N° 904

GUILLERMO LASSO MENDOZA

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

CONSIDERANDO:

Que el numeral 11 del artículo 66 de la Constitución de la República reconoce y garantiza el derecho a guardar reserva sobre sus convicciones;

Que el numeral 19 del artículo 66 de la Constitución de la República reconoce y garantiza el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección;

Que el numeral 13 del artículo 147 de la Constitución de la República faculta al Presidente de la República a expedir los reglamentos necesarios para la aplicación de las leyes, sin contravenirlas ni alterarlas, así como los que convengan a la buena marcha de la administración;

Que en el Quinto Suplemento del Registro Oficial No. 459 de 26 de mayo de 2021, se expidió la Ley Orgánica de Protección de Datos Personales, en cuyo artículo 2 se dispone que la Ley regula el tratamiento de datos personales contenidos en cualquier tipo de soporte;

Que es necesario emitir el Reglamento a la Ley Orgánica de Protección de Datos Personales para establecer con claridad los preceptos y procedimientos para la ejecución de la Ley; y,

En ejercicio de las funciones conferidas en el numeral 13 del artículo 147 de la Constitución de la República, expide el siguiente:

REGLAMENTO GENERAL DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I
GENERALIDADES

Artículo 1.- Objeto.- El presente Reglamento General tiene por objeto desarrollar la normativa para la aplicación de la Ley Orgánica de Protección de Datos Personales y la protección de los derechos y libertades fundamentales de los titulares de datos personales.

Artículo 2.- Ámbito.- Este Reglamento se aplica a todas las personas naturales y jurídicas, nacionales y extranjeras, del sector público y privado, que realicen tratamiento de datos personales, en el contexto de que sus actividades como responsable o encargado de tratamiento de datos personales, tenga lugar en el territorio ecuatoriano o no.

El presente Reglamento también se aplica al tratamiento de datos personales por parte de personas naturales y jurídicas, que actúen como responsables y encargados del tratamiento de datos personales de titulares no residentes en Ecuador, cuando sus actividades de tratamiento sean realizadas en territorio nacional.

El presente Reglamento aplicará para los responsables y encargados del tratamiento de datos personales no establecidos en territorio ecuatoriano a quienes les resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público. Estos deberán designar a un apoderado especial de acuerdo con el artículo 3 de este Reglamento

Artículo 3.- De la obligación de contar con poder de los responsables y/o encargados del tratamiento de datos de residentes ecuatorianos fuera del territorio nacional.- Los responsables y encargados del tratamiento de datos personales no establecidos en el Ecuador deberán designar a un apoderado especial, de conformidad con las siguientes reglas:

1. Cuando el responsable y/o encargado del tratamiento de datos personales no tenga domicilio en territorio nacional, conforme el Articulo 3, numeral 3 de la Ley Orgánica de Protección de Datos Personales, deberán designar un apoderado especial en el Ecuador con residencia en el país, que cuente con facultades suficientes para comparecer a nombre de su representado ante instancias administrativas y judiciales en la materia.
2. De forma excepcional, no será necesaria la designación de dicho apoderado o representante, cuando el tratamiento de datos personales sea ocasional y no incluya el manejo a gran escala de datos personales de categoría especial establecidos en el artículo 25 de la Ley y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas naturales, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento.

La Autoridad de Protección de Datos Personales emitirá una guía técnica respecto de la aplicabilidad de los criterios anteriores.

Artículo 4.- Definiciones.- Sin perjuicio de lo dispuesto en la Ley, para efectos de la aplicación del presente Reglamento, se establecen las siguientes definiciones:

1. **Actividades familiares o domésticas:** aquellas en las cuales el tratamiento de los datos personales se dé en un entorno de amistad, parentesco o grupo personal cercano, en propiedad privada, y que no tenga como finalidad su comunicación o transferencia con fines comerciales.
2. **Datos relativos a la salud:** La definición de datos de salud establecida en la Ley comprende la información relativa a todos los aspectos de salud, tanto físicos como psíquicos, de la persona. Se incluyen todos los datos relativos al estado de salud del titular que dan información sobre su estado de salud física o mental pasado, presente o futuro. Así también contiene la información sobre la persona natural recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia; todo número, símbolo o dato asignado a una persona natural que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del titular, independientemente de su fuente.
3. **Normas corporativas vinculantes:** Las políticas o códigos de conducta jurídicamente vinculantes dentro de un grupo de empresas o en una unión de empresas que tienen la finalidad de ofrecer garantías suficientes cuando los datos personales van a ser transferidos internacionalmente a uno o varios responsables o encargados del tratamiento que están en un tercer país sin nivel adecuado.
4. **Persona Identificable:** se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.
5. **Representante:** Persona natural o jurídica establecida en el territorio ecuatoriano que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 3, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud de la Ley Orgánica de Protección de Datos Personales y al presente Reglamento.

6. **Tercero:** Persona natural o jurídica, autoridad pública, servicio u organismo distinto del titular, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable.
7. **Tratamiento a gran escala:** es aquel que afecta a una gran cantidad de datos, referentes a un elevado número de titulares, procedentes de una amplia diversidad geográfica, y que pueden entrañar un riesgo a sus derechos y libertades. Para determinar cuándo se está en presencia de un tratamiento "*a gran escala*" la Autoridad de Protección de Datos Personales y los responsables del tratamiento deberán tener en cuenta los siguientes aspectos:

   a. El número de interesados o titulares, bien como cifra concreta o como proporción de la población correspondiente;
   b. El volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
   c. La duración o permanencia de la actividad de tratamiento de datos; y,
   d. El alcance geográfico de la actividad de tratamiento.

   Se considera tratamiento a gran escala:

   a. El tratamiento de datos de pacientes en el desarrollo normal de la actividad de un hospital, o de las instituciones que conforman el Sistema Nacional de Salud;
   b. El tratamiento de datos de desplazamiento de las personas que utilizan el sistema de transporte público de una ciudad (p. ej. seguimiento a través de tarjetas de transporte);
   c. El tratamiento de datos de geolocalización en tiempo real de clientes por parte de un responsable del tratamiento de datos personales especializado en la prestación de estos servicios;
   d. El tratamiento de datos de clientes en el desarrollo normal de la actividad de una compañía de seguros, corredores, agentes, prestadores o de instituciones financieras;
   e. El tratamiento de datos personales para publicidad comportamental por un motor de búsqueda; y,
   f. El tratamiento de datos (contenido, tráfico, ubicación) por proveedores de servicios de telefonía o internet.

Artículo 5.- De la recogida del consentimiento.- El responsable de datos personales deberá obtener el consentimiento del titular de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.

En todos los casos en los que de conformidad con la Ley se requiera el consentimiento explícito del titular para el tratamiento de sus datos, el responsable deberá informar previa y detalladamente los tipos de tratamiento, finalidades, el tiempo de conservación, las medidas de protección a adoptarse, las consecuencias de su entrega, entre otros aspectos determinados en la Ley, lo cual deberá ser consentido inequívocamente por el titular.

El consentimiento del titular deberá reflejar de manera indubitada la aceptación de éste en relación con el tratamiento de sus datos personales a través de una declaración, pronunciamiento para darse de baja o clara acción afirmativa. El consentimiento otorgado por el titular deberá ser demostrado por el responsable que lo obtiene, cuando así sea requerido por la autoridad competente.

Cuando los datos personales recogidos pertenecen a un incapaz, bastará con el consentimiento del representante legal debidamente acreditado ante el responsable, en los términos señalados en el presente artículo. El consentimiento de niñas, niños y adolescentes y, en general, de personas incapaces, se obtendrá a través de sus representantes legales y curadores, según lo dispuesto en la Ley Orgánica de Protección de Datos Personales y el Código Civil.

El silencio o la inacción, por sí solos, no presumen el consentimiento del titular.

Artículo 6.- De la revocatoria del consentimiento.- El titular tendrá derecho a retirar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará a la licitud del tratamiento de datos llevado a cabo hasta el momento de la revocatoria. El responsable del tratamiento deberá contar con un procedimiento sencillo para que el titular pueda revocar su consentimiento.

El responsable del tratamiento deberá suspender el tratamiento de los datos del titular que haya revocado su consentimiento, una vez recibida la notificación por parte del titular.

