado, cualquier información disponible sobre su origen.
7. La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere la Ley 81 de 2019, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.

Art. 25. Identificación de la información solicitada. Cuando el responsable del tratamiento trate una gran cantidad de datos relativos al titular y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que éste solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos.

Art. 26. Ejercicio del derecho de rectificación. Cuando el titular de los datos ejercite el derecho de rectificación deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar la documentación que sustente la inexactitud o el carácter incompleto de los datos objeto de tratamiento.

El responsable del tratamiento comunicará cualquier rectificación de datos personales a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si así lo solicita.

Art. 27. Ejercicio del derecho de cancelación. Cuando el titular de los datos ejercite el derecho de cancelación deberá indicar en su solicitud a qué datos se refiere. Deberá acompañar, cuando sea preciso la documentación que sustente la cancelación.

Procederá la cancelación cuando:

1. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
2. El interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico.
3. El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.
4. Los datos personales hayan sido tratados ilícitamente.
5. Los datos personales deban suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.

El responsable del tratamiento comunicará cualquier cancelación a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si así lo solicita.

Art. 28. Excepciones al ejercicio al derecho de cancelación: No procederá la cancelación solicitada cuando el tratamiento sea necesario:

1. Para el cumplimiento de una obligación legal que requiera el tratamiento de datos que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.
2. Por razones de interés público en el ámbito de la salud pública.
3. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho de cancelación pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.
4. Para la formulación, el ejercicio o la defensa de reclamaciones.

Art. 29. Ejercicio del derecho de oposición. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento, que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto fines de mercadeo, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada actividad de mercadeo. En estos casos los datos personales dejarán de ser tratados para dichos fines.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Art. 30. Ejercicio del derecho de portabilidad. El interesado tendrá derecho a recibir los datos personales que le incumben, en un formato estructurado, genérico, de uso común y lectura mecánica, bien para reutilizarlos para sí mismo, o para transmitirlos a otro responsable del tratamiento sin que el responsable pueda impedirlo.

Son condiciones para el ejercicio de este derecho:

1. Que los datos los haya facilitado el titular directamente al responsable del tratamiento.
2. Que el tratamiento esté basado en el consentimiento o en un contrato.
3. Que sea un volumen relevante de datos y el tratamiento se efectúe por medios autorizados.

El interesado tendrá derecho a que los datos personales se transmitan directamente a él o que el responsable los transmita directamente a otro responsable cuando sea técnicamente posible, por medios seguros e interoperables.

Quedan excluidos de este derecho los datos que deriven de otra condición de licitud para el tratamiento o los que resulten de la elaboración propia del responsable del tratamiento.

Art. 31. Limitaciones al ejercicio de los derechos. Sin perjuicio de las limitaciones indicadas, en los artículos anteriores, podrán limitarse el ejercicio de los derechos del titular de los datos personales, en cualquiera de los siguientes casos:

1. Cuando el tratamiento sea necesario para el cumplimiento de un objetivo de interés público.
2. Cuando el tratamiento impida o entorpezca el debido trámite dentro de un proceso administrativo o judicial o por seguridad del Estado.
3. Cuando sea necesario para el ejercicio de las funciones propias de las autoridades públicas.
4. Cuando sea solicitado por las autoridades judiciales competentes para el aseguramiento del cumplimiento de la ley, con las condiciones previstas en la Ley 81 de 2019.
5. Cuando el responsable del tratamiento acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular.
6. Cuando el tratamiento sea necesario para el cumplimiento de una ley.
7. Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

Capítulo III
Utilización de datos personales

Sección primera
Obligaciones del regulador, del responsable del tratamiento y del custodio de los datos

Art. 32. Obligaciones del regulador o autoridad reguladora. El regulador o autoridad reguladora de cada sector, contará con un período de nueve meses, a partir de la entrada en vigencia del presente decreto, para establecer dentro de su normativa todos los protocolos, procesos y los procedimientos de tratamiento y transferencias segura que deban cumplir los sujetos regulados.

