ANEXO LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO 1

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente. Es decir, no solamente nombres y apellidos sino número de cédula, el número de placa de vehículos, número de matrícula, correo electrónico, es decir, todo dato que me hace identificable, con el que van a poder descubrir quién soy.

Dato biométrico: relativo a las características físicas o fisiológicas de una persona.

Dato genético: relacionado con características genéticas heredadas o adquiridas que proporciona información fisiología o de salud.

Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera. La regulación de la protección de estos datos estará a cargo de la Superintendencia de Bancos y de la Junta de Política y Regulación Financiera.

Datos relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria.

Datos sensibles: relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos. El tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, entre ellos:

- Recopilación, registro, organización, conservación, custodia, adaptación, modificación, eliminación, consulta, aprovechamiento, distribución, transferencia, o cualquier otra forma de habilitación de acceso, destrucción.

Base de Datos: Conjunto estructurado de datos en cualquier forma, modalidad de creación, almacenamiento, centralizado o descentralizado.

Consentimiento: Manifestación de la voluntad:

- libre (sin presión)
- específica (sobre medios y finales del tratamiento),
- informada (transparente)
- inequívoca (que no queden dudas del alcance de lo autorizado)

Por la que el titular de los datos personales autoriza al responsable del tratamiento a procesarlos. Puede revocarse en cualquier momento sin justificación, el responsable debe establecer mecanismos sencillos para este trámite.

Integrantes del sistema de protección de datos:

1) **Titular:** persona natural cuyos datos son objeto de tratamiento: es decir el dueño de los datos, cliente, colaborador, proveedor, accionista, etc.,

2) **Responsable del tratamiento:** institución pública o privada que decide sobre la finalidad y tratamiento de datos.

3) **Encargado del tratamiento:** institución pública o privada que trata datos personales a nombre del responsable del tratamiento. Ej. El banco da información personal de sus clientes a un Courier para que entregue los estados de cuenta. Recibe directrices del responsable para cuidar esos datos recibidos.

4) **Destinatario:** tercero que ha sido comunicado con los datos personales. Ejemplo: SRI,

Ministerio del Trabajo, IESS, Banco central, etc. (se convierte en un nuevo responsable de esos datos)

5) **Autoridad de Protección de Datos Personales:** Autoridad pública e independiente que se encarga de supervisar aplicación de la Ley. Ente de control que dictará directrices para TODO el ecosistema de protección de datos.

6) **Delegado de protección de datos personales:** Rol que cumple una persona natural, asesorando y supervisando el cumplimiento de la Ley por parte del responsable. Es un punto de contacto, intermediario o facilitador entre el cliente y la institución a la que se entregó los datos y también entre la institución y la autoridad.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado entre ellos:

- Recopilación, registro, organización, conservación, custodia, adaptación, modificación, eliminación, consulta, aprovechamiento, distribución, transferencia, o cualquier otra forma de habilitación de acceso, destrucción.

Ámbito de aplicación LEY: datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior.

No aplica a:

- Personas naturales que los utilicen en actividades familiares o domésticas
- Actividades periodísticas o contenidos editoriales
- En casos de gestión de riesgos por desastres naturales y, seguridad y defensa del Estado
- Datos o bases de datos establecidos para la prevención, investigación, detección enjuiciamiento de infracciones penales

Ámbito de aplicación REGLAMENTO:

- Es aplicable a todas las personas naturales y jurídicas, nacionales y extranjeras del sector público y privado, que realicen tratamiento de datos personales, tenga lugar en el territorio ecuatoriano o no.

CAPITULO 2
PRINCIPIOS

Lealtad.- para el titular debe quedar claro que se están recogiendo, utilizando, sus datos personales y no podrán ser usados por medios o para fines ilícitos.

Transparencia.- la información o comunicación deberá ser accesible en un lenguaje sencillo y claro.

Finalidad.- deberán ser explícitas, legítimas y comunicadas al titular.

Proporcionalidad del tratamiento.- no excesivo con relación a las finalidades para las cuales hayan sido recogidos.

Confidencialidad.- sigilo y secreto.

Calidad y exactitud.- íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad.

Conservación.- Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento. El responsable del tratamiento establecerá plazos para su supresión o revisión periódica.

La conservación ampliada para fines de archivo en interés público, investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad

Seguridad de datos personales.- implementar todas las medidas de seguridad, adecuadas y

necesarias, organizativas, técnicas, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad.
Responsabilidad proactiva y demostrada.- El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales.
Aplicación favorable al titular.- En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.
Independencia del control.- La Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.