Artículo 7.- Tratamiento legítimo.- Para efectos del correcto tratamiento de datos personales, se considerará lo siguiente:

1. **Cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos:** Se entenderá que el tratamiento de datos personales está basado en el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos, debidamente motivado y de acuerdo con los principios establecidos en la Ley, cuando la competencia correspondiente esté atribuida en una norma con rango de ley.

   El tratamiento de datos personales realizado sobre esta base legitimadora deberá observar lo siguiente:

   a. Los tipos de datos objeto del tratamiento;
   b. Los titulares o interesados afectados;
   c. Las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación;
   d. La limitación de la finalidad;
   e. Los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo.

   El tratamiento de datos personales bajo esta base legitimadora deberá cumplir un objetivo de interés público y ser proporcional al fin legítimo perseguido.

2. **Intereses vitales del interesado o de otra persona:** Será lícito el tratamiento de datos personales si es necesario para proteger un interés esencial para la vida del interesado o de otra persona, como epidemias o situaciones de emergencia humanitaria. Los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física, cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente.

3. **Interés legítimo del responsable:** En el caso de que sea necesario satisfacer un interés legítimo del responsable del tratamiento o de un tercero interesado, se aplicará la regla de ponderación, siempre que no prevalezcan los intereses o derechos y libertades del titular.

La ponderación se realizará a través de una evaluación meticulosa que atienda los siguientes factores:

a. Evaluación del interés legítimo del responsable del tratamiento o del tercero interesado que deberá ser necesario y proporcionado;

b. Impacto sobre los titulares que mida las consecuencias reales o potenciales derivadas del tratamiento;

c. Equilibrio provisional, que contemple las medidas adoptadas por el responsable del tratamiento para cumplir sus obligaciones en términos de proporcionalidad y transparencia; y,

d. Garantías adicionales aplicadas por el responsable del tratamiento para impedir cualquier impacto indebido sobre los titulares.

4. **Fuente accesible al público:** Para el tratamiento de datos personales que consten en bases de datos de acceso público, se considerará que los datos deben ser obtenidos de fuentes accesibles al público, según la definición de la Ley y el presente Reglamento, respetando el principio de limitación de la finalidad, atendiendo a las razones concretas que han determinado la publicación de la información, especialmente cuando dicha publicación se realiza en cumplimiento de una obligación legal o por razones de interés público.

Consecuentemente, el tratamiento de los datos personales obtenidos de fuentes accesibles al público requiere que la finalidad pretendida con el nuevo tratamiento sea compatible con la finalidad que justificó la publicación de los datos, por lo que el hecho de que los datos figuren en fuentes públicas no determina la posibilidad de realizar un tratamiento indiscriminado por parte de los responsables.

CAPÍTULO II
CONSERVACIÓN DE DATOS PERSONALES

Artículo 8.- Plazos de conservación de los datos personales.- Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean estrictamente necesarios para el cumplimiento de las finalidades que justificaron el tratamiento.

La Autoridad de Protección de Datos regulará los plazos de conservación de datos personales atendiendo las disposiciones aplicables a la materia de que se trate.

Artículo 9.- Eliminación, bloqueo o anonimización.- Una vez cumplida la o las finalidades del tratamiento y cuando no exista disposición legal o reglamentaria o no incurra la necesidad de mantener los datos en virtud del interés legítimo del responsable, o por cumplimiento de una obligación legal que establezca lo contrario, el responsable deberá proceder a la eliminación, bloqueo o anonimización de los datos en su posesión.

El responsable establecerá procedimientos para la conservación, revisión periódica, eliminación de los datos personales.

Artículo 10.- Fichero de registro.- El fichero del registro de la base de datos deberá contener obligatoriamente el plazo de conservación de los datos, que deberá observar necesariamente la materia, naturaleza del dato, su tratamiento y finalidad.

Artículo 11.- Eliminación de datos.- Finalizado el plazo de conservación de los datos, el responsable del tratamiento de datos deberá proceder a la eliminación segura de los mismos.

La eliminación de datos personales no aplicará cuando el tratamiento sea necesario en los siguientes supuestos:

1. Por razones de interés público en el ámbito de la salud pública y privada, así como en materia estatal, seguridad, laboral y educación;
2. Para la formulación, el ejercicio o la defensa de reclamaciones.

La Autoridad de Protección de Datos Personales podrá requerir información cuando lo considere necesario. Para el efecto, ajustará los requerimientos a normas, lineamientos sobre plazo de conservación y estándares internacionales sobre la eliminación de datos.

CAPÍTULO III
DERECHOS

Artículo 12.- Medios para el ejercicio de los derechos.- Para efectivizar el ejercicio de los derechos establecidos en la Ley Orgánica de Protección de Datos Personales, el responsable habilitará, preferentemente, herramientas o canales informáticos simplificados de fácil acceso para el titular, con la finalidad de receptar y atender

oportunamente las solicitudes o peticiones formuladas que permitan y garanticen una interacción segura, fiable y rápida entre el responsable y el titular, sin perjuicio de que también puedan ser presentadas por medios físicos.

Por lo tanto, se podrán habilitar plataformas digitales, centros de contacto, líneas telefónicas u otros mecanismos tecnológicos que se consideren idóneos para la presentación de las solicitudes por parte de los titulares.

En todos los casos, el requirente deberá demostrar la titularidad o la representación legal para ejercer el derecho.

Artículo 13.- Contenido de la solicitud.- En la solicitud para el ejercicio de los derechos consagrados en la Ley, se hará constar:

1. Los nombres y apellidos completos del titular, número de cédula de identidad o pasaporte y dirección domiciliaria o electrónica para notificaciones. Cuando se actúa en calidad de representante legal, se hará constar también los datos de la o del representado;
2. De ser posible, la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados y cualquier otro elemento o documento que facilite la localización de los datos personales;
3. Relación de lo que solicita expuesto de manera clara y precisa;
4. Derecho o derechos que desea ejercer; y,
5. A la solicitud se acompañará los documentos que acrediten la identidad o, en su caso, la representación legal o convencional del titular.

Artículo 14.- Requerimiento de información adicional.- En caso de que la información constante en la solicitud requiera ser aclarada o ampliada, el responsable podrá requerir al titular, por una sola vez y dentro del término de cinco (5) días de recibida la solicitud, que la aclare o complete.

El titular emplazado contará con el término de diez (10) días contados a partir del día siguiente en el que haya sido notificado, para aclarar o completar la solicitud.

Si el titular aclara o completa la solicitud dentro del término concedido, el responsable le dará la debida atención, caso contrario, la archivará notificando este particular al titular

con las razones de su decisión. El archivo del requerimiento inicial no impedirá la presentación de una nueva solicitud.

Artículo 15.- Registro de solicitudes.- El responsable deberá registrar todas las solicitudes de ejercicio de derechos, incluyendo el detalle de la atención dada a las mismas. La Autoridad de Protección de Datos determinará el contenido de dichos registros.

Artículo 16.- Reclamo ante la Autoridad de Protección de Datos Personales.- El titular de datos personales que encuentre motivos para creer que se han vulnerado sus derechos con la respuesta que el responsable ha dado a su solicitud, o que no haya recibido respuesta en el plazo establecido, podrá acudir a la Autoridad de Protección de Datos a presentar su reclamo, el cual se sustanciará conforme al procedimiento previsto en el Código Orgánico Administrativo y en la normativa complementaria que, para el efecto, emita la Autoridad de Protección de Datos.

El procedimiento de reclamo contemplará la debida notificación al responsable a fin de que ejerza su derecho a la defensa.

CAPÍTULO IV
DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS

Artículo 17.- De los datos de personas fallecidas.- A efectos de que los titulares de derechos sucesorios, o las personas o instituciones que el fallecido haya designado expresamente para ello, puedan ejercer los derechos de acceso, rectificación, actualización y eliminación de los datos del fallecido ante el responsable del tratamiento, según lo dispuesto en la Ley, deberán acreditar su comparecencia a través de los instrumentos legales reconocidos por el ordenamiento jurídico ecuatoriano.

Los derechos podrán ser ejercidos las veces que se considere oportuno, dentro de las limitaciones que plantea la normativa vigente para el ejercicio de derechos por parte de los titulares de los datos personales.