Art. 33. Responsabilidad en el tratamiento. El responsable del tratamiento y el custodio de la base de datos implementarán los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la Ley 81 de 2019 y en el presente decreto. Rendirán cuentas sobre el tratamiento de datos personales en su posesión al titular de los datos y a la autoridad de control.

Para ello, deberán elaborar una ficha técnica que contendrá los protocolos, procesos y procedimientos de gestión y transferencia segura de los datos, que será fiscalizado y supervisado por la autoridad de control.

Los responsables del tratamiento y los custodios de la base de datos podrán adoptar, entre otras, las siguientes medidas:

1. Elaborar protocolos y procesos de protección de datos personales obligatorios y exigibles al interior de la organización del responsable del tratamiento o custodios de la base de datos.
2. Revisar periódicamente los procedimientos de gestión y transferencia segura de los datos personales para determinar las modificaciones que se requieran. Para ello podrán establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
3. Cumplir con las normas o estándares nacionales o internacionales en materia de protección de datos personales.
4. Adoptar mecanismos de autorregulación vinculantes en materia de protección de datos personales.
5. Elaborar y mantener actualizado el registro de bases de datos a que se refiere la Ley 81 de 2019.
6. Evaluar el impacto de los tratamientos de datos a realizar, antes de su ejecución, para garantizar la proporcionalidad minimización de datos en el tratamiento.
7. Establecer protocolos para la atención y respuesta al ejercicio de los derechos por los titulares de los datos.
8. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.
9. Designar a un oficial de protección de datos, que participe de forma adecuada y en tiempo oportuno, en todas las cuestiones relativas a la protección de datos personales.

Art. 34. Deber de confidencialidad. Los responsables del tratamiento y/o los custodios de la base de datos, así como todas las personas que intervengan en cualquier fase del tratamiento de los datos, estarán sujetas al deber de secreto o confidencialidad, respecto de los datos personales objeto de tratamiento a los que tengan acceso por razón de sus funciones. Para tal fin, garantizarán que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad y así lo reflejarán en los protocolos de tratamiento de datos de sus entidades públicas y privadas.

Esta obligación será complementaria al secreto profesional de conformidad con la ley aplicable. Se aplicará durante todo el tiempo que dure el tratamiento y se mantendrá aun cuando hubiese finalizado la relación del empleado o funcionario con el responsable del tratamiento o el custodio de la base de datos.

Art. 35. Registro de las bases de datos. El registro de las bases de datos transferidas a terceros constará por escrito, por cualquier medio, inclusive por medios electrónicos.

Respecto de cada base de datos se dejará constancia en dicho registro de:

1. La identificación de la base de datos.
2. La identificación del responsable de la base de datos.
3. La naturaleza de los datos personales que contiene, esto es, la descripción del universo de personas que comprende la base de datos.
4. Las condiciones de legitimación aplicables.
5. La finalidad o finalidades del tratamiento.
6. Los procedimientos de obtención y tratamiento de los datos.
7. El plazo de conservación de los datos.
8. El destino de los datos y las personas naturales o jurídicas a las que pueden ser transferidos.
9. Las medidas técnicas y organizativas de seguridad adoptadas, al menos un resumen de ellas o la referencia a la política o protocolo donde se describen.
10. Los protocolos aplicables a la base de datos, tales como los referentes a la atención y respuesta del ejercicio de los derechos por los titulares de los datos.
11. La descripción técnica de la base de datos.
12. La identificación y periodo de todas las personas que han ingresado a los datos personales dentro de los quince días hábiles desde que se inicie la actividad.

Los responsables del tratamiento y/o los custodios de la base de datos mantendrán el registro actualizado, de forma que responda con veracidad a la realidad de los tratamientos que se lleven a cabo. Estará a disposición de la autoridad de control cuando ésta lo requiera.

Art. 36. Seguridad de los datos personales. Las medidas técnicas y organizativas deben ser suficientes para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios y tratamiento de los datos personales. Para ello se tomará como referencia las normas o estándares nacionales e internacionales en la materia, así como también los mecanismos de autorregulación vinculantes o cualquier otro mecanismo que se determine adecuado para tales fines.