CAPÍTULO 3
DERECHOS
1. Derecho a la Información: conforme los principios de lealtad y transparente por cualquier medio.
2. Derecho de Acceso, a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales.
3. Derecho de Rectificación y actualización: a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos.
4. Derecho de Eliminación: que el responsable del tratamiento suprima sus datos personales.
5. Derecho de Oposición o negarse al tratamiento de sus datos personales.
6. Derecho a la Portabilidad: a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado.
7. Derecho a la Suspensión del tratamiento de los datos.
8. Derecho a la Consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales.
9. Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, incluida la elaboración de perfiles que atenten contra derechos y libertades fundamentales
10. Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.
11. Derecho a la educación digital en el uso y manejo adecuado y responsable de las tecnologías en apego a la dignidad e integridad humana, la vida privada y reputación en línea y la ciudadanía digital.

CAPÍTULO 4
CATEGORIAS ESPECIALES
a) Datos sensibles; como etnia, identidad de género, identidad cultural, religión, ideología
b) Datos de niñas, niños y adolescentes;
c) Datos de salud; y,
d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

Queda prohibido el tratamiento de datos personales sensibles salvo circunstancias como:
- El titular haya dado su consentimiento explícito
- Sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos
- ámbito del Derecho laboral y de la seguridad y protección social

Datos Crediticios: Salvo prueba en contrario será legítimo y lícito el tratamiento de datos destinados a informar sobre la solvencia patrimonial o crediticia, incluyendo cumplimiento o incumplimiento de obligaciones comerciales o crediticias que permitan evaluar la capacidad de pago del titular de los datos.
Datos relativos a la salud.- Las instituciones que conforman el Sistema Nacional de Salud y los profesionales de la salud pueden recolectar y tratar los datos de sus pacientes que estén o hubiesen estado bajo tratamiento.
Tratamiento de datos relativos a la salud.- deberá cumplir con parámetros mínimos y aquellos que determine la Autoridad de Protección de Datos Personales en la normativa:
1. Confidencialidad y secreto profesional. El titular de la información deberá brindar su consentimiento previo
2. Siempre que sea posible, deberán ser previamente anonimizados o seudonimizados.
3. Todo tratamiento de datos de salud anonimizados deberá ser autorizado previamente por la Autoridad de Protección de Datos Personales.

CAPÍTULO 6
SEGURIDAD DE DATOS PERSONALES
Seguridad de los datos personales: El responsable o encargado del tratamiento de datos personales según el caso, deberá tomar en cuenta las categorías y volumen de datos personales, implementar un proceso de verificación, evaluación.

Entre otras medidas, se podrán incluir las siguientes;

- Medidas de anonimización, seudonomización o cifrado de datos personales;
- Medidas para mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso, de forma rápida en caso de incidentes; y
- Acogerse a estándares internacionales para la protección de derechos y libertades, implementación y de seguridad de la información o códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Medidas de seguridad en el ámbito del sector público.- El mecanismo gubernamental de seguridad de la información deberá incluir las medidas en el caso de tratamiento de datos personales frente vulnerabilidad, a accesos cualquier riesgo, amenaza, no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita.

Evaluación de impacto del tratamiento de datos personales. Cuando se haya identificado por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera. La evaluación de impacto relativa a la protección de los datos deberá efectuarse previo al inicio del tratamiento de datos personales y será de carácter obligatoria en caso de:
a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;
b) Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales, o
c) Observación sistemática a gran escala de una zona de acceso público.
otificación de vulneración de seguridad.- El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos

Personales y la ARCOTEL, a más tardar 5 días después de que haya tenido constancia de ella. El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, máximo dentro del término de 2 días contados a partir de la fecha en la que tenga conocimiento de ella.

Acceso a datos personales para atención a emergencias e incidentes informáticos. Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, de incidentes de seguridad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad, nacionales e internacionales, podrán acceder y efectuar tratamientos sobre los datos personales contenidos en las notificaciones de vulneración a las seguridades, durante el tiempo necesario, exclusivamente para la detección, análisis, protección y respuesta ante cualquier tipo de incidentes así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

Garantía del secreto de las comunicaciones y seguridad de datos personales.- Para la correcta prestación de los servicios de telecomunicaciones deben garantizar el secreto de las comunicaciones y seguridad de datos personales. Únicamente por orden judicial, los prestadores de servicios de telecomunicaciones podrán utilizar equipos, infraestructuras e instalaciones que permitan grabar los contenidos de las comunicaciones específicas dispuestas por los jueces competentes. Si se evidencia un tratamiento de grabación o interceptación de las comunicaciones no autorizadas por orden judicial, se aplicará lo dispuesto en la presente Ley.