Artículo 18.- De los datos crediticios.- A efectos de lo dispuesto en la Ley, será lícito el tratamiento de datos personales que tenga como fin informar sobre el cumplimiento o incumplimiento de obligaciones comerciales o crediticias. La Junta de Política y

Regulación Financiera, como organismo de regulación, y la Superintendencia de Bancos, como organismo de control, regularán la protección de los datos crediticios, en el ámbito de sus competencias.

Artículo 19.- De los datos de menores de edad.- De conformidad con lo previsto en la Ley Orgánica de Protección de Datos Personales, para el tratamiento de datos personales de menores de 15 años de edad, se requerirá el consentimiento de su representante legal.

Para el tratamiento de datos sensibles, así como para las decisiones basadas en valoraciones automatizadas de menores de edad, se requerirá el consentimiento expreso de su representante legal.

Los adolescentes a partir de los 15 años de edad podrán otorgar su consentimiento explícito para el tratamiento de sus datos personales. Para este efecto, el responsable deberá proporcionar información clara, en un lenguaje sencillo propio de su edad, utilizando métodos que le permitan entender lo que ocurrirá con sus datos personales, las finalidades que se persiguen, los derechos que tiene y cómo ejercerlos y cualquier otra información necesaria para obtener su consentimiento explícito.

También podrá otorgar el consentimiento del adolescente mayor de 15 años, quien ejerce la representación legal, sin perjuicio de que el adolescente, en cualquier momento, pueda revocar este consentimiento. El representante legal del adolescente no podrá revocar el consentimiento otorgado explícitamente por el adolescente en su calidad de titular.

Artículo 20.- Del interés superior del niño.- El consentimiento obtenido para el tratamiento de datos personales de un menor de edad, no podrá, bajo ninguna circunstancia, menoscabar el interés superior de la niña, niño o adolescente, conforme a las disposiciones del Código de la Niñez y Adolescencia y demás normativa vigente. De identificarse aquello, el consentimiento obtenido será considerado inválido.

CAPÍTULO V
TRANSFERENCIA O COMUNICACIÓN DE DATOS A TERCEROS

Artículo 21.- Transferencia de datos personales a un tercero.- La transferencia o comunicación de datos personales a un tercero o encargado requerirá el consentimiento del titular, a menos que, previo a realizar la misma, se han disociado los datos, se han

utilizado mecanismos de cifrado robustos de los datos u otros mecanismos orientados a la privacidad e intimidad de los titulares de los datos personales; de manera que no se pueda identificar a qué persona se refieren.

Artículo 22.- Supuestos para la transferencia de datos a terceros.- La transferencia o comunicación de datos personales a terceros se podrá realizar siempre que concurran los siguientes supuestos:

1. Para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del tercero destinatario, en cuyo caso el destinatario se obliga a cumplir con la normativa de protección de datos; y,
2. Cuando se cuente con el consentimiento previo del titular, el cual puede ser revocado en cualquier momento.

No se requerirá el consentimiento del titular en los supuestos previstos en la Ley.

Artículo 23.- Ejercicio de derechos en los casos de transferencia de datos a terceros.- El titular de los datos personales ejercerá los derechos de rectificación, actualización, oposición y eliminación, directamente ante el responsable del tratamiento, quien, a su vez, deberá notificar de aquello al tercero destinatario de la comunicación de datos personales para que proceda con la rectificación, actualización, oposición o eliminación, según sea el caso.

CAPÍTULO VI
VULNERACIÓN A LA SEGURIDAD DE DATOS PERSONALES

Artículo 24.- De la notificación de vulneración de seguridad.- De conformidad con lo dispuesto en la Ley, el responsable del tratamiento deberá notificar a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de Telecomunicaciones cualquier vulneración a la seguridad de los datos personales, siempre que sea probable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas naturales.

Se entiende que la vulneración o violación a la seguridad constituye un riesgo para los derechos y las libertades de las personas naturales cuando concurre cualquiera de las siguientes causales:

1. Cuando los datos fueron destruidos, ya no existen o no están disponibles de una forma que sea de utilidad para el responsable del tratamiento;
2. Cuando los datos personales han sido alterados, corrompidos o dejan de estar completos;
3. Cuando el responsable del tratamiento ha perdido el control o el acceso a los datos, o ya no obran en su poder; o,
4. Cuando el tratamiento no ha sido autorizado o es ilícito, lo cual incluye la divulgación de datos personales o el acceso por parte de destinatarios que no están autorizados a recibir o acceder a los datos o cualquier otra forma de tratamiento que se ejecuta contrariando las disposiciones de la Ley.

Artículo 25.- Finalidad de la notificación.- Las notificaciones de las vulneraciones de seguridad de datos personales tendrán como finalidad principal que la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de Telecomunicaciones lleven un registro estadístico sobre vulneraciones para determinar posibles medidas de seguridad para cada una de ellas, así como identificar sectores o instituciones más vulnerables y promover la adaptación de estándares internacionales y mejores prácticas en la gestión de incidentes y vulnerabilidades.

Artículo 26.- Contenido de la notificación.- La notificación de vulneración de seguridad deberá contener lo siguiente:

1. La naturaleza y tipo de vulneración;
2. Identificar los titulares o interesados afectados;
3. El detalle inicial de los sistemas vulnerados;
4. La causa presunta de la vulneración;
5. El volumen y tipos de datos expuestos o comprometidos;
6. Las medidas adoptadas y previstas para responder y remediar la vulneración con la finalidad de mitigar las consecuencias presuntas;
7. La evaluación del riesgo que la vulneración implica para los derechos y libertades de los titulares; y,
8. Otros aspectos determinados por la Autoridad de Protección de Datos Personales.

Artículo 27.- Notificación de vulneración de seguridad por parte del encargado.- El encargado deberá notificar al responsable del tratamiento de datos personales la vulneración de la seguridad de datos personales.

La notificación de vulneración de seguridad deberá contener la misma información detallada en el artículo precedente, a excepción de la evaluación del riesgo.

Artículo 28.- Notificación de vulneración de seguridad al titular.- La notificación de vulneración de datos al titular contendrá la misma información establecida en los artículos anteriores.

La notificación deberá realizarse en lenguaje claro y sencillo, observando los derechos de los titulares.

La Autoridad de Protección de Datos Personales velará por que las excepciones a la obligación de notificación señaladas en la Ley sean utilizadas de manera restringida y de manera justificada.

CAPÍTULO VII
EVALUACIÓN DE IMPACTO

Artículo 29.- Evaluación de impacto del tratamiento de datos personales.- La evaluación de impacto consiste en un análisis preventivo, de naturaleza técnica, mediante el cual el responsable valora los impactos reales del tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con el cumplimiento de los principios y el respeto de los derechos y de las obligaciones establecidas en la Ley Orgánica de Protección de Datos Personales, este Reglamento y demás normativa aplicable.

Artículo 30.- Objeto de la evaluación de impacto.- La evaluación de impacto tiene por objeto:

1. Identificar y describir los riesgos potenciales y probables de determinados tratamientos de datos personales;
2. Describir las acciones concretas para la gestión de los riesgos identificados;

3. Actuar de forma preventiva en el cumplimiento de las obligaciones establecidas en la Ley, su Reglamento y demás normativa aplicable; y,
4. Propiciar lineamientos para la construcción de una cultura preventiva de la protección de datos personales de la organización.

Artículo 31.- Evaluación de impacto obligatoria.- Las evaluaciones de impacto del tratamiento de datos serán obligatorias en los casos establecidos en la Ley y deberán realizarse de forma previa al inicio del tratamiento de datos personales.

Los responsables utilizarán los criterios establecidos en el presente Reglamento para determinar en qué casos se está en presencia de una evaluación sistemática y exhaustiva de aspectos personales, de un tratamiento a gran escala de categorías especiales de datos, de datos relativos a condenas e infracciones penales o, de una observación sistemática a gran escala de una zona de acceso público.

En caso de duda, el responsable podrá dirigir una consulta a la Autoridad de Protección de Datos Personales con la finalidad de que determine la obligatoriedad de la evaluación de impacto. La Autoridad de Protección de Datos personales deberá contestar dicha consulta en el término máximo de cinco (5) días contados desde la recepción de la consulta.

