POLÍTICA DE PRIVACIDAD

1. PROPÓSITO DEL USO:

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una empresa, pública o privada, jurídica o natural, ésta se hace mediante el responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Si bien, la responsabilidad del tratamiento de los datos recae en el responsable del

tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la empresa responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales han de conocer la normativa de protección de datos, la política de protección de datos de la organización y el Manual Interno de Seguridad; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

2. CUMPLIMIENTO

Para garantizar el cumplimiento de sus obligaciones de seguridad en la información, EVOLUCION LEGAL S.A.S. cuenta con una persona responsable velar por desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en el Manual Interno de Seguridad.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, el personal propio de EVOLUCION LEGAL S.A.S.

Todos los usuarios identificados en el presente documento de seguridad están obligados a cumplir con las medidas de seguridad establecidas para el

tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la Ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

3. TIPOS DE DATOS:

3.1. Dato personal

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

3.2. Dato público

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o del servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

3.3. Dato semiprivado

Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

3.4. Dato privado

Es un dato personal que por su naturaleza íntima o reservada sólo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y

expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

3.5. Dato sensible

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

4. NORMATIVIDAD

4.1. LEY 1581 DE 2012

Expedida por el congreso de la republica

Titulo: "Por la cual se dictan disposiciones generales para la protección de datos personales".

Aplicación: Por medio de la cual se va a desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma explica por qué se recopilan los datos y para qué se utilizarán.

4.2. DECRETO 1377 de 2013

Titulo: "Por medio del cual se reglamenta parcialmente la ley 1581 de 2012"

Expedido por el presidente de la República de Colombia.

Aplicación: Mediante la cual se reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

4.3. DECRETO 1074 DE 2015

Titulo: "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo."

Expedido por el presidente de la República de Colombia.

Aplicación: El Ministerio de Comercio, Industria y Turismo tiene como objetivo primordial dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con la competitividad, integración y desarrollo de los sectores productivos de la industria.

5. . DEFINICIONES ESTABLECIDAS EN EL ARTÍCULO 3 DE LA LEPD Y EL CAPÍTULO 25 SECCIÓN 1 ARTÍCULO 2.2.2.25.1.3 DEL DECRETO 1074 DE 2015.

5.1. Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

5.2. Autenticación: Procedimiento de verificación de la identidad de un usuario.

5.3. Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

5.4. Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

5.5. Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

5.6. Contraseña: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

5.7. Control de acceso: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.

5.8. Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación.

5.9. Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

5.10. Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

5.11. Datos sensibles: Se entiende por datos sensible aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su

discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

5.12. Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

5.13. Identificación: Proceso de reconocimiento de la identidad de los usuarios.

5.14. Incidencia: Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

5.15. Perfil de usuario: Grupo de usuarios a los que se da acceso.

5.16. Recurso protegido: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

5.17. Responsable de seguridad: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.

5.18. Sistema de información: Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.

5.19. Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

5.20. Soporte: Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.

5.21. Usuario: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

5.22. Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

5.23. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

5.24. Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

5.25. Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

6. PRINCIPIOS DE LA PROTECCIÓN DE DATOS.

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el tratamiento de datos personales que se han de aplicar, de

manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

6.1. Principio de legalidad: El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), el Decreto 1377 de 2013, el Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

6.2. Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

6.3. Principio de libertad: El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento.

El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley de Protección de Datos

(LEPD):

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

b) Datos de naturaleza pública.

c) Casos de urgencia médica o sanitaria.

d) Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.

e) Datos relacionados con el registro civil de las personas.

6.4. Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y

comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

6.5. Principio de transparencia: En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

a) El tratamiento al cual será sometidos sus datos y la finalidad del mismo.

b) El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.

c) Los derechos que le asisten como Titular.

d) La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

6.6. Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley de Protección de Datos (LEPD) y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

6.7. Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su

adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el Manual Interno de Seguridad, de obligado cumplimiento para todo usuario y personal de EVOLUCION LEGAL S.A.S. Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

6.8. Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de la misma.

7. Categorías especiales de datos.

7.1. Datos sensibles.

Los datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Según el artículo 6 de la Ley Estatuaria de Protección de datos Personales (LEPD), se prohíbe el tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b) El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c) El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

d) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e) El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

7.2. Derechos de los niños, niñas y adolescentes.

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos: - Que responda y respete el interés superior de los niños, niñas y adolescentes. - Que se asegure el respeto de sus derechos fundamentales. Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la

privacidad y protección de su información personal y la de los demás. Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1377 de 2013. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

7.3. Derechos de los Titulares.

De acuerdo con el artículo 8 de la LEPD y al capítulo 25 sección 4 del decreto 1074 de 2015, los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

a) Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.

b) Por sus causahabientes, quienes deberán acreditar tal calidad.

c) Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.

d) Por estipulación a favor de otro y para otro.

e) Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

8. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Los derechos del Titular son los siguientes:

8.1. Derecho de acceso o consulta: Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud,

respecto al origen, uso y finalidad que les han dado a sus datos personales.

8.2. Derechos de quejas y reclamos: La Ley distingue cuatro tipos de reclamos:

a. Reclamo de corrección: El derecho del Titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan al error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
b. Reclamo de supresión: El derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
c. Reclamo de revocación: El derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
d. Reclamo de infracción: El derecho del Titular a solicitar que se subsane el

incumplimiento de la normativa en materia de Protección de Datos.

8.3. Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento: Salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.

8.4. Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones: El Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

9. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO.

De acuerdo al artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de EVOLUCION LEGAL S.A.S., en los términos y condiciones recogidos en la misma. No será necesaria la autorización del Titular cuando se trate de: Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial. - Datos de naturaleza pública. - Casos de urgencia médica o sanitaria.

10. RESPONSABLE DEL TRATAMIENTO.

El responsable del tratamiento de las bases de datos objeto de esta política es EVOLUCION LEGAL S.A.S, cuyos datos de contacto son:

Dirección: Cra. 43A #7-50 Medellín. Colombia.

Correo electrónico: gerenciacomercial@evolucionlegalsas.com

Teléfono: 3127496591

10.1. Las obligaciones del responsable del tratamiento.

Las obligaciones en materia de seguridad de los datos de EVOLUCION LEGAL S.A.S, son las siguientes:

a) Coordinar e implantar las medidas de seguridad recogidas en el Manual Interno de Seguridad.

b) Difundir el referido documento entre el personal afectado.

c) Mantener el Manual Interno de Seguridad actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la empresa, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.

d) Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos en el Manual Interno de Seguridad.

e) Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.

f) Autorizar, salvo delegación expