**EXPOSICIÓN DE MOTIVOS**

1. **ANTECEDENTES Y CONTEXTO INTERNACIONAL**

El vertiginoso desarrollo de las tecnologías de la información y la comunicación ha transformado la forma en que se generan, almacenan y comparten datos personales. Hoy más que nunca, el derecho a la privacidad adquiere una nueva dimensión frente a los retos de la era digital, caracterizada por la interconexión global y la transmisión transfronteriza de datos.

La Asamblea General de las Naciones Unidas, mediante la Resolución 68/167 “El Derecho a la Privacidad en la Era Digital” (2013), exhortó a todos los Estados miembros a garantizar el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales, y a adoptar las medidas necesarias para prevenir vulneraciones de este derecho fundamental.

En el ámbito regional, la Organización de los Estados Americanos (OEA) ha impulsado desde 1996 iniciativas, guías y principios orientadores para fortalecer la protección de datos personales en las Américas. Destacan la “Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas” (Comité Jurídico Interamericano, 2015) y los “Principios Actualizados sobre la Privacidad y la Protección de Datos Personales”, adoptados por la Asamblea General de la OEA mediante la resolución AG/RES. 2974 (LI-O/21).

Estos instrumentos reconocen el derecho de toda persona a ser protegida contra injerencias indebidas en su vida privada, su honor, su imagen y su reputación, consolidando así la autodeterminación informativa como un derecho fundamental emergente, que otorga a cada individuo la capacidad de decidir cómo se recopila, utiliza, conserva y transmite su información personal.

1. **MARCO CONSTITUCIONAL Y SITUACIÓN NORMATIVA NACIONAL**

En el ordenamiento jurídico guatemalteco, la Constitución Política de la República establece la base fundamental para la protección de los datos personales y la privacidad. El artículo 24 garantiza la inviolabilidad de la correspondencia, documentos y libros personales, y el secreto de las comunicaciones, extendiendo esta protección a las comunicaciones digitales y a los productos de la tecnología moderna.

El artículo 30 reconoce la publicidad de los actos administrativos, estableciendo límites razonables para proteger datos suministrados por particulares bajo garantía de confidencialidad. Asimismo, el artículo 31 otorga a toda persona el derecho de conocer, rectificar y actualizar la información que de ella conste en archivos o registros estatales, prohibiendo expresamente los registros de filiación política, salvo los previstos para fines electorales.

Actualmente, la Ley de Acceso a la Información Pública (Decreto 57-2008) regula de manera parcial algunos aspectos relacionados con la protección de datos personales, como el *habeas data*, la información confidencial y reservada. Sin embargo, esta regulación resulta insuficiente para responder a la complejidad de los procesos actuales de recolección, tratamiento y transferencia internacional de datos personales. Guatemala carece de una legislación integral y específica que desarrolle principios rectores, derechos, obligaciones, procedimientos y sanciones claros para garantizar la protección efectiva de los datos personales.

1. **DESAFÍOS EMERGENTES Y NECESIDAD DE LA LEY**

El uso masivo de tecnologías de la información y la comunicación, junto con la facilidad de almacenamiento y transmisión de datos a nivel global, han generado una creciente exposición de la población a riesgos como el acceso ilegítimo, la divulgación no autorizada, el uso indebido de información sensible y la suplantación de identidad.

El acceso no autorizado a datos personales puede afectar múltiples esferas de la vida de una persona: su reputación, su integridad patrimonial, su capacidad de acceder a servicios financieros, de salud o educativos, y en última instancia, su dignidad humana.

En este contexto, se vuelve imprescindible establecer un marco normativo que asegure el tratamiento legítimo, proporcional, informado y seguro de los datos personales, y que garantice la responsabilidad de quienes los recaban, almacenan, procesan y transfieren, incluyendo las transferencias transfronterizas.

La iniciativa de Ley de Protección de Datos Personales tiene como finalidad:

* Fortalecer la garantía constitucional del derecho a la privacidad y la protección de los datos personales de toda persona, sin distinción de nacionalidad o residencia.
* Desarrollar los derechos de Acceso, Rectificación, Cancelación y Oposición como herramientas efectivas de la autodeterminación informativa.
* Crear reglas claras para la recolección, almacenamiento, procesamiento y transferencia de datos personales, fijando estándares mínimos de seguridad y períodos de retención razonables.
* Establecer sanciones administrativas proporcionales y disuasorias para quienes incumplan sus obligaciones, y garantizar la existencia de procedimientos ágiles para la protección de los derechos de los titulares.
* Consolidar en una entidad rectora técnica y especializada, la Superintendencia de Transformación Digital, que ejercerá funciones de supervisión, control y sanción de forma independiente.
* Promover la confianza ciudadana en el entorno digital, la innovación tecnológica y la competitividad económica de Guatemala, facilitando la inversión responsable en infraestructura de datos, como centros de almacenamiento y servicios basados en datos.

1. **CONTENIDO DE LA INICIATIVA DE LEY**

La ley propuesta se inspira en principios y mejores prácticas consagrados por la comunidad internacional. Reconoce el Reglamento General de Protección de Datos (RGPD) de la Unión Europea como un referente normativo clave y se alinea con los compromisos adquiridos en el Sistema Interamericano y las resoluciones de la OEA.

Su contenido toma en cuenta la experiencia comparada de América Latina, donde la mayoría de los países ya cuentan con leyes de protección de datos personales armonizadas. La adopción de esta ley permite a Guatemala fortalecer su posición regional, asegurar el flujo legítimo de información con estándares equivalentes y evitar barreras para la cooperación internacional y la inversión.

La Ley de Protección de Datos Personales propuesta se estructura en siete títulos, organizados en capítulos y artículos que desarrollan de forma coherente y progresiva los principios, derechos, obligaciones, procedimientos y medidas institucionales necesarias para garantizar el derecho fundamental a la privacidad y la protección de los datos personales en Guatemala.

El Título I contiene las Disposiciones Generales, distribuidas en dos capítulos.

* El Capítulo I establece el objeto, el ámbito de aplicación de la ley, las reglas para las bases de datos en el país, las excepciones específicas y las condiciones para transferencias transfronterizas.
* El Capítulo II define términos clave y principios rectores que orientan todo el régimen de protección, brindando certeza jurídica sobre conceptos como dato personal, dato sensible, consentimiento, responsable del tratamiento, encargado y transferencia de datos.

El Título II desarrolla los Derechos de los Titulares de Datos Personales y su Ejercicio, divididos en dos capítulos.

* El Capítulo I reconoce los derechos de protección, acceso, rectificación, cancelación o supresión, oposición y limitación del tratamiento, así como sus condiciones y límites.
* El Capítulo II refuerza el carácter irrenunciable de estos derechos, dispone su gratuidad y establece lineamientos para el cobro de costos estrictamente necesarios, asegurando el ejercicio efectivo y asequible de los derechos de los titulares de los datos.

El Título III regula las Obligaciones y Responsabilidades en el Tratamiento de Datos, incluyendo disposiciones sobre la entrega de información a autoridades judiciales, normas de utilización y retención de datos (estableciendo un período mínimo de conservación de cinco años), los requisitos del aviso de privacidad, la notificación de vulneraciones de seguridad, y las formas y requisitos del consentimiento, incluyendo las excepciones y procedimientos de revocación.

El Título IV establece el régimen de Transferencia de Datos Personales, definiendo claramente cuándo una transferencia se considera lícita, las condiciones específicas para transferencias internacionales y las responsabilidades solidarias del remitente y el receptor de los datos, alineando la normativa con estándares internacionales de protección.

El Título V regula a la Entidad Rectora, designando a la Superintendencia de Transformación Digital como autoridad nacional en materia de protección de datos personales. Describe su estructura operativa, su Intendencia especializada y detalla 19 atribuciones clave, que abarcan supervisión, inspección, emisión de certificaciones, guías y programas de capacitación, así como mecanismos de cooperación y coordinación interinstitucional.

El Título VI contiene el Régimen Sancionatorio, con la clasificación de infracciones en leves, graves y gravísimas, y un catálogo claro de sanciones proporcionales, medidas de cobro y lineamientos procedimentales que garantizan el debido proceso y la aplicación efectiva de la ley. Se establece además que los recursos derivados de las multas serán fondos privativos de la Superintendencia, fortaleciendo su independencia operativa.

Finalmente, el Título VII incorpora las Disposiciones Transitorias y Finales, otorgando un plazo de veinticuatro meses para la implementación progresiva de la ley por parte de responsables y encargados del tratamiento, y seis meses para la emisión de los reglamentos y guías técnicas por la entidad rectora. Se dispone además la vigencia efectiva de la ley treinta días después de su publicación en el Diario Oficial.

En conjunto, esta estructura permite una regulación integral, coherente y técnicamente robusta para fortalecer la protección de los datos personales, promover la confianza en el entorno digital y garantizar el respeto de derechos fundamentales en consonancia con la Constitución Política de la República de Guatemala y los tratados internacionales ratificados por el país.

Por todo lo expuesto, se somete a consideración del Honorable Congreso de la República de Guatemala la aprobación de la Ley de Protección de Datos Personales, como una acción impostergable para garantizar el ejercicio pleno de los derechos fundamentales en la era digital, promover la competitividad del país y consolidar la confianza ciudadana en el uso responsable de la información.

**DECRETO NÚMERO \_\_\_-2025**

**EL CONGRESO DE LA REPÚBLICA DE GUATEMALA**

**CONSIDERANDO**

Que la Constitución Política de la República de Guatemala, en su artículo 24, garantiza la inviolabilidad de la correspondencia, documentos y libros personales, y el secreto de las comunicaciones, reconociendo con ello el derecho a la privacidad, incluso en el contexto de las nuevas tecnologías de la información y la comunicación.

**CONSIDERANDO**

Que la protección de los datos personales y del derecho a la privacidad es un deber del Estado y un derecho inherente a la dignidad humana, consagrado en instrumentos internacionales suscritos y ratificados por Guatemala, tales como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Declaración Americana de los Derechos y Deberes del Hombre, y la Convención Americana sobre Derechos Humanos.

**CONSIDERANDO**

Que el artículo 31 del texto constitucional reconoce el derecho de toda persona a conocer lo que de ella conste en archivos o registros estatales, a conocer la finalidad de esa información y a solicitar su corrección o actualización, prohibiendo expresamente los registros de filiación política, salvo los propios de las autoridades electorales y partidos políticos.

**CONSIDERANDO**

Que el avance de la digitalización, el uso intensivo de tecnologías de la información y el creciente intercambio de datos personales entre entidades públicas y privadas exigen un marco normativo integral que garantice los derechos de las personas frente al tratamiento de sus datos, especialmente en contextos de interconexión y transferencia internacional.

**CONSIDERANDO**

Que la protección adecuada de los datos personales no solo fortalece el ejercicio de derechos fundamentales, sino que también genera condiciones favorables para la innovación, la confianza ciudadana en el entorno digital, la competitividad económica y la atracción de inversiones tecnológicas.

**POR TANTO**

En ejercicio de las atribuciones que le confiere el artículo 171 literal a) de la Constitución Política de la República de Guatemala,

**DECRETA**

La siguiente

**LEY DE PROTECCIÓN DE DATOS PERSONALES**

**TÍTULO I: DISPOSICIONES GENERALES**

**Capítulo I: Objeto y Ámbito de Aplicación**

**Artículo 1. Objeto de la Ley.** Esta Ley tiene por objeto garantizar la protección de los datos personales, estableciendo los principios, derechos, obligaciones y procedimientos que regulan su tratamiento, para salvaguardar la privacidad, dignidad y derechos fundamentales de las personas.

**Artículo 2. Ámbito de Aplicación.** La presente Ley es aplicable a toda persona individual o jurídica, de derecho público o privado, que trate datos personales dentro del territorio de Guatemala.

**Artículo 3. Bases de Datos.** Las bases de datos que se encuentren en el territorio de la República que almacenen o contengan datos personales de nacionales o extranjeros, o cuyo responsable del tratamiento de los datos esté domiciliado en el país, quedan sujetas a las disposiciones establecidas en esta Ley y su reglamentación.

Se excluyen de esta normativa las bases de datos reguladas por normas especiales, siempre que estas establezcan estándares técnicos mínimos necesarios para garantizar la protección y tratamiento correcto de los datos personales.

El almacenamiento o transferencia transfronteriza de datos personales confidenciales, sensibles o restringidos originados o almacenados dentro de la República será permitido, siempre que el responsable del almacenamiento de los datos cumpla con los estándares de protección de datos personales exigidos por esta Ley, o pueda demostrar que cumple con estándares y normas equivalentes o superiores.

Se exceptúan de los requerimientos del párrafo anterior los siguientes casos:

1. Cuando el titular haya otorgado su consentimiento para la transferencia.
2. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrarse por el interesado o en interés de este.
3. Cuando se trate de transferencias bancarias, dinerarias o bursátiles del mercado de valores.
4. Cuando la transferencia de información sea requerida en cumplimiento de tratados internacionales ratificados por la República de Guatemala.

En todos los casos, el tratamiento o transferencia de datos personales realizada a través de internet o cualquier otro medio de comunicación electrónica, digital o física, deberá cumplir con estándares, normas, certificaciones, protocolos, medidas técnicas y de gestión informática adecuados para preservar la seguridad de los datos.

**Artículo 4. Excepciones.** Se excluyen del ámbito de aplicación de esta Ley:

1. Los datos que proporcione una persona natural para actividades exclusivamente personales o domésticas.
2. Los datos que proporcionen autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
3. Los datos de carácter financiero y crediticio, que podrán ser regulados por normativa especial.
4. Los datos los relativos a la seguridad nacional.
5. Cuando se trate de datos relacionados con organismos internacionales, en cumplimiento de lo dispuesto en los tratados y convenios vigentes ratificados por el país.
6. Los resultantes de información obtenida mediante un procedimiento previo de disociación o anonimización, de manera que el resultado no pueda asociarse al titular de los datos personales.

**Capítulo II: Definiciones y Principios Rectores**

**Artículo 5. Definiciones.** Para los efectos de esta ley, los términos siguientes se entenderán así:

1. **Almacenamiento de datos.** Conservación o custodia de datos en una base de datos establecida en cualquier medio provisto, incluido el de las Tecnologías de la Informaci6n y la Comunicación (TICs).
2. **Base de datos.** Conjunto ordenado de datos de cualquier naturaleza, cualquiera que sea la forma o modalidad de su creaci6n, organización o almacenamiento, que permite relacionar los datos entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su responsable.
3. **Consentimiento**. Manifestación de la voluntad del titular de los datos, mediante la cual se efectúa el tratamiento de estos.
4. **Datos confidenciales.** Aquellos datos que por naturaleza no deben ser de conocimiento público o de terceros no autorizados, incluyendo aquellos que estén protegidos por la ley, por acuerdos de confidencialidad o no divulgación, a fin de salvaguardar información. En los casos de la Administración Pública, son aquellos datos cuyo tratamiento está limitado para fines de esta Administración o si se cuenta con el consentimiento expreso del titular, sin perjuicio de lo dispuesto por leyes especiales o por las normativas que las desarrollen. Los datos confidenciales siempre serán de acceso restringido.
5. **Dato anónimo.** Aquel dato cuya identidad no puede ser establecida por medios razonables o el nexo entre este y la persona natural a la que se refiere.
6. **Dato caduco**. Aquel dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiera norma expresa, por el cambio de los hechos o circunstancias que consigna.
7. **Dato personal.** Cualquier información concerniente a personas naturales, que las identifica o las hace identificables.
8. **Dato disociado.** Aquel dato que no puede asociarse al titular ni permitir por su estructura, contenido o grado de desagregación la identificación de la persona, sea esta natural.
9. **Dato sensible.** Aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros, sujetos a regulación y dirigidos a identificar de manera unívoca a una persona natural.
10. **Procedimiento de disociación o anonimización.** Todo tratamiento de datos que impide que la información disponible en la base de datos pueda asociarse a persona natural determinada o determinable.
11. **Responsable del tratamiento de los datos.** Persona natural o jurídica, de derecho público o privado, lucrativa o no, que le corresponde las decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos.
12. **Encargado del tratamiento de datos.** Persona individual o jurídica, que de manera conjunta o separada, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
13. **Titular de los datos.** Persona natural a la que se refieren los datos.
14. **Transferencia de datos.** Dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extrafronterizo, los datos a personas naturales o jurídicas distintas del titular, ya sean determinadas o indeterminadas.
15. **Tratamiento de datos.** Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir o cancelar datos, o utilizarlos en cualquier otra forma.

**TÍTULO II: DERECHOS DE LOS TITULARES DE DATOS PERSONALES Y SU EJERCICIO**

**Capítulo I: Derechos de los titulares de los datos**

**Artículo 6. Derecho a la protección de los datos personales.** Toda persona, por sí misma o por medio de su representante con facultades especiales, tendrá derecho a conocer si sus datos personales están siendo procesados para garantizar la protección de los mismos.

Asimismo, tendrán derecho a obtener una reproducción inteligible de sus datos personales y a transferirlos cuando así lo consideren pertinente.

Tratándose de los datos personales de personas fallecidas, corresponderá a sus herederos o sucesores ejercer los derechos correspondientes, debiendo acreditar con documentación su calidad de heredero o sucesor.

**Artículo 7. Derecho de acceso a datos personales.** El titular de datos personales tendrá derecho a obtener toda la información que sobre sí mismo se encuentre en bases de datos o registros físicos. Este derecho será ejercido de manera gratuita, conforme a lo establecido en la presente ley.

La información deberá ser suministrada:

1. En forma clara y sin codificaciones, acompañada de una explicación de los términos utilizados, los sujetos que han consultado dicha información y con qué propósito.
2. De manera completa, salvo que los datos hayan sido seudonimizados o disociados, dejando constancia de estas circunstancias.

El acceso se podrá realizar mediante consulta directa del titular o su representante, previa verificación de su identidad, o mediante sistemas tecnológicos que permitan una lectura clara y comprensible.

**Artículo 8. Derecho de rectificación.** El titular de los datos personales tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos cuando estos sean inexactos, incompletos o no se encuentren actualizados. Además, podrá solicitar la rectificación y actualización de los datos cuando hayan sido tratados en incumplimiento de las disposiciones de la presente ley.

Para ejercer este derecho, el titular deberá ofrecer documentación que acredite la procedencia de la rectificación o informar la ubicación donde se encuentren almacenados los datos.

El responsable del tratamiento deberá cumplir con lo solicitado de manera gratuita, resolviendo en un plazo máximo de veinte días hábiles contados a partir de la recepción de la solicitud. El incumplimiento de esta obligación habilitará al interesado para presentar una denuncia ante la entidad rectora, la cual garantizará sus derechos.

Durante el proceso de verificación para rectificar la información, los datos objeto de análisis deberán ser bloqueados, indicando que se encuentran en proceso de revisión o actualización, según lo solicitado.

**Artículo 9. Derecho de cancelación o supresión.** El titular o sus representantes podrán solicitar la eliminación de los datos personales que le conciernan cuando se cumpla al menos una de las siguientes condiciones:

1. Los datos ya no sean necesarios con relación a los fines para los cuales fueron tratados.
2. El titular retire su consentimiento, siempre que dicho consentimiento haya sido el fundamento para el tratamiento.
3. El titular se oponga al tratamiento y no existan motivos legítimos prevalentes para conservar los datos.
4. Los datos personales hayan sido obtenidos o tratados ilícitamente.
5. La supresión sea necesaria para cumplir una obligación legal aplicable al responsable.
6. Los datos personales hayan sido obtenidos en relación con servicios dirigidos a menores.

El derecho de cancelación no procederá en los siguientes casos:

1. Cuando el ejercicio de este derecho perjudique derechos o intereses legítimos de terceros.
2. Cuando exista una obligación legal que exija la conservación de los datos.
3. En casos necesarios para el ejercicio de la libertad de expresión, información o prensa.
4. Cuando los datos hayan sido disociados o se utilicen para fines de investigación científica, histórica o estadística, siempre que se garanticen medidas de protección adecuadas.
5. Cuando se trate de datos de carácter crediticio.

**Artículo 10. Derecho de oposición.** El titular tendrá derecho a solicitar el cese del tratamiento de sus datos personales, incluida la elaboración de perfiles con fines comerciales o de mercadotecnia directa.

El derecho de oposición no será aplicable cuando:

1. El tratamiento sea necesario para cumplir una misión realizada en interés público o en el ejercicio de facultades otorgadas al responsable.
2. El tratamiento sea necesario para satisfacer intereses legítimos del responsable o un tercero, siempre que no prevalezcan los derechos fundamentales del titular, especialmente en el caso de menores de edad.

**Artículo 11. Derecho a la limitación del tratamiento.** El titular podrá solicitar la limitación del tratamiento de sus datos personales cuando:

1. Impugne la exactitud de los datos, durante el plazo necesario para su verificación.
2. El tratamiento sea ilícito y el titular se oponga a la supresión, optando por la limitación del uso.
3. El responsable ya no necesite los datos, pero el titular los requiera para la formulación, ejercicio o defensa de reclamaciones.
4. El titular haya manifestado oposición al tratamiento, mientras se verifica si los motivos del responsable prevalecen sobre los del titular.

La limitación permanecerá vigente mientras subsistan las razones que motivaron su solicitud.

**Capítulo II: Ejercicio de los Derechos**

**Artículo 12. Ejercicio irrenunciable de los derechos del titular.** El titular de los datos personales podrá ejercer, en cualquier momento, los derechos reconocidos en la presente Ley. Estos derechos son de carácter irrenunciable, garantizando su aplicación plena e inalienable en todas las circunstancias, salvo las excepciones expresamente establecidas en la ley.

Ningún acuerdo, acto jurídico o disposición administrativa podrá limitar o restringir el ejercicio de los derechos del titular sobre sus datos personales. Cualquier estipulación en contrario será nula de pleno derecho.

En el caso de que existan disposiciones legales específicas que establezcan limitaciones, estas deberán interpretarse de manera restrictiva y únicamente en el marco de lo dispuesto por la normativa vigente aplicable.

**Artículo 13. Gratuidad del ejercicio de los derechos.** El ejercicio de los derechos que reconoce esta ley es gratuito y sólo podrán realizarse cobros de los costos de reproducción, certificación o envío. La reproducción o envío de la información será sufragada por el solicitante, sin embargo, su valor no podrá ser superior al de los materiales utilizados o de los costos de remisión. El responsable deberá publicar y comunicar a los interesados de los costos de reproducción y envío de sus datos personales.

En caso de que los datos personales deban entregarse en dispositivos magnéticos o electrónicos, el interesado deberá aportar el medio en que serán almacenados. Para el envío por vía electrónica no tendrá costo alguno, siempre y cuando sea posible realizar a través de dicho mecanismo.

**TÍTULO III: OBLIGACIONES Y RESPONSABILIDADES EN EL TRATAMIENTO DE DATOS**

**Capítulo I: Reglas Generales para el Tratamiento de Datos**

**Artículo 14. Información a autoridades judiciales.** Los responsables de bases de datos deberán entregar a las autoridades judiciales competentes la información relacionada al almacenamiento o transferencia de datos personales que sea debidamente solicitada para el aseguramiento del cumplimiento de la Ley.  En cualquier caso, la solicitud tendrá que estar debidamente proporcionada, no admitiéndose en ningún caso solicitudes masivas de información sobre datos personales.

En todo caso, dicha solicitud deberá ir dirigida al responsable de la base de datos o al titular de los datos, que es el único que puede responderla, ordenando en su caso al responsable de los datos o quien lo tuviera por mandato o encargo de dicho responsable, que entregue los datos a la autoridad judicial competente.

**Artículo 15. Utilización y retención de Datos Personales.** Los responsables del tratamiento de datos solo podrán transferir información sobre estos cuando cuenten con el consentimiento previo, informado e inequívoco del titular, salvo las excepciones establecidas en esta Ley o en las leyes especiales.

El consentimiento otorgado por el titular de los datos deberá ser trasladado por la persona que lo obtuvo al encargado o responsable del tratamiento de datos.

Salvo disposición legal expresa o consentimiento expreso en contrario, los responsables y encargados del tratamiento podrán conservar los datos personales por un período mínimo de cinco (5) años, contado a partir de la fecha de su recolección o de la última actualización efectuada por el titular.

**Artículo 16. Aviso de Privacidad.** Previo al tratamiento y recolección de datos se debe informar al titular sobre los términos bajo los cuales serán tratados sus datos personales mediante un aviso de privacidad.

El contenido del aviso de privacidad deberá incluir, como mínimo, la siguiente información:

* 1. El domicilio del responsable.
  2. Los datos personales que serán sometidos a tratamiento, identificando aquellos que sean sensibles.
  3. El fundamento legal que faculta al responsable para realizar el tratamiento.
  4. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento del titular.
  5. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos que esta ley reconoce y los mecanismos para revocar el consentimiento.
  6. Indicación del nombre del delegado y lugar o medios para presentar la solicitud de derechos que reconoce esta ley.
  7. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.
  8. Los datos de contacto de la entidad subcontratada encargada del tratamiento de datos personales, en caso de existir.
  9. El uso de cookies, en caso de que aplique.

El aviso de privacidad podrá ser difundido por medios físicos o electrónicos al titular de los datos personales, debiendo ser redactado y estructurado de manera clara y sencilla. En ningún caso, el responsable podrá eximirse de la obligación de comunicarlo por escrito al titular al momento de que este otorgue su consentimiento informado para que sus datos puedan ser tratados.

**Artículo 17. Notificación de Vulneraciones a la Seguridad de los Datos Personales.** Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, incluyendo daño, pérdida, alteración, destrucción, acceso ilegítimo o cualquier uso ilícito o no autorizado, aun cuando ocurra de manera accidental, deberá notificar el hecho a la Superintendencia de Transformación Digital y al titular o titulares de los datos que hayan sido afectados.

Esta notificación deberá realizarse en un plazo máximo de setenta y dos (72) horas desde que se tuvo conocimiento de la vulneración.

La notificación deberá incluir, al menos, la siguiente información:

* 1. La naturaleza del incidente.
  2. Los datos personales comprometidos.
  3. Las acciones correctivas realizadas de forma inmediata.
  4. Las recomendaciones al titular sobre medidas para proteger sus intereses.
  5. Los medios disponibles para que el titular obtenga más información.

El responsable deberá documentar toda vulneración ocurrida, incluyendo fecha, motivo, hechos relacionados, efectos e implicaciones, así como las medidas correctivas adoptadas para evitar nuevas vulneraciones.

**Artículo 18. Formas del Consentimiento.** El consentimiento para el tratamiento de datos personales deberá ser expreso y podrá manifestarse de forma verbal, escrita o a través de signos inequívocos, siempre que quede constancia en medios físicos, electrónicos o tecnológicos.Tratándose de datos personales sensibles, el consentimiento deberá ser otorgado por escrito.

El responsable del tratamiento de datos es quien debe obtener el consentimiento del titular de los datos y trasladarlo al encargado del tratamiento de datos, cuando corresponda.

**Artículo 19. Requisitos del Consentimiento.** El consentimiento del titular o su representante para el tratamiento de datos personales, especialmente datos sensibles, deberá ser:

* 1. Libre: Sin error, dolo, mala fe, violencia u otra afectación a la voluntad.
  2. Específico: Para una o varias finalidades determinadas.
  3. Informado: Con conocimiento previo del uso de los datos y sus consecuencias.
  4. Expreso: Inequívoco y demostrable, ya sea en medios físicos o electrónicos.
  5. Individualizado: Debe existir un consentimiento por cada titular de datos personales.

**Artículo 20. Excepciones al Consentimiento.** No será necesario el consentimiento para el tratamiento de datos personales en los siguientes casos:

* 1. Cuando los datos estén en fuentes de acceso público y no sean sensibles.
  2. Para la prestación de servicios sanitarios o gestión médica en situaciones de emergencia, bajo secreto profesional.
  3. Cuando sean de carácter económico, financiero, bancario, crediticio o comercial.
  4. En situaciones de emergencia que puedan dañar a un individuo o proteger intereses vitales.
  5. Cuando los datos sean disociados.
  6. En casos de personas reportadas como desaparecidas, conforme a la legislación aplicable.
  7. Cuando deriven de una relación contractual, científica o profesional.
  8. Cuando sean datos personales que el titular haya hecho manifiestamente públicos.
  9. Para fines de investigación científica, histórica o estadística, siempre que no obstaculicen gravemente estos fines y los datos sean seudonimizados.

**Artículo 21. Revocación del Consentimiento.** El titular podrá revocar su consentimiento en cualquier momento de forma expresa, sin efectos retroactivos, mediante mecanismos gratuitos, expeditos y sencillos dispuestos por el responsable.

Esta revocación no afectará el tratamiento basado en otras causales previstas en esta ley que justifiquen su licitud.

**Artículo 22. Trámite de la Revocación.** Una vez recibida la solicitud de revocación, el delegado contará con un plazo de cinco (5) días hábiles para resolver. En caso de que un encargado del tratamiento también gestione los datos, el delegado deberá comunicarle la resolución en el mismo plazo para su ejecución inmediata.

**Artículo 23. Negativa a la Revocación.** En caso de negativa del responsable a tramitar la revocación, el titular podrá presentar una denuncia ante la Entidad Rectora sin perjuicio de otras acciones legales aplicables.

**TÍTULO IV: TRANSFERENCIA DE DATOS PERSONALES**

**Artículo 24. Transferencias de Datos Lícitas.** Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes:

1. Que cuente con el consentimiento del titular de los datos.
2. Que el país u organismo internacional o supranacional receptor proporcione un nivel de protección equivalente o superior al establecido en esta ley.
3. Que esté prevista en una ley o tratado en los que Guatemala sea parte.
4. Que sea necesaria para la prevención o diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.
5. Que sea efectuada a cualquier sociedad del mismo grupo económico del responsable del tratamiento, siempre que los datos personales no sean utilizados para finalidades distintas a aquellas que originaron su recolección.
6. Que sea necesaria en virtud de un contrato celebrado o por celebrar en interés inequívoco del titular de los datos, por el responsable del tratamiento y un tercero.
7. Que sea necesaria o legalmente exigida para la salvaguarda de un interés público o para la representación legal del titular de los datos personales o la administración de justicia.
8. Que sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o en caso de colaboración judicial internacional.
9. Que sea requerida para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos.
10. Que sea requerida para concretar transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la legislación que les resulte aplicable.
11. Que tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el lavado de activos, los delitos informáticos, la pornografía infantil y el narcotráfico.
12. Que el responsable del tratamiento que transfiere los datos y el destinatario adopten mecanismos de autorregulación vinculante, siempre que éstos sean acordes a las disposiciones previstas en esta ley.
13. Que se realice en el marco de cláusulas contractuales que contengan mecanismos de protección de los datos personales acordes con las disposiciones previstas en esta ley, siempre que el titular sea parte.

El responsable de los datos que transfiere los mismos y el receptor de los datos personales serán solidariamente responsables por la licitud del tratamiento de los datos transferidos.

**TÍTULO V: ENTIDAD RECTORA**

**Capítulo I: Designación**

**Artículo 25. Designación.** Para efectos de la presente ley, se designa a la Superintendencia de Transformación Digital, que se podrá abreviar STD, creada mediante la Ley Marco para la Transformación Digital, como la autoridad nacional en materia de protección de datos personales. La STD ejercerá la función de ente rector, supervisor y sancionador en materia de protección de datos.

La STD ejercerá sus atribuciones a través de la Intendencia especializada en Protección de Datos Personales, la cual se estructurará mediante su reglamento interno, garantizando que cuente con personal técnico especializado, presupuesto propio y capacidad operativa suficiente para el cumplimiento de sus funciones.

La STD podrá coordinar con otras instituciones estatales, internacionales y de la sociedad civil, la implementación de estrategias, reglamentos y mecanismos que garanticen el efectivo resguardo de los datos personales.

**Capítulo II: Atribuciones sobre la protección de datos**

**Artículo 26. Atribuciones.** La Superintendencia de Transformación Digital tendrá las siguientes atribuciones en materia de protección de datos personales:

1. Controlar, inspeccionar y supervisar a las instituciones obligadas en el marco de aplicación de la presente ley.
2. Ejercer la potestad sancionadora en materia de protección de datos personales, conforme a la presente ley.
3. Garantizar la efectiva protección de los datos personales de acuerdo con las facultades que le otorga esta ley.
4. Promover programas de divulgación de esta ley dirigidos a los sujetos obligados al cumplimiento de la misma y a la población en general, con énfasis en sensibilizar sobre los riesgos, normas, garantías y derechos en el tratamiento de datos personales, priorizando la niñez, adolescencia y adultos mayores.
5. Resolver controversias entre titulares, responsables y encargados del tratamiento en relación con la clasificación y desclasificación de datos personales sensibles.
6. Proporcionar apoyo técnico a los responsables del tratamiento en la elaboración y ejecución de programas de protección de datos personales.
7. Cooperar y compartir información con otras autoridades de control en el ejercicio de sus funciones, garantizando que no se comprometan datos personales o sensibles, y prestando asistencia mutua para asegurar coherencia en la aplicación de esta ley.
8. Dictar políticas de actuación sobre el manejo, mantenimiento, y protección de los datos personales, considerando las buenas prácticas internacionales aplicables.
9. Crear mecanismos de certificación y desarrollar sellos o marcas relacionados con la protección de datos personales, así como autorizar a terceros para emitir certificaciones en la materia.
10. Revisar periódicamente las certificaciones expedidas y, de ser procedente, realizar auditorías anuales sobre estas.
11. Impartir capacitaciones a instituciones públicas y privadas, así como a sus miembros, en protección de datos personales y su gestión.
12. Emitir guías de implementación de esta ley, que deberán publicarse en la página web, redes sociales y otros medios pertinentes.
13. Asesorar y cooperar con los entes obligados para asegurar el cumplimiento de esta ley.
14. Recomendar cláusulas contractuales que garanticen la protección de datos personales según esta ley.
15. Elaborar modelos de formularios para solicitudes de los derechos de los titulares de los datos y revocación de consentimiento.
16. Realizar o apoyar investigaciones científicas o académicas sobre la aplicación de esta ley.
17. Asistir y asesorar a los ciudadanos sobre los alcances de esta ley y los mecanismos legales para la defensa de los derechos que garantiza.
18. Solicitar a entidades públicas y privadas información sobre antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos personales, garantizando la seguridad y confidencialidad de la información suministrada.
19. Realizar todas aquellas otras acciones que le confiera esta ley, sus reglamentos u otras disposiciones legales aplicables.

**TÍTULO VI: RÉGIMEN SANCIONATORIO**

**Capítulo I: Infracciones**

**Artículo 27. Clasificación de las Infracciones.** Las infracciones a la presente ley se clasifican en leves, graves y gravísimas, conforme a los siguientes criterios:

a) **Infracciones Leves:**

1. No remitir información requerida por la Superintendencia de Transformación Digital dentro de los plazos establecidos.
2. No contar con medidas básicas de seguridad para la recolección, almacenamiento o transmisión de datos.

b) **Infracciones Graves:**

1. Tratar datos personales sin contar con el consentimiento válido cuando sea exigible.
2. Incumplir los principios y garantías dispuestos en esta ley.
3. Obstaculizar o restringir injustificadamente el ejercicio de los derechos ARCO-POL.
4. Almacenar datos sin condiciones de seguridad adecuadas.
5. No notificar vulneraciones de seguridad conforme a lo establecido.
6. Incumplir requerimientos formales o inspecciones de la autoridad competente.

c) **Infracciones Gravísimas:**

1. Tratar datos sensibles sin consentimiento válido o de forma dolosa.
2. Transferir datos personales internacionalmente en violación de esta ley.
3. Reincidir en infracciones graves en un plazo inferior a dos años.
4. Destruir, alterar o falsear información para evadir responsabilidades.

**Capítulo II: Sanciones**

**Artículo 28. Sanciones.** En caso de cometerse alguna infracción a la Ley, se impondrán las siguientes sanciones:

1. Para infracciones leves: Multa de hasta cien (100) salarios mínimos para actividades no agrícolas.
2. Para infracciones graves: Multa de hasta quinientos (500) salarios mínimos para actividades no agrícolas.
3. Para infracciones gravísimas: Multa de hasta mil (1,000) salarios mínimos para actividades no agrícolas.

**Artículo 29. Procedimiento.** La entidad rectora estará facultada para investigar y sancionar a las personas naturales o jurídicas responsables del tratamiento de datos personales, así como a los encargados de bases de datos, cuando se determine que han infringido los derechos del titular.

1. Inicio del Procedimiento: El procedimiento podrá iniciarse de oficio o a solicitud de parte interesada.
2. Audiencia y Prueba: Se concederá un plazo de cinco (5) días hábiles para la audiencia del presunto infractor. Si se solicita la apertura a prueba, esta se otorgará por un plazo perentorio de diez (10) días hábiles.
3. Resolución y Notificación: La resolución deberá ser emitida dentro de los cinco (5) días siguientes al vencimiento del periodo de prueba y notificada en un plazo no mayor a diez (10) días hábiles.
4. Impugnación: Las decisiones serán impugnables mediante recurso de revocatoria, conforme a la Ley de lo Contencioso Administrativo.
5. Convenios de Pago: La Superintendencia de Transformación Digital podrá suscribir convenios de pago de hasta doce (12) meses, previa solicitud del sancionado y justificación de las causas que impidan el pago inmediato.
6. Cobro Coactivo: Las multas impuestas serán cobradas por la vía económico-coactiva, sirviendo como título ejecutivo la certificación de la resolución que las imponga.

Los recursos obtenidos de las multas se considerarán fondos privativos de la Superintendencia de Transformación Digital.

**TÍTULO VII: DISPOSICIONES TRANSITORIAS Y FINALES**

**Artículo 30. Implementación.** Las personas individuales y jurídicas, públicas o privadas, responsables o encargadas del tratamiento de datos personales deberán adecuar sus procesos, sistemas, políticas y procedimientos a lo dispuesto en esta ley dentro del plazo de veinticuatro meses contados a partir de su entrada en vigor.

**Artículo 31. Reglamentación.** La Superintendencia de Transformación Digital deberá emitir los reglamentos necesarios para la implementación de esta ley dentro de los seis (6) meses siguientes a su entrada en vigor. Además deberá emitir guías técnicas para facilitar la implementación progresiva de las obligaciones en materia de protección de datos que establece esta ley.

**Artículo 32. Vigencia.** La presente ley entrará en vigor treinta (30) días después de su publicación en el Diario Oficial.