Artículo 32.- Requisitos de la evaluación de impacto.- En los casos en que sea obligatoria, la evaluación de impacto será presentada ante la Autoridad de Protección de Datos Personales y contendrá, al menos, lo siguiente:

1. La descripción sistemática de las operaciones de tratamiento y las finalidades de ese tratamiento;
2. La justificación de la necesidad de llevar a cabo esas operaciones de tratamiento, así como su proporcionalidad con respecto de la finalidad;
3. La evaluación de riesgos a los derechos y libertades de los titulares; y,
4. Las medidas previstas para hacer frente a los riesgos, las garantías, medidas de seguridad y mecanismos destinados a salvaguardar y demostrar el respeto al derecho de los titulares a la protección de sus datos personales.

La información otorgada en virtud de los numerales precedentes debe limitarse a la que sea necesaria para respaldar la evaluación y no incluir detalles potencialmente

confidenciales relacionados con las implementaciones de seguridad o la información confidencial.

CAPÍTULO VIII
RESPONSABLE DEL TRATAMIENTO

Artículo 33.- Obligaciones del responsable del tratamiento.- El responsable del tratamiento deberá, tanto en el momento de la determinación de los medios para el tratamiento como en el momento mismo del procesamiento de datos personales, aplicar medidas apropiadas que sean adecuadas para la observancia efectiva de los principios de protección de datos, así como de los derechos reconocidos en la Ley. Para ello, tendrá en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como la probabilidad y la gravedad de los riesgos para los intereses de los titulares.

Artículo 34.- Estado de la técnica.- Se entiende por estado de la técnica a los progresos actuales de la tecnología disponible en el mercado, que deberá ser considerado al determinar las medidas técnicas y organizativas adecuadas. El responsable del tratamiento deberá evaluar continuamente el estado de la técnica.

Artículo 35.- Costos de aplicación.- Los costos de aplicación no se limitan solamente a términos monetarios sino también a los recursos que, en general, deba invertir el responsable del tratamiento, incluidos el tiempo y el humano. El responsable del tratamiento deberá evaluar los riesgos que conlleva el tratamiento para los derechos y libertades de los titulares y estimar los costos de la aplicación de las medidas adecuadas para mitigar dichos riesgos. La incapacidad de asumir los costos no es excusa para el incumplimiento de la Ley y el presente Reglamento, para lo cual se observará el principio de proporcionalidad entre el volumen del tratamiento de los datos y la capacidad económica del responsable del tratamiento.

Artículo 36.- De la prueba de las medidas de protección.- Los responsables del tratamiento deberán demostrar que han aplicado todas la medidas necesarias para la protección de datos personales. Para ello, el responsable del tratamiento podrá determinar los indicadores clave de rendimiento adecuados para demostrar el cumplimiento. Estos indicadores pueden incluir métricas para demostrar la eficacia de las medidas tomadas. Las métricas pueden ser cuantitativas, como el nivel de riesgo, la reducción de las

reclamaciones, la reducción del tiempo de respuesta cuando los interesados ejercen sus derechos; o, cualitativas, como las evaluaciones del rendimiento, el uso de escalas o evaluaciones de expertos.

Artículo 37.- Responsables conjuntos.- Si dos o más responsables del tratamiento determinan conjuntamente los mismos fines y los medios del tratamiento de los datos personales, se considerarán responsables conjuntos, quienes definirán sus respectivas tareas y responsabilidades en materia de protección de datos de forma transparente a través de un contrato, en la medida en que estas no estén ya definidas en disposiciones legales, buscando precautelar los intereses y derechos de los titulares.

Dicho acuerdo no impedirá que el titular o interesado ejerza sus derechos contra cualquiera de los responsables conjuntos del tratamiento y que estos sean responsables solidarios ante la autoridad de control y los titulares.

Además, cada responsable conjunto deberá cumplir las obligaciones que determina la Ley, en función de las responsabilidades asumidas en el acuerdo, cuya evidencia deberá estar a disposición de la autoridad de control, cuando así lo solicite. En este sentido, cada responsable conjunto es sujeto del régimen sancionador, en forma diferenciada sobre la base de las responsabilidades adquiridas.

Los acuerdos de protección de datos entre responsables conjuntos deben ser compartidos con los titulares interesados cuando así sea requerido por éstos, sobre la base del principio de transparencia.

Artículo 38.- Registro de actividades de tratamiento.- El responsable del tratamiento que cuente con cien o más trabajadores, llevará un registro de todas las actividades de tratamiento de datos personales que sean de su competencia.

Este registro contendrá la siguiente información:

1. El nombre y los datos de contacto del responsable del tratamiento y, en su caso, del responsable que actúa conjuntamente con el responsable del tratamiento de datos personales, así como el nombre y los datos de contacto del delegado de protección de datos;
2. Los fines del tratamiento;

3. Las categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales;
4. Identificar a los titulares y las categorías de datos personales de los titulares;
5. En su caso, el uso de perfiles;
6. En su caso, definir las transferencias de datos personales a organismos de un tercer país o a una organización internacional;
7. Descripción de las bases legitimadoras que facultan el tratamiento;
8. Los plazos de retención previstos para la supresión o la revisión de la necesidad de conservar las diferentes categorías de datos personales; y,
9. Una descripción general de las medidas técnicas, jurídicas, administrativas y organizativas.

El registro se llevará por escrito o electrónicamente. Los responsables pondrán a disposición de la Autoridad de Protección de Datos Personales los registros de actividades cuando ésta lo solicite.

Artículo 39.- Extensión de la obligación de registro.- La obligación de registro de actividades también la tendrán los responsables de tratamiento que, teniendo menos de cien trabajadores, cumplan alguna de las siguientes condiciones:

1. El tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los titulares, de acuerdo con el análisis de riesgos, amenazas y vulnerabilidades, de conformidad con lo dispuesto en la ley;
2. No se trate de un tratamiento ocasional; o,
3. Incluya categorías especiales de datos personales.

CAPÍTULO IX
ENCARGADO DEL TRATAMIENTO

Artículo 40.- Encargado.- El encargado del tratamiento deberá ofrecer garantías suficientes para aplicar medidas técnicas, jurídicas, administrativas y organizativas apropiadas para que el tratamiento cumpla con las disposiciones de la Ley garantizando el adecuado tratamiento de los datos personales y la protección de los derechos de los titulares.

Artículo 41.- De la relación entre responsable y encargado.- La relación entre el responsable del tratamiento y un encargado debe regirse por un contrato escrito, en el cual se detallen las instrucciones encomendadas respecto del tratamiento de datos personales y, al menos, los siguientes aspectos:

1. El objeto;
2. La duración;
3. La naturaleza;
4. La finalidad del tratamiento de los datos;
5. La categoría de los datos personales;
6. Identificar a los titulares de los datos personales tratados; y,
7. Las obligaciones y responsabilidades del encargado.

El encargado del tratamiento deberá respetar las instrucciones que, para el efecto, determine el responsable en cuanto al tratamiento de los datos personales. Para ello, deberá establecer las medidas técnicas y organizativas adecuadas, previo a brindar el servicio, que deberán ser equiparables a aquellas a las que está obligado el responsable en función de los datos y los tipos de tratamiento aplicables, de tal forma que se garantice la protección de datos de los titulares.

Artículo 42.- Obligación del responsable.- El responsable del tratamiento de datos personales será el directo obligado de garantizar el correcto ejercicio de los derechos reconocidos en la Ley a los titulares, sin embargo, el encargado deberá asistir al responsable y realizar todas las acciones necesarias, y bajo su responsabilidad, para que el responsable pueda cumplir con esta obligación.

Artículo 43.- Responsabilidad del encargado.- El encargado del tratamiento que, por cualquier causa, determine los fines y los medios del tratamiento, se considerará, para efectos de la Ley, responsable del tratamiento en lo que respecta a dicho tratamiento. En tal sentido, para que el encargado sea considerado como tal, debe actuar a nombre y por cuenta del responsable y conforme a las instrucciones documentadas. Si el encargado considera que una instrucción es ilegal, informará al responsable del tratamiento, sin demora injustificada, para que se corrija la instrucción, de ser pertinente.

Artículo 44.- Registro de actividades del tratamiento.- El encargado del tratamiento deberá mantener un registro de actividades del tratamiento cuando el responsable del

tratamiento esté obligado a ello, de conformidad con lo previsto en la Ley, el presente Reglamento y demás normativa aplicable.

Artículo 45.- Contratación.- El encargado del tratamiento podrá contratar a un tercero para complementar la prestación de un servicio al responsable del tratamiento de datos personales, siempre que esto se haga constar expresamente en el contrato celebrado entre el responsable y el encargado del tratamiento. Caso contrario, requerirá la autorización escrita del responsable del tratamiento para la subcontratación.

En este caso, el tercero contratado asumirá las obligaciones del encargado de tratamiento establecidas en la ley y en el presente Reglamento, debiendo cumplir con las instrucciones de tratamiento de datos establecidas entre el responsable y encargado del tratamiento, en aquello que fuere pertinente en función de los servicios que han sido contratados.

Artículo 46.- Eliminación de datos personales.- El encargado deberá devolver o eliminar todos los datos personales, según las instrucciones impartidas por el responsable del tratamiento, una vez finalizada la relación que justifica el tratamiento de datos personales, destruyendo todas las copias existentes, salvo que exista la obligación de conservar los datos en virtud de una disposición legal.

Artículo 47.- Revisión de registros.- El encargado de tratamiento deberá permitir al responsable o a la persona determinada por este, en cualquier momento que así lo solicite el responsable, la revisión de los registros y procesos que tengan relación con los tratamientos de datos personales encomendados, a fin de verificar el correcto cumplimiento del contrato y las obligaciones de la Ley y el presente Reglamento, así como la adopción de medidas técnicas, organizativas y de seguridad adecuadas.

En tal sentido, el encargado deberá proporcionar al responsable o a la persona determinada por este, todas las facilidades y toda la información necesaria para demostrar el cumplimiento de sus obligaciones.

CAPÍTULO X
DELEGADO DE PROTECCIÓN DE DATOS

Artículo 48.- Delegado de protección de datos.– El delegado de protección de datos personales es la persona natural que se encarga principalmente de asesorar, velar y

supervisar, de manera independiente, el cumplimiento de las obligaciones legales imputables al responsable y al encargado del tratamiento de datos personales.

Podrá realizar otras actividades relacionadas con la protección de datos personales que le sean encomendadas por el responsable, siempre que no supongan o exijan del delegado una preparación diversa ni exista un conflicto con las responsabilidades previamente adquiridas.

El delegado de protección de datos personales desempeñará sus funciones de manera profesional, con total independencia del responsable y del encargado del tratamiento de datos personales, quienes estarán obligados a facilitar la asistencia, recursos y elementos que les sea oportunamente requeridos para garantizar el cumplimiento de los deberes, funciones y responsabilidades a cargo del delegado.

Sin perjuicio de lo que disponga la Ley y este Reglamento, corresponderá a la Autoridad de Protección de Datos Personales emitir la normativa que garantice la independencia del delegado de protección de datos personales en el desempeño de sus funciones en relación con el responsable y encargado.

Artículo 49.- Tipo de contratación.- El delegado de protección de datos podrá ser contratado por el responsable del tratamiento de datos personales, bajo la figura de relación de dependencia o a través de un contrato de prestación de servicios. Sin perjuicio de lo indicado, en cualquiera de los casos, deberá respetar y garantizar que se presten los servicios de manera independiente.

Tratándose de las instituciones del sector público, el delegado de protección de datos será designado por la máxima autoridad institucional.

Artículo 50.- Delegado de protección de datos de grupos empresariales.- Los grupos empresariales podrán designar a un único delegado de protección de datos personales, en la medida en que pueda ejecutar sus actividades y sin que esto genere conflicto de intereses.

Artículo 51.- Prohibición de sanción al delegado de protección de datos. - El responsable y el encargado del tratamiento de datos personales deberán respetar el trabajo que ejecute el delegado de protección de datos personales, y no se aplicarán sanciones

por el hecho de desempeñar y cumplir sus funciones. En caso que el delegado sea sancionado o removido por motivo de la ejecución de sus funciones, podrá poner este hecho en conocimiento de la Autoridad de Protección de Datos Personales, que valorará las circunstancias en las que se produjo la desvinculación o sanción y validará las sanciones que correspondan, sin perjuicio de las acciones legales o judiciales a que hubiere a lugar por parte del delegado perjudicado.

La Autoridad de Protección de Datos Personales establecerá el procedimiento de denuncia y las sanciones correspondientes para los casos de remoción o sanción injustificadas del delegado de protección de datos.

Artículo 52.- Buenas prácticas.- Los responsables o encargados del tratamiento de datos personales, que no se encuentren dentro de las categorías de obligados a designar un delegado de protección de datos, podrán hacerlo de manera voluntaria como un mecanismo de buena práctica y como parte de las medidas de responsabilidad proactiva a adoptar.

En atención a sus necesidades institucionales, los responsables y encargados del tratamiento de datos personales podrán designar un delegado suplente, que actuará en caso de ausencia o impedimento temporal o definitivo del primero.

Artículo 53.- Actividades de control permanente y sistematizado de datos.- Para determinar si las actividades de un responsable o encargado en materia de protección de datos requieren de un control permanente, se deberá considerar, entre otros factores que defina la Autoridad de Protección de Datos Personales, alguno de los siguientes:

1. Si el tratamiento de datos es continuado o si se produce en intervalos concretos durante un periodo de tiempo;
2. Si el tratamiento de datos es recurrente o repetido en momentos prefijados; o,
3. Si el tratamiento tiene lugar de manera constante o periódica.

Así mismo, para determinar si el control es sistematizado, además de aquellos que determine la Autoridad de Protección de Datos Personales, se deberá verificar alguno de los siguientes aspectos:

1. Si el tratamiento de datos está de alguna manera preestablecido, organizado o es metódico;
2. Si el tratamiento de datos tiene lugar como parte de un plan general de recogida de datos; o,
3. Si el tratamiento de datos es llevado a cabo como parte de una estrategia.

En caso de suscitarse dudas entre los responsables y encargados respecto a los supuestos que dan lugar a la designación del delegado de protección de datos personales, podrán dirigir sus respectivas consultas a la Autoridad de Protección de Datos Personales, cuya decisión será de cumplimiento obligatorio para los consultantes.

Artículo 54.- Tratamiento a gran escala de datos de categoría especiales.- Para determinar el tratamiento de datos de categorías especiales a gran escala, se considerarán, entre otros factores que defina la Autoridad de Protección de Datos Personales, los establecidos en el presente Reglamento.

Artículo 55.- Requisitos para ser delegado.- Sin perjuicio de otros requisitos que establezca la Autoridad de Protección de Datos Personales, para ser delegado de protección de datos personales, se requerirá:

1. Estar en goce de los derechos políticos;
2. Ser mayor de edad;
3. Tener título de tercer nivel en Derecho, Sistemas de Información, de Comunicación, o de Tecnologías; y,
4. Acreditar experiencia profesional de por lo menos cinco años;

Artículo 56.- Impedimento para ser delegado.- Sin perjuicio de otras que defina la Autoridad de Protección de Datos Personales, no podrán ser delegados de protección de datos personales las siguientes personas:

1. Quienes formen parte de los órganos de administración y control del responsable y encargado;
2. Los socios o accionistas del responsable y encargado;
3. Los cónyuges de los administradores, directores o comisarios de la compañía, en caso de haberlos, del responsable y encargado, o sus parientes hasta el cuarto grado de consanguinidad o segundo de afinidad; y,

4. Quienes tengan conflictos de intereses con el responsable y encargado, para lo cual la Autoridad de Protección de Datos Personales emitirá la normativa correspondiente en la que se establecerán los supuestos específicos que darían lugar a dicho conflicto de intereses.

Tratándose de las instituciones del sector público, la Autoridad de Protección de Datos Personales definirá las incompatibilidades para ser delegado de protección de datos personales para cada caso en particular.

Artículo 57.- Acuerdos de Confidencialidad.- El delegado de protección de datos personales suscribirá un acuerdo de confidencialidad respecto de la información que llegase a conocer o respecto de la cual pueda llegar a tener acceso por el desempeño de su cargo. Las partes acordarán, libremente, los términos y condiciones del acuerdo, pero en ningún caso tales documentos podrán limitar el acceso del delegado a la información que estime necesaria para el desempeño de su función.

El incumplimiento de los acuerdos de confidencialidad estará sujeto a las responsabilidades civiles y penales a las que hubiere lugar.

Este deber de guardar confidencialidad subsistirá incluso una vez que haya concluido la relación jurídica con el responsable o encargado.

CAPÍTULO XI
RESPONSABILIDAD PROACTIVA Y AUTORREGULACIÓN

Artículo 58.- Obligatoriedad.- El responsable del tratamiento está obligado a aplicar medidas técnicas, jurídicas, administrativas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos que realiza es conforme con la normativa. Para ello se deberá atender:

1. La naturaleza;
2. El ámbito;
3. La finalidad del tratamiento; y,
4. Los riesgos.

Esta obligación implica también revisar y actualizar las medidas cuando sea necesario.

Artículo 59.- Medidas de protección de datos desde el diseño.- El responsable del tratamiento tiene la obligación de establecer medidas técnicas y organizativas adecuadas para aplicar los principios establecidos en la normativa de forma eficaz, y proteger los derechos de los titulares, de manera previa al tratamiento de datos personales.

Para la fijación de estas medidas debe tenerse en cuenta:

1. La naturaleza, ámbito y finalidad del tratamiento;
2. Los riesgos de diversa probabilidad y gravedad asociados al tratamiento;
3. El estado de la técnica; y,
4. El coste de aplicación.

Artículo 60.- Medidas de protección de datos por defecto.- El responsable del tratamiento adoptará las medidas técnicas y organizativas apropiadas para garantizar que, mediante ajustes, por defecto, solo puedan tratarse aquellos datos personales cuyo tratamiento sea necesario para la respectiva finalidad específica del tratamiento.

Además, mediante los respectivos ajustes, las medidas deben garantizar que, por defecto, los datos no puedan ser accesibles a un número indefinido de personas de forma automatizada.

Esta obligación es aplicable a:

1. La cantidad de los datos recopilados;
2. La extensión del tratamiento;
3. El período de almacenamiento; y,
4. La accesibilidad

Para acreditar el cumplimiento de esta medida, podrá utilizarse un mecanismo de certificación, según lo previsto en la Ley Orgánica de Protección de Datos Personales.

Artículo 61.- Mecanismos de autorregulación.- Los mecanismos de autorregulación pueden ser adoptados para el cumplimiento de los principios, ejercicio de derechos, medidas de seguridad, transferencias, procedimientos y, en general, para cumplir

cualquiera de las obligaciones previstos en la Ley Orgánica de Protección de Datos Personales, este Reglamento y demás normativa aplicable.

Los mecanismos de autorregulación constituyen instrumentos que permiten adecuar de mejor forma esquemas de cumplimiento para sectores específicos o en situaciones muy particulares, y dar cumplimiento a la Ley Orgánica de Protección de Datos Personales, así como el resto de normativa aplicable.

Artículo 62.- Mecanismos de autorregulación.- Serán mecanismos de autorregulación los siguientes:

1. Esquemas certificados en materia de protección de datos personales por el Servicio Ecuatoriano de Acreditación;
2. Reglas específicas creadas para adaptar la normativa de protección de datos personales a un determinado sector o situación. En este tipo de reglas estarán comprendidos los códigos de conducta, las normas corporativas vinculantes y las cláusulas tipo; y,
3. Esquemas validados por la Autoridad de Protección de Datos Personales, conforme a las reglas que para el efecto emita.

Artículo 63.- Registro de mecanismos de autorregulación.- La Autoridad de Protección de Datos Personales mantendrá un registro de mecanismos de autorregulación a fin de dar a conocer la siguiente información:

1. Las reglas destinadas a adaptar la normativa de datos personales para determinado sector o situación, con la finalidad de facilitar y hacer efectivo su cumplimiento;
2. Las entidades de acreditación autorizadas por el Servicio Ecuatoriano de Acreditación en materia de protección de datos personales;
3. Las entidades de evaluación acreditadas para otorgar certificaciones en materia de protección de datos personales por el Servicio Ecuatoriano de Acreditación, en el marco de la Ley, este Reglamento y las reglas que se emitan para el efecto; y,
4. Los responsables y encargados que hayan adoptado algún mecanismo.

SECCIÓN I
CERTIFICACIÓN

Artículo 64.- Objeto de la certificación.- La certificación tiene por objeto determinar el grado de cumplimiento de un mecanismo de autorregulación con relación a las obligaciones de la Ley Orgánica de Protección de Datos Personales, este Reglamento y demás normativa aplicable.

Corresponderá, privativamente, a la Autoridad de Protección de Datos Personales emitir y actualizar periódicamente los parámetros básicos o estándares mínimos de evaluación a los que deberán someterse los responsables y encargados para obtener la certificación a la que se refiere este Reglamento.

Artículo 65.- Temporalidad de la certificación.- La certificación se expedirá por un periodo máximo de tres años, vencido el cual podrá ser renovada en las mismas condiciones, siempre y cuando se cumplan los requisitos establecidos para el efecto.

Artículo 66.- Entidades de certificación.- La certificación en materia de protección de datos estará a cargo de las entidades de certificación acreditadas por el Servicio Ecuatoriano de Acreditación, de conformidad con la normativa que para el efecto emitan en conjunto la Autoridad de Protección de Datos Personales y la Autoridad Nacional de Acreditación.

Para la acreditación de la entidad de certificación se revisará el cumplimiento de, entre otros establecidos por la Autoridad de Protección de Datos Personales, los siguientes requisitos:

1. Haber demostrado su independencia y pericia en relación con el objeto de la certificación;
2. Haber establecido procedimientos adecuados para la expedición, revisión periódica y la retirada de sellos y certificaciones de cumplimiento en materia de protección de datos; y,
3. Haber demostrado que sus funciones y cometidos no dan lugar a conflictos de intereses.

Para la aprobación de las entidades certificadoras se tomará en cuenta, además, el cumplimiento por parte de estas entidades de normas internacionales como la relativa a los requisitos para organismos que certifican productos, procesos y servicios.

Artículo 67.- Revocatoria.- Cuando el responsable o encargado del tratamiento de datos personales dejen de cumplir con los requisitos que dieron paso al otorgamiento de la certificación, ésta podrá ser revocada por el mismo organismo de certificación que la otorgó o por la autoridad de control competente.

SECCIÓN II
CÓDIGOS DE CONDUCTA

Artículo 68.- Aprobación de códigos de conducta.- Cualquier persona natural o jurídica, asociación, gremio o grupo de empresas podrá presentar, para aprobación de la Autoridad de Protección de Datos, códigos de conducta que tengan como fin el cumplimiento de la normativa vigente en materia de protección de datos personales.

Los códigos de conducta deberán contener al menos lo siguiente:

1. Exposición de motivos, clara y concisa, que describa detalladamente el objetivo del código, su ámbito de aplicación y cómo facilitará la aplicación efectiva de la Ley y este Reglamento;
2. Ámbito de aplicación que determine de forma específica las operaciones de tratamiento o las características del tratamiento de datos personales que abarca, así como las categorías de responsables o encargados del tratamiento a las que se aplica. Esto incluirá las cuestiones del tratamiento que pretenda abordar el código y aportará soluciones prácticas; y,
3. Mecanismos de supervisión para controlar el pleno cumplimiento de sus disposiciones.

Artículo 69.- Admisibilidad.- El proponente del código presentará formalmente su proyecto de código, ya sea en formato electrónico o físico a la Autoridad de Protección de Datos Personales.

Presentado el proyecto de código, la Autoridad de Protección de Datos, en el término máximo de cinco (5) días, examinará si cumple con los requisitos de forma establecidos

en el artículo anterior. Si lo hace calificará, tramitará y dispondrá la evaluación del contenido del proyecto de código.

Si el proyecto no cumple con los requisitos formales, la Autoridad de Protección de Datos Personales dispondrá que el proponente la complete o aclare en el término de cinco (5) días, determinando explícitamente el o los defectos. Si no lo hace, ordenará el archivo y la devolución del proyecto, sin necesidad de dejar copias.