CAPÍTULO VII
OBLIGACIONES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

1) Tratar datos personales conforme a la Ley, en su reglamento, en directrices emitidas por la Autoridad de Protección de Datos Personales, o la normativa.
2) Aplicar e implementar requisitos y herramientas administrativas, técnicas a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley.
3) Aplicar e implementar procesos de verificación, evaluación, valoración periódica;
4) Implementar políticas de protección de datos personales afines a cada caso en particular;
5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
6) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
8) Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas;
9) Implementar la protección de datos personales desde el diseño y por defecto;
10) Suscribir contratos de confidencialidad y manejo adecuado de datos personales;
11) Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la presente Ley.
12) Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales;
13) Designar al Delegado de Protección de Datos Personales, en los casos que corresponda;

14) Permitir y contribuir a la realización de auditorías o inspecciones

Delegado de protección de datos personales.- Se designará un delegado de protección de datos personales en los siguientes casos:
1) Cuando el tratamiento se lleve a cabo por quienes conforman el sector público.
2) Cuando las actividades del responsable o encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento
3) Cuando se refiera al tratamiento a gran escala de categorías especiales de datos
4) Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado
La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación.

Registro Nacional de protección de datos personales.- El responsable del tratamiento de datos personales deberá reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales, sobre lo siguiente:

- Identificación de la base de datos o del tratamiento;
- El nombre domicilio legal y datos de contacto del responsable y encargado del tratamiento de datos personales;
- Características y finalidad del tratamiento de datos personales;
- Naturaleza de los datos personales tratados;
- Identificación, nombre, domicilio legal y datos de contacto de los destinatarios de los datos personales, incluyendo encargados y terceros;
- Medios utilizados para implementar los principios, derechos y obligaciones;
- Requisitos y herramientas administrativas técnicas y físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
- Tiempo de conservación de los datos.

CAPÍTULO XI
MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO
Medidas correctivas.- La Autoridad de Protección de Datos Personales dictará medidas correctivas para evitar que se siga cometiendo la infracción y o se repita nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.

Las medidas correctivas podrán consistir, entre otras, en:
1) El cese del tratamiento, bajo determinadas condiciones o plazos;
2) La eliminación de los datos; y,
3) La imposición de medidas técnicas, jurídicas, organizativas o administrativas.

La Autoridad de Protección de Datos Personales, en el marco de esta Ley, dictará, para cada caso; las medidas correctivas, para corregir, revertir o eliminar las conductas contrarias a la presente Ley, su reglamento.

Infracciones leves del Responsable de protección de datos.- Se consideran infracciones leves las siguientes:
1. No tramitar, tramitar fuera del término previsto o negar injustificadamente las peticiones o

quejas realizadas por el titular;
2. No implementar protección de datos desde el diseño y por defecto;
3. No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales;
4. Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;
5. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

Infracciones graves del Responsable de protección de datos tales como:

- No implementar medidas a fin de garantizar el tratamiento de datos personales
- Utilizar información o datos para fines distintos a los declarados;
- Ceder o comunicar datos personales sin cumplir con los requisitos y procedimientos;
- No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales
- No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas;
- No implementar medidas para prevenir, riesgos y las vulneraciones a la seguridad de datos personales que hayan sido identificadas;
- No notificar a la Autoridad de Protección de Datos Personales y al titular, de vulneraciones a la seguridad y protección de datos personales;
- No suscribir contratos que incluyan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
- No mantener actualizado el Registro Nacional de protección de datos personales.
- No designar al delegado de protección de datos personales cuando corresponda;
- No permitir y no contribuir a la realización de auditorías o inspecciones
- Incumplir las medidas correctivas por dicha causa la aplicación de una sanción por infracción leve, e incurrir de forma reiterada en faltas leve.

De las infracciones del Encargado de protección de datos Leves:
1) No colaborar con el responsable del tratamiento datos personales;
2) No facilitar el acceso al responsable del tratamiento de datos personales a toda la información referente al cumplimiento de las obligaciones
3) No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales
4) Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

Graves:
1) Realizar tratamientos de datos personales sin observar los principios y derechos desarrollados en la presente Ley
2) No tratar datos personales de conformidad con lo previsto, en el contrato que mantenga con el responsable del tratamiento de datos personales;
3) No suscribir contratos que contengan cláusulas de confidencialidad y tratamiento adecuado de datos personales
4) No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;

5) No implementar medidas preventivas y correctivas en la seguridad de los datos personales a fin de evitar vulneraciones;
6) No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales, una vez haya culminado su encargo;
7) Proceder a la comunicación de datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente Ley;
8) Incumplir las medidas por dicha causa la aplicación de una sanción por infracción leve; y,
9) No notificar al responsable del tratamiento de datos personales sobre cualquier vulneración de la seguridad de datos personales.