Para determinar estas medidas, se considerarán los siguientes factores:

1. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
2. El estado de la tecnología.
3. Los costos para la aplicación de las medidas.
4. La naturaleza de los datos personales tratados, en especial, si se trata de datos personales sensibles.
5. El alcance, contexto y las finalidades del tratamiento.
6. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.
7. El número de los titulares afectados.
8. Las posibles consecuencias que se derivarían de una violación de seguridad de los datos para los titulares:
9. Las violaciones de seguridad de los datos previas, ocurridas en el tratamiento de datos personales.

Una vez analizados los riesgos del tratamiento y determinadas las medidas a adoptar, el responsable del tratamiento y/o el custodio de la base de datos llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

La autoridad de control podrá establecer normas técnicas mínimas para hacer aplicables las disposiciones del contenido de este artículo, teniendo en cuenta la naturaleza de la información procesada, las características específicas del tratamiento y el estado actual de la tecnología, especialmente dirigidas a pequeñas y medianas empresas.

Art. 37. Notificación de violaciones de la seguridad de los datos personales. Cuando el responsable del tratamiento tenga conocimiento de una violación de seguridad, entendida ésta como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales, aun cuando ocurra de manera accidental, en cualquier fase del tratamiento y que represente un riesgo para la protección de los datos personales, notificará de inmediato dicho incidente a la autoridad de control y a los titulares afectados.

El custodio de la base de datos deberá informar al responsable del tratamiento de manera inmediata cuando tenga conocimiento de una violación de seguridad.

La notificación que realice el responsable del tratamiento a los titulares afectados estará redactada en un lenguaje claro y sencillo.

La notificación se realizará en el plazo de las setenta y dos horas a partir de que se conozca el incidente y contendrá, al menos, la siguiente información:

1. La naturaleza del incidente.
2. Los datos personales comprometidos.
3. Las acciones correctivas realizadas de forma inmediata.
4. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses.
5. Los medios disponibles al titular para obtener mayor información al respecto.

Art. 38. Documentación de las violaciones de la seguridad de los datos personales. El responsable del tratamiento documentará toda violación de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificado, como mínimo, la siguiente información y conservándola a disposición de la autoridad de control:

1. La fecha en que ocurrió.
2. El motivo de la violación.
3. Los hechos relacionados con ella y sus efectos
4. Las medidas correctivas implementadas de forma inmediata y definitiva.

La autoridad de control verificará la gravedad del incidente y para salvaguardar los derechos de los titulares, podrá ordenar que el responsable del tratamiento adopte medidas, tales como la amplia difusión del hecho en los medios de comunicación y/o medidas para revertir o mitigar los efectos del incidente.

Cuando la violación de seguridad tenga lugar en redes públicas de comunicación, se atenderá también a lo que se establezca en las normas especiales sobre telecomunicaciones, relacionadas con la seguridad pública y la defensa nacional.

Sección segunda
Medidas de responsabilidad para el cumplimiento

Art. 39. Mecanismos de autorregulación vinculante. La autoridad de control impulsará la elaboración de mecanismos de autorregulación vinculantes con el objeto de facilitar el cumplimiento de la Ley 81 de 2019 y este decreto a los responsables del tratamiento y custodios de la base de datos, tomando en cuenta las características específicas de los distintos sectores de la actividad productiva o grupos económicos de empresas.

Quienes promuevan la adopción de un mecanismo de autorregulación vinculante deberán someterlo a la aprobación de la autoridad de control quien deberá resolver en un plazo de cuarenta y cinco días hábiles.

Art. 40. Contenido del mecanismo de autorregulación vinculante. En el contenido de los mecanismos de autorregulación vinculante debe quedar consignado:

1. El cumplimiento de los principios de tratamiento.
2. Los protocolos de información y transparencia con el titular de los datos.
3. Los procedimientos de recogida, tratamiento, transferencias y conservación de los datos.
4. Las condiciones de cumplimiento para las transferencias internacionales de datos.
5. La atención y respuesta al ejercicio de los derechos por los titulares de los datos.
6. Las medidas técnicas y organizativas dirigidas a garantizar la seguridad en el tratamiento y transferencia de los datos.