Artículo 70.- Evaluación del fondo.- Admitido el proyecto de código, la Autoridad de Protección de Datos Personales deberá, en el término de un treinta (30) días, evaluar y verificar que el código contribuya a la correcta aplicación de la Ley, el presente Reglamento y la normativa aplicable en materia de protección de datos, teniendo en cuenta las características específicas de los diversos sectores del tratamiento, así como las obligaciones y los requisitos concretos de los responsables o encargados del tratamiento a los que se aplique.

Además de los criterios que determine la Autoridad de Protección de Datos para la aprobación de los Códigos de Conducta, se verificará que el proyecto cumpla con los siguientes criterios:

1. Satisfacer una necesidad puntual de ese sector o actividad de tratamiento;
2. Especificar la aplicación de la Ley y el Reglamento a la naturaleza de la actividad o el sector del tratamiento;
3. Aportar mejoras al sector en cuanto al cumplimiento de la legislación en materia de protección de datos;
4. Establecer normas realistas, aplicables, concretas, inequívocas y estar formuladas con la calidad y coherencia interna necesarias para aportar valor;
5. Desarrollar de manera específica, práctica y precisa cómo ha de aplicarse la ley, el reglamento y demás normativa de protección de datos;
6. Aportar garantías suficientes y eficaces para mitigar el riesgo que entraña el tratamiento de datos y respetar los derechos y las libertades de los particulares;
7. Disponer de mecanismos eficaces para supervisar el cumplimiento del código; y,
8. Identificar y proponer específicamente las estructuras, procedimientos y órganos que velen por una supervisión eficaz y una sanción de las infracciones.

Los citados mecanismos pueden incluir una auditoría periódica y requisitos de presentación de informes, la gestión clara y transparente de las reclamaciones y los procedimientos de solución de conflictos, sanciones específicas y medidas correctivas en caso de infracción del código, así como mecanismos para denunciar las infracciones de sus disposiciones.

CAPÍTULO XII
TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS

Artículo 71.- Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección.- De oficio o a petición de parte, la Autoridad de Protección de Datos Personales, mediante resolución motivada, determinará los países, organizaciones o personas jurídicas que cuentan con adecuados niveles de protección para transferencia de datos personales. Para ello, revisará que los estándares de protección sean equivalentes o superiores a aquellos establecidos en la Ley y demás normativa respectiva.

La resolución tendrá efectos generales, por lo que las transferencias internacionales hacia ese país, organización o persona jurídica no requerirá de autorización previa.

Artículo 72.- Contenido y publicación de la resolución.- La Autoridad de Protección de Datos Personales establecerá el mecanismo de revisión periódica de los niveles adecuados de protección, que deberá llevarse a cabo anualmente. De ser el caso, podrá revocar, modificar o suspender la resolución que reconoció el adecuado nivel de protección al país, organización o persona jurídica, sin que este acto tenga efectos retroactivos.

La resolución será publicada en el Registro Oficial y por medios digitales disponibles al público en su página web institucional.

Artículo 73.- Criterios de estándares de nivel adecuado de protección.- Para determinar si un país, organización o persona jurídica posee un nivel adecuado de protección de datos se tendrá en cuenta los siguientes criterios, sin perjuicio de otros que pueda definir la Autoridad de Protección de Datos:

1. La legislación nacional y normativa sectorial del país, que tenga incidencia en materia de protección de datos personales;
2. La legislación en materia de seguridad nacional, pública y, en general aquella que tenga relación con la defensa y seguridad del Estado, así como la legislación penal. En estas materias se deberá poner especial énfasis en la revisión de las disposiciones que habiliten el acceso a datos personales por parte de las autoridades de ese país, organización o persona jurídica;
3. La normativa sobre transferencias ulteriores de datos personales a terceros países, organizaciones o personas jurídicas;
4. La jurisprudencia vinculada a la protección de datos personales;
5. El reconocimiento de derechos y los mecanismos para su ejercicio en favor de los titulares de datos personales;
6. El establecimiento de deberes y obligaciones de los responsables y encargados del tratamiento de datos personales;
7. La existencia de una autoridad de protección de datos personales que sea independiente y que tenga competencias de control y vigilancia del cumplimiento de la normativa en materia protección de datos personales, así como de sanción en caso del cometimiento de infracciones en esta materia. Además, deberá brindar asistencia y asesoría a los titulares y cooperación internacional con otras autoridades; y,
8. Los compromisos internacionales asumidos por el país, organización o persona jurídica en cuanto a la materia de protección de datos personales.

Artículo 74.- Transferencia o comunicación internacional mediante garantías adecuadas.- De conformidad con la Ley, los instrumentos jurídicos que sustentan la transferencia internacional de datos personales a un país, organización o territorio económico internacional que no haya sido calificado por la Autoridad de Protección de Datos de tener un nivel adecuado de protección serán los siguientes:

1. Instrumentos jurídicamente vinculantes y exigibles entre las autoridades u organismos públicos;
2. Normas corporativas vinculantes aprobadas por la Autoridad de Protección de Datos;
3. Cláusulas tipo de protección de datos adoptadas por organismos internacionales de protección de datos avaladas por la autoridad de control;

4. Códigos de conducta, que incluyan compromisos vinculantes del responsable o el encargado del tratamiento en el tercer país, organización o territorio económico internacional de aplicar garantías adecuadas, que incluya las relativas a los derechos de los interesados;
5. Mecanismos de certificación que incluyen sellos y marcas de protección, que incorporen compromisos vinculantes del responsable o el encargado del tratamiento en el tercer país, organización o territorio económico internacional de aplicar garantías adecuadas, así como aquellos relativos a los derechos de los interesados; y,
6. Cláusulas contractuales que no correspondan a las cláusulas tipo y que estén debidamente autorizadas por la autoridad de protección de datos.

Artículo 75.- Normas corporativas vinculantes.- Son normas corporativas vinculantes las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en la República del Ecuador, para garantizar una adecuada protección de los datos personales, que permiten realizar transferencias internacionales de datos personales a un responsable o encargado en uno o más países, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Todo grupo empresarial, o unión de empresas dedicadas a una actividad económica conjunta, tendrá la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de datos a terceros países, siempre que tales normas corporativas incorporen todos los principios de tratamiento de datos personales y derechos aplicables y garantías de seguridad adecuadas para la transferencia de datos de personales.

Artículo 76.- Autorización de normas corporativas vinculantes.- Para que las normas corporativas vinculantes constituyan garantías adecuadas de protección, deberán ser autorizadas por la Autoridad de Protección de Datos.

Para ello, la Autoridad de Protección de Datos deberá observar que las normas corporativas vinculantes cumplan los siguientes requisitos:

1. Sean jurídicamente vinculantes;
2. Confieran expresamente a los titulares derechos exigibles en relación con el tratamiento de sus datos personales; y,

3. Cumplan con los requisitos establecidos en la Ley.

Artículo 77.- Transferencia o comunicación internacional en casos no contemplados.- En casos no contemplados en los artículos precedentes, la Autoridad de Protección de Datos Personales autorizará, con carácter previo, la transferencia internacional de datos personales, únicamente cuando el responsable cumpla con alguno de los siguientes supuestos:

1. Que mediante contrato entre el responsable o encargado y el destinatario, este último se obligue, voluntaria y formalmente, a cumplir con la Ley, el Reglamento y demás normativa aplicable, así como a aceptar la autoridad y competencia de la Autoridad de Protección de Datos y de los tribunales ecuatorianos, para cualquier efecto relacionado con el tratamiento de los datos objeto de la transferencia; o,
2. Que mediante contrato entre el responsable o encargado y el destinatario, este último se obligue, voluntaria y formalmente, a cumplir con la Ley, el Reglamento y demás normativa aplicable, y que en el país o territorio donde se encuentre establecido el destinatario se garantice el ejercicio de los derechos, incluido aquel a presentar una reclamación ante una autoridad de protección de datos personales y el derecho a la tutela judicial efectiva, por parte de los titulares.

Artículo 78.- Registro de información sobre transferencias internacionales en el Registro Nacional de Protección de Datos.- En el Registro Nacional de Protección de Datos se registrará la siguiente información:

1. El país donde se ubica el destinatario de los datos;
2. Las categorías de datos objeto de la transferencia;
3. Las finalidades de la transferencia;
4. El nombre, denominación, razón social o nombre comercial con el que se identifique al destinatario;
5. El mecanismo o esquema autorizado, conforme a la Ley y este Reglamento, para realizar la transferencia; y,
6. El criterio de excepción utilizado de los previstos en la Ley, cuando sea el caso.