SANCIONES
Sanciones por infracciones leves.- La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas:
1. Servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente Ley, serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;
2. Si el responsable o el encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.
La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos:

a) La intencionalidad
b) Reiteración de la infracción
c) La naturaleza del perjuicio ocasionado
d) Reincidencia

Sanciones por infracciones graves.- Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente Ley serán sancionados con una multa de entre 10 a 20 salarios básicos unificados;

Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

CAPÍTULO XII
AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES
Funciones atribuciones y facultades.- es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley. Funciones, atribuciones y facultades:
1) Ejercer la supervisión, control y evaluación de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales;
2) Ejercer la potestad sancionadora respecto de responsables, delegados, encargados y terceros

3) Conocer, sustanciar y resolver los reclamos interpuestos por el titular o aquellos iniciados de oficio, así como aplicar las sanciones correspondientes;
4) Realizar o delegar auditorias técnicas al tratamiento de datos personales;
5) Emitir normativa general o técnica, criterios y demás actos que sean necesarios
6) Crear, dirigir y administrar el Registro Nacional de Protección de Datos Personales, así como coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento;
7) Promover una coordinación adecuada y eficaz con los encargados de la rendición de cuentas y participar en iniciativas internacionales y regionales para la protección de la protección de los datos personales;
8) Dictar las cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas;
9) Atender consultas en materia de protección de datos personales;
10) Ejercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos;
11) Ejercer la representación internacional en materia, de protección de datos personales;
12) Emitir directrices para el diseño y contenido de la política de tratamiento de datos personales;
13) Establecer directrices para el análisis, evaluación y selección de medidas de seguridad de los datos personales;
14) Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas;
15) Publicar periódicamente una guía de la normativa relativa a la protección de datos personales;
16) Promover e incentivar el ejercicio del derecho a la protección de datos personales, así como la concientización en las personas con especial énfasis en actividades dirigidas a grupos de atención prioritaria tales como niñas niños y adolescentes; 17) Controlar y supervisar el ejercicio del derecho a la protección de datos personales dentro del tratamiento de datos llevado a cabo a través del Sistema Nacional de Registros Públicos

REGLAMENTO DE LA LOPDP
CAPÍTULO I
CONSERVACIÓN DE DATOS PERSONALES
Art. 9.- 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.

CAPÍTULO III
DERECHOS
EL responsable habilitará preferentemente herramientas o canales informáticos simplificados de fácil acceso para atender las solicitudes: plataformas, centros de contacto, líneas telefónicas, entre otros.
Art. 13.- 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.
5. A la solicitud se acompañará los documentos que acrediten la identidad o, en su caso, la representación legal o convencional del titular.

CAPÍTULO X
DELEGADO DE PROTECCIÓN DE DATOS

Art. 49.- 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.

Art. 50.- 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.

Art. 55.- 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.
4. Acreditar experiencia profesional de por lo menos cinco años.

Art. 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 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.
3. 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.

CAPÍTULO XIII
AUTORIDAD DE PROTECCIÓN DE DATOS

Art. 84.- 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.

FIDELITY MARKETING reitera que, como titular o encargado de la información personal compartida con el aliado o proveedor, tiene derecho a conocer, actualizar y rectificar su información personal de las bases de datos de la entidad, así como a solicitar prueba y/o revocar el consentimiento otorgado para el tratamiento de los datos personales, esto último, siempre y cuando no se mantenga una relación contractual u obligación legal vigente con **FIDELITY MARKETING**. Así, el aliado o proveedor acepta conocer la política de Habeas Data y se compromete a que sobre la información personal entregada, se establecerán mecanismos de control, prevención y detección de fraudes de acuerdo con los parámetros de seguridad establecidos en esta política y a atender peticiones, quejas y reclamos que sobre la misma llegare a existir, para lo cual informará de manera inmediata cuando evidencie la ocurrencia de riesgo o falta sobre el uso de la información, al Email: incidencias@fidelitymkt.com o a la línea telefónica 593 2 3944580, o o en la dirección que corresponde al país de operación: https://fidelitymkt.com/.
Que Las **PARTES** aceptan que esta política hace parte integral del contrato de prestación de servicios proveedor o convenio de estipulación en favor de terceros celebrado entre las mismas, por lo cual este documento se acepta con la firma del cualquiera de los anteriores.

Anexo Ley Orgánica de Protección de Datos Personales
Fidelity Marketing Ecuador FMKT S.A.

Fecha de actualización 10 de abril de 2025.