La adhesión a un mecanismo de autorregulación vinculante supondrá una garantía de cumplimiento para el custodio de la base de datos y para las transferencias internacionales de datos a los efectos previstos en la Ley 81 de 2019.

Una vez aprobados serán publicados en la Gaceta Oficial.

Art. 41. Evaluaciones de impacto relativas a la protección de datos. Atendiendo a la gravedad del riesgo que presente el tratamiento para los datos personales, así como a la novedad de la tecnología utilizada, la Autoridad de Control, podrá ordenar que se presente un informe de evaluación de impacto en protección de datos.

El informe debe contener, como mínimo, una descripción de los tipos de datos recopilados, la metodología utilizada para la recopilación y garantía de seguridad de la información, y el análisis del responsable en relación con medidas, salvaguardas y mecanismos de mitigación de riesgos adoptados.

La autoridad de control podrá solicitar a las entidades que publiquen los informes de evaluación de impacto en protección de datos que lleven a cabo y sugerirles la adopción de normas y buenas prácticas para el tratamiento de datos personales.

Art. 42. Oficial de protección de datos. El oficial de información, que desarrolla la ley 33 de 2013, será también para los efectos de la ley 81 de 2019, y el presente decreto, el oficial de protección de datos personales, para el sector público.

Las entidades privadas, podrán designar un oficial de protección de datos, que podrá ser personal laboral o profesional con contrato de servicios, suscrito con el responsable del tratamiento o el custodio de la base de datos.

La designación de un Oficial de Protección de Datos Personales para el sector privado no es obligatoria, no obstante, si fuera el caso, la autoridad de control la tomará en cuenta como criterio para la graduación de las sanciones.

Art. 43. Perfil del oficial de protección de datos. Para ser oficial de protección de datos se requiere una experiencia profesional previa en la materia y el conocimiento del sector de actividad de la entidad pública y privada en la que ejercerá sus funciones.

La designación del oficial de protección de datos personales se estimará válida por parte de la autoridad de control, sólo cuando el responsable del tratamiento o el custodio de la base de datos lo notifique formalmente y de manera expresa. Lo mismo ocurrirá en el caso de que dicha designación sea revocada.

La autoridad de control, llevará un registro de los oficiales de protección de datos y podrá organizar capacitaciones dirigidas a fortalecer sus funciones.

Art. 44. Desempeño y funciones del oficial de protección de datos. El oficial de protección de datos desempeñará sus funciones con independencia, siendo obligación del responsable del tratamiento o del custodio de la base de datos garantizar esta independencia y evitar cualquier conflicto de interés. Debe tener una interlocución directa con la dirección u órgano de toma de decisión de la entidad a la que representa en esta materia y se le beberán proporcionar los medios necesarios para que pueda cumplir su misión.

Las funciones principales del oficial de protección de datos son:

1. Participar en tiempo y forma en las cuestiones referidas a la protección de datos personales.
2. Informar y asesorar al responsable del tratamiento o al custodio de la base de datos en las cuestiones relacionadas con el cumplimiento de la Ley 81 de 2019, del presente decreto o de cualquier disposición legal aplicable en cada caso.
3. Supervisar el cumplimiento de la normativa. Para ello podrá examinar, a solicitud del responsable del tratamiento o del custodio de la base de datos o por iniciativa propia, tratamientos de datos personales que se estén llevando a cabo y realizar recomendaciones para la adopción de medidas correctoras necesarias cuando los tratamientos analizados no sean conformes con la normativa aplicable.
4. Promover la capacitación de las personas que asuman tareas relacionadas con el tratamiento de los datos personales.
5. Cooperar con la autoridad de control.
6. Ser la unidad de enlace con la autoridad de control.
7. Asesorar al responsable del tratamiento o al custodio de la base de datos en la respuesta a los requerimientos y observaciones formalmente notificados por la autoridad de control.
8. Ser la unidad de enlace con los titulares de los datos para las cuestiones relativas al tratamiento de los datos y a sus derechos.

Art. 45. Límite de la responsabilidad del oficial de protección de datos personales. El oficial de protección de datos personales no tendrá la consideración de responsable del tratamiento o custodio de la base de datos por prestar sus servicios en la entidad correspondiente.

Sección tercera
Relaciones del responsable del tratamiento con terceros

Art. 46. Solicitud de transferencia de datos personales. La solicitud de transferencias de datos será documentada. Para ello, el responsable del tratamiento que transfiere y el que recibe, deberá dejar constancia de la solicitud y de la recepción de los datos transferidos, conforme a las obligaciones que a cada uno le corresponden en la Ley 81 de 2019 y el presente decreto.

En el caso de las solicitudes de transferencia de datos personales por las autoridades judiciales competentes, será necesario que la solicitud cumpla con el principio de proporcionalidad y se limite a los mínimos datos personales que sean necesarios para conocer del cumplimiento de la ley que se esté conociendo.

Art. 47. Contrato de custodio de la base de datos. El responsable del tratamiento elegirá únicamente un custodio de la base de datos que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la Ley 81 de 2019, del presente decreto y se garantice la protección de los derechos del titular de los datos.

Se entenderán por garantías suficientes, entre otras, contar con un mecanismo de autorregulación vinculante; haber designado un oficial de protección de datos; contar con una certificación en materia de seguridad de los datos personales o haberse sometido a una auditoria de cumplimiento por parte del responsable del tratamiento.

El responsable del tratamiento y el custodio de la base de datos dejarán constancia por escrito o por cualquier medio admisible como prueba, inclusive por medios electrónicos, el contenido del mandato que implique tratamiento de datos por cuenta del responsable del tratamiento.

Art. 48. Contenido del contrato de custodio de la base de datos. Se estipularán, entre otras, las siguientes condiciones:

1. El tratamiento de los datos personales conforme a las instrucciones, debidamente documentadas, del responsable del tratamiento.
2. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
3. La obligación de informar al responsable del tratamiento cuando ocurra una violación de la seguridad de los datos personales que trata según sus instrucciones.
4. La confidencialidad respecto de los datos personales tratados.
5. La prohibición de transferir datos personales, salvo que el responsable lo solicite o la transferencia derive de una subcontratación autorizada por el responsable del tratamiento.
6. La información que el custodio deba poner a disposición del responsable para que éste pueda acreditar el cumplimiento de sus obligaciones.
7. La colaboración con el responsable del tratamiento en todo lo relativo a garantizar el cumplimiento, en particular, en cuanto a la atención y respuesta al ejercicio de los derechos.
8. La eliminación, devolución o comunicación, al responsable del tratamiento o a un nuevo custodio de la base de datos designado por el responsable del tratamiento, los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable del tratamiento, excepto que una ley exija la conservación de los datos personales. En este caso, los datos serán devueltos al responsable del tratamiento que garantizará su conservación por el tiempo establecido en la Ley 81 de 2019 o en otras leyes especiales.

Art. 49. Responsabilidad del custodio de la base de datos. El custodio de la base de datos no recurrirá a otro custodio, sin la autorización previa por escrito, específica o general, del responsable del tratamiento. En este último caso, el custodio de la base de datos informará al responsable del tratamiento de cualquier cambio previsto en la incorporación o sustitución de otros custodios, dándole así la oportunidad de oponerse a dichos cambios.

Cuando un custodio de la base de datos recurra a otro custodio para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable del tratamiento, se impondrán a este otro custodio las mismas obligaciones de protección de datos personales que las estipuladas entre el responsable y el custodio inicial. Se dejará constancia por escrito, por cualquier medio de prueba admisible. Si ese otro custodio incumple sus obligaciones de protección de datos personales, el custodio inicial de la base de datos inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones.

Art. 50. Contratos de responsabilidad solidaria. Cuando la base de datos sea alimentada por dos o más responsables que determinen conjuntamente los objetivos y los medios del tratamiento serán considerados, responsables solidarios del tratamiento. Los responsables solidarios determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la Ley 81 de 2019 y el presente decreto, en particular en cuanto al ejercicio de los derechos del titular y a sus respectivas obligaciones de suministro de información a que se refiere el artículo 10 del presente decreto, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por la ley que les sea aplicable. Dicho acuerdo podrá designar un punto de contacto para los titulares de los datos.

El acuerdo indicado en este artículo establecerá debidamente las funciones y relaciones respectivas de los responsables solidarios en relación con los titulares de los datos. Se pondrán a disposición de los titulares de los datos los aspectos esenciales del acuerdo.

Indistintamente del acuerdo en la determinación de los objetivos y los medios del tratamiento, los titulares de los datos personales podrán ejercer los derechos que se les reconoce en la Ley 81 de 2019 frente a, y en contra de, cada uno de los responsables del tratamiento.

Sección cuarta
Transferencias extrafronterizas de datos

Art. 51. Condiciones para las transferencias extrafronterizas de datos. Los datos objeto de tratamiento podrán ser transferidos a otro país siempre que se reúna alguna de las condiciones siguientes:

1. Para países u organizaciones internacionales que brindan un grado de protección de datos personales equivalente o superior al previsto en la Ley 81 de 2019 y el presente decreto;
2. Cuando el responsable ofrece y prueba garantías adecuadas de cumplimiento de los principios, los derechos del titular y el régimen de protección de datos personales previsto en la Ley 81 de 2019 y el presente decreto.
3. Consentimiento del titular de los datos

4. Necesaria para la prevención o diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.
5. Necesaria para la salvaguarda del interés público o para la representación legal del titular de los datos personales o administración de justicia.
6. Necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o en casos de colaboración judicial internacional.
7. Necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos.
8. Que sea requerida para concretar transferencias bancarias o bursátiles en lo relativo a las transacciones respectivas y conforme a la legalización que les resulte aplicable.
9. Que tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el lavado de activos, los delitos informáticos, la pornografía infantil y el narcotráfico.
10. Cuando concurra alguna de las demás condiciones previstas en la Ley 81 de 2019.

Art. 52. Nivel de protección equivalente o superior. Para evaluar el cumplimento de la condición que establece el numeral 1 del artículo anterior, la autoridad de control, tomará en cuenta los criterios siguientes:

1. El respeto a los derechos humanos y las libertades fundamentales.
2. Las normas generales y sectoriales de la legislación vigente en el país de destino o en la organización internacional o supranacional;
3. La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país receptor o a las cuales esté sujeta una organización internacional o supranacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos personales, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y
4. Los compromisos internacionales asumidos por el país receptor u organización internacional o supranacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

   La autoridad de control podrá publicar el listado de destinos que reúnan estas condiciones.

Art. 53. Garantías adecuadas. Son garantías adecuadas para la transferencia de datos personales extrafronterizos los siguientes:

1. Las cláusulas contractuales suscritas entre el exportador y el destinatario que ofrezcan garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares.
2. Los modelos de cláusulas contractuales que valide la autoridad de control para ser utilizadas por exportador y destinatario como garantía de la transferencia.
3. Los mecanismos de autorregulación vinculante convenidos entre el exportador y el destinatario y aprobado por la autoridad de control o reconocida por ésta, siempre y cuando éstos sean acordes con las disposiciones previstas en la Ley 81 de 2019 y el presente decreto. La autoridad de control podrá promulgar el listado de mecanismos de autorregulación vinculantes que se reconocen a estos efectos.
4. Si el exportador y el destinatario pertenecen al mismo grupo económico y los tratamientos queden sujetos a unas normas corporativas que les vinculen.

Capítulo IV
Autoridad de control

Art. 54. Autoridad de control. La Autoridad Nacional de Transparencia y de Acceso a la Información, a través de la Dirección de Protección de Datos Personales, es el organismo rector en materia de protección de datos personales. Contará con el apoyo de la Autoridad Nacional para la Innovación Gubernamental, cuando se trate de aspectos relacionados con las Tecnologías de la Información y las Comunicaciones.

La Dirección de Protección de Datos Personales, resolverá, las quejas y peticiones presentadas a la Autoridad de Control. Sus decisiones pueden ser impugnadas mediante recurso de reconsideración ante la misma o de apelación que se interpondrá ante el Director General de la Autoridad Nacional de Transparencia y Acceso a la Información.

Art. 55. Composición de la Dirección de Protección de Datos Personales. La Dirección de Protección de Datos Personales deberá estar dotada de perfiles de nivel asesor y de nivel técnico para el desempeño de sus funciones.

Art. 56. Miembros de la Dirección de Protección de Datos Personales. Formarán parte de la Dirección de Protección de Datos Personales los servidores públicos que la Dirección General de autoridad de control designe.

Cada miembro de la Dirección de Protección de Datos Personales poseerá la titulación, la experiencia, la idoneidad y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de las atribuciones y el ejercicio de las facultades descritas para su puesto.

Los servidores públicos asignados a la Dirección de Protección de Datos Personales desempeñarán sus funciones conforme al deber de confidencialidad.

Sección primera
Designación y composición

Art. 57. Atribuciones y facultades de la autoridad de control. La Autoridad Nacional de Transparencia y Acceso a la Información, como autoridad de control, tiene las siguientes atribuciones y facultades, que serán ejercidas por la Dirección General:

1. Velar por la debida reserva y protección de los datos personales en poder del Estado o de las entidades privadas.
2. Promover la sensibilización de responsables del tratamiento y custodios de las bases de datos sobre las obligaciones que les incumben en la materia. Para ello podrá realizar, directamente o a través de terceros, actividades de capacitación de servidores públicos en materia de protección de datos personales. Igualmente podrá promover capacitaciones para responsables y custodios del tratamiento del sector privado con el objetivo de contribuir a la difusión y conocimiento de la normativa aplicable y de su interpretación. A tal fin podrá celebrar convenios con entidades reguladoras, empresas y sectores de actividad.
3. La sensibilización del público para la comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de sus datos personales. A tal fin, podrá recibir informes, recomendaciones, observaciones y sugerencias que aporten los ciudadanos o la sociedad civil relacionadas con la protección de los datos personales y atenderlos e impulsarlos en las entidades involucradas para su atención.
4. Asesorar a las entidades del Estado sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas naturales con respecto al tratamiento de datos personales; a tal fin emitirá dictámenes sobre cualquier asunto relacionado con la protección de los datos personales, pudiendo llevar a cabo una previa evaluación de impacto en protección de datos cuando se requiera para garantizar la proporcionalidad y minimización de los datos personales previstas en dichas medidas legislativas y administrativas.
5. Solicitar el apoyo de la Autoridad Nacional para la Innovación Gubernamental, cuando se trate de aspectos relacionados a las tecnologías de la información y la comunicación.

   Estas atribuciones y facultades podrán ser delegadas a la Dirección de Protección de Datos Personales.

Art. 58. Atribuciones y facultades de la Dirección de Protección de Datos Personales. Sin perjuicio de las atribuciones y facultades que le pudiera delegar la Dirección General, conforme al artículo anterior del presente decreto, la Dirección de Protección de Datos Personales tiene las siguientes:

1. Fiscalizar y supervisar:
   a. Realizar evaluaciones, informes y análisis de procedimientos en los que se realicen tratamientos de datos personales a todos los responsables o custodios del tratamiento de los datos para lo cual podrá solicitarles, a través del oficial de protección de datos personales, información, documentación y certificaciones de sus bases de datos, las cuales no podrán ser negadas; adoptar modelos de cláusulas contractuales que, conforme al artículo 33 de la Ley 81 de 2019, constituyan una condición de licitud de las transferencias de datos, intra y extrafronterizas.
   b. Aprobar mecanismos de autorregulación vinculantes de conformidad con lo dispuesto en el artículo 33 de la Ley 81 de 2019 y en el artículo 38 del presente decreto.
   c. Llevar a cabo inspecciones sectoriales, por iniciativa propia o a petición de terceros, que le permitirán evaluar el cumplimiento de la Ley 81 de 2019 y el presente decreto. La autoridad de control podrá apoyarse en la colaboración de las entidades reguladoras del sector de actividad, en su caso. Y, en todo caso, con el apoyo de la Autoridad Nacional para la Innovación Gubernamental, cuando se trate de aspectos relacionados con las Tecnologías de la Información y la Comunicación.
   d. Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos reconocidos en el artículo 15 de la Ley 81 de 2019.
2. Sancionar:
   a. Al responsable del tratamiento, así como al custodio de la base de datos por las infracciones de la Ley 81 de 2019.
   b. En el caso de faltas leves, la citación tendrá por objeto que el responsable o custodio exponga los motivos del incumplimiento. Una vez analizados los motivos, la autoridad de control podrá darle un plazo hasta de quince días hábiles para que le sea remitido lo requerido.

c. Sancionar a todo responsable del tratamiento, así como al custodio de la base de datos con una multa aplicando los criterios de graduación previstos en el presente decreto.
d. En el caso de faltas muy graves, la opinión formal del Consejo de Protección de Datos Personales será orientativa y no tendrá carácter vinculante.
e. Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del titular de los datos reconocidos en el artículo 15 de la Ley 81 de 2019.

Sección Segunda
Poderes correctivos

Art. 59. Responsables. Los responsables del tratamiento y/o custodios de las bases de datos son responsables del cumplimiento y quedan sujetos a la fiscalización y supervisión de la autoridad de control a través de la Dirección de Protección de Datos Personales.

Art. 60. Procedimiento en caso de vulneración de la normativa de protección de datos personales. El procedimiento administrativo sancionador se regirá por las normas generales previstas en la Ley 38 de 2000 y las que resulten aplicables en su caso.

Art. 61. Publicidad de las sanciones. Ejecutoriada la sanción impuesta a los responsables del tratamiento o custodios de la base de datos, la autoridad de control podrá poner en conocimiento de la opinión pública, por cualquier medio, el contenido de sus resoluciones, cuando lo considere útil y oportuno para informar sobre una práctica irregular y falta de cooperación.

Art. 62. Criterios de graduación de las sanciones. Las sanciones previstas en los numerales 2 y 3 del artículo 43 de la Ley 81 de 2019 se aplicarán teniendo en cuenta los criterios de graduación siguientes:
1. La intencionalidad.
2. La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución en firme.
3. La naturaleza y cuantía de los perjuicios causados.
4. En plazo de tiempo durante el que se haya venido cometiendo la infracción.
5. El beneficio que haya reportado al infractor la comisión de la infracción.
6. El volumen de la facturación a que afecte la infracción cometida.
7. La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
8. La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
9. La afectación a los derechos de los menores de edad.
10. El haber designado un oficial de protección de datos personales.
11. La adopción reiterada y demostrada de mecanismos y procedimientos internos capaces de minimizar el daño, dirigidos al tratamiento seguro y adecuado de los datos, como, por ejemplo: la adopción de una política de buenas prácticas y gobernanza.
12. La pronta adopción de medidas correctivas.
13. La proporcionalidad entre la gravedad de la falta y la intensidad de la sanción.

Art. 63. Prescripción de la acción. La acción de las infracciones tipificadas en la Ley 81 de 2019 prescriben en los siguientes plazos:
1. Las infracciones leves, prescriben en el plazo de un año.
2. Las infracciones graves prescriben en el plazo de tres años.
3. Las infracciones muy graves prescriben en el plazo de cinco años.

El plazo de prescripción de las infracciones comenzará a correr el día siguiente al que se haya cometido la acción que motiva la infracción.

Se interrumpe la prescripción de la infracción por el inicio de la investigación o del procedimiento sancionador.

Art. 64. Prescripción de la sanción. Las sanciones impuestas con arreglo a la Ley 81 de 2019 prescriben en los siguientes plazos:
1. Las sanciones leves prescriben en un plazo de tres años.
2. Las sanciones graves prescriben en un plazo de cinco años.
3. Las sanciones muy graves son imprescriptibles.

El plazo de prescripción de las sanciones comenzará a correr el día siguiente al que se haya impuesto.

Se interrumpe la prescripción de la sanción por cualquier acto que tienda a la ejecución de la resolución que la impuso.

Art. 65. Entrada en vigencia. Este Decreto Ejecutivo comenzará a regir a partir de su promulgación.

Fundamento de derecho: Constitución Política de la República; Ley 38 de 31 de julio de 2000, Ley 33 de 25 de abril de 2013 y Ley 81 de 26 de marzo de 2019.

COMUNÍQUESE Y CÚMPLASE.