La Autoridad de Protección de Datos privilegiará la utilización de medios digitales para el registro de la información descrita, y emitirá las reglas conforme a las cuales se

realizará el registro de la información, los medios disponibles para el registro, los plazos, así como los mecanismos para la actualización de dicha información, de ser el caso.

CAPÍTULO XIII
AUTORIDAD DE PROTECCIÓN DE DATOS

Artículo 79.- Autoridad de Protección de Datos Personales.- La Autoridad de Protección de Datos Personales goza de autonomía administrativa, técnica, operativa y financiera. Estará a cargo del Superintendente de Protección de Datos Personales y tendrá su sede en el Distrito Metropolitano de Quito.

El Estatuto Orgánico Funcional será aprobado por la máxima autoridad y contendrá la estructura institucional necesaria para el cumplimiento de sus fines y atribuciones.

Artículo 80.- Atribuciones.- La Autoridad de Protección de Datos Personales, además de las señaladas en la Ley de la materia, tendrá las siguientes:

1. Hacer cumplir las regulaciones en el marco de la protección de datos personales;
2. Registrar las bases de datos que contengan datos personales en el Registro Nacional de Protección de Datos Personales;
3. Dirigir y administrar el Registro Único de Responsables y Encargados Incumplidos;
4. Emitir regulaciones para la protección de datos personales;
5. Emitir los informes técnicos dentro de los mecanismos de control y supervisión que se dispongan;
6. Proponer reformas a la Ley y su reglamento;
7. Emitir guías de referencias que ayuden a los responsables y encargados del tratamiento de datos en el proceso de adecuación y cumplimiento de la normativa de protección de datos personales;
8. Conocer y resolver las peticiones, quejas, reclamos y recursos que se propongan en el ámbito de su competencia y de conformidad con la Ley; y,
9. Las demás que se le asignen en este reglamento.

Artículo 81.- Planes anuales.- Las actividades de control se realizarán de acuerdo con el plan anual aprobado por la máxima autoridad, el cual será elaborado considerando la naturaleza de las organizaciones controladas, el volumen y la sensibilidad de los datos

personales sujetos a tratamiento, la aplicación de los diferentes procedimientos de control y la disponibilidad presupuestaria.

Se podrán ejecutar procedimientos de control no considerados dentro de los planes anuales si la situación lo amerita, basados en criterios de criticidad, oportunidad y posibles lesiones al derecho a la protección de datos personales de uno o más titulares de datos personales.

Artículo 82.- Mecanismos de control. - La Autoridad de Protección de Datos Personales determinará los procedimientos de control que se regirán por las reglas previstas en el Código Orgánico Administrativo.

Artículo 83.- Atribuciones del Superintendente de Protección de Datos Personales.- Son atribuciones del Superintendente de Protección de Datos Personales, a más de las señaladas en la Ley y este Reglamento, las siguientes:

1. Representar legal y judicialmente a la Autoridad de Protección de Datos Personales, en todos los actos, contratos y relaciones jurídicas sujetas a su competencia.
2. Elaborar y publicar, anualmente, información estadística, de las organizaciones sujetas a su control y de los tratamientos de datos personales.
3. Formular, aprobar y ejecutar el presupuesto de la Autoridad de Protección de Datos Personales.
4. Preparar estudios y propuestas sobre reformas legales y reglamentarias que se requieran para el correcto ejercicio del derecho a la protección de datos personales, y ponerlos en consideración de los órganos encargados de aprobarlas.
5. Aprobar y expedir normas internas, resoluciones y manuales que sean necesarios para el buen funcionamiento de la Autoridad a su cargo.

Artículo 84.- Registro Nacional de Protección de Datos Personales.- El Registro Nacional de Protección de Datos Personales constituye un registro público a cargo de la Autoridad de Protección de Datos Personales, que contiene las bases de datos personales o tratamiento realizado por los responsables de tratamiento de datos personales en los términos previstos en la Ley.

Artículo 85.- Responsabilidad del registro.- El reporte y la actualización de la información en el Registro Nacional de Protección de Datos Personales, será obligación del responsable de tratamiento.

Esta obligación no implica el registro de los datos contenidos en la base de datos o que son objeto del tratamiento, y se realizará de manera independiente por cada base de datos o tratamiento.

La Autoridad de Protección de Datos Personales regulará los procesos de reporte y actualización en el Registro Nacional de Protección de Datos Personales a su cargo que deberán cumplir los responsables de tratamiento de datos personales.

Artículo 86.- Inscripción oportuna.- El reporte de bases de datos o tratamiento en el Registro Nacional de Protección de Datos Personales deberá realizarse dentro del término de diez días contados a partir del día siguiente al inicio del tratamiento.

Artículo 87.- Registro Único de Responsables y Encargados del tratamiento de datos personales incumplidos. - El Registro Único de Responsables y Encargados de tratamiento de datos personales incumplidos constituye un registro público a cargo de la Autoridad de Protección de Datos, en el que se harán constar los responsables y encargados del tratamiento que hubieren incurrido en alguna de las infracciones establecidas en la Ley y cuenten con una resolución firme, de conformidad con lo dispuesto en el ordenamiento jurídico vigente.

Dicho registro contendrá los siguientes datos:

1. Nombre de la persona natural o jurídica infractora;
2. Indicación de la infracción cometida;
3. Indicación de la sanción impuesta; y,
4. Reiteración o reincidencias en el cometimiento de infracciones.

Artículo 88.- Fines del Registro Único de Responsables y Encargados del tratamiento de datos personales Incumplidos.- El Registro Único de Responsables y Encargados del tratamiento de datos personales Incumplidos será utilizado exclusivamente para fines estadísticos, preventivos y de capacitación.

La Autoridad de Protección de Datos guardará la confidencialidad y privacidad de los datos contenidos en el Registro y aplicará las medidas de seguridad a fin de proteger la información personal contenida en el mismo.

La Autoridad de Protección de Datos mantendrá permanentemente actualizado el Registro, de tal forma que responda con veracidad y exactitud a los datos contenidos en el mismo.

Artículo 89.- Plazo de conservación.- El plazo máximo de conservación de los datos contenidos en el Registro de Responsables y Encargados del Tratamiento de datos personales Incumplidos es de siete (7) años contados desde la fecha de la emisión de la resolución o sentencia en firme.

CAPÍTULO XIV
RÉGIMEN SANCIONATORIO

Artículo 90.- Cometimiento de infracciones.- En los casos en que se presuma el cometimiento de alguna de las infracciones previstas en la Ley, la Autoridad de Protección de Datos iniciará el correspondiente procedimiento administrativo sancionatorio, de conformidad con las disposiciones establecidas en el Código Orgánico Administrativo.

La resolución que ponga fin al procedimiento deberá estar debidamente fundamentada y motivada, de conformidad con lo establecido en la Ley.

Las sanciones a las que hubiere lugar se impondrán sin perjuicio de la responsabilidad civil o penal que resulten del cometimiento de la infracción.

DISPOSICIÓN GENERAL

Los procedimientos administrativos se regirán por lo previsto en el Código Orgánico Administrativo.

N° 904

GUILLERMO LASSO MENDOZA

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

DISPOSICIÓN TRANSITORIA

PRIMERA.- La implementación y funcionamiento de la Superintendencia de Protección de Datos Personales estará sujeta a la disponibilidad presupuestaria, previo dictamen favorable del ente rector de las finanzas públicas.

SEGUNDA.- En el plazo máximo de un (1) año, contado a partir de la fecha de implementación y funcionamiento de la Superintendencia de Protección de Datos Personales, esta coordinará y llevará a cabo capacitaciones técnicas y cursos de formación dirigidos al público en general, orientados a promover el ejercicio del derecho a la protección de datos personales y a la profesionalización de los delegados de protección de datos personales. Para tal efecto, podrá celebrar alianzas con instituciones de educación superior con experiencia en la materia, así como con organizaciones especializadas que promuevan la protección de datos personales.

DISPOSICIÓN FINAL

El presente Reglamento General entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en el Palacio Nacional, Distrito Metropolitano de Quito, el 6 de noviembre de 2023.

Guillermo Lasso Mendoza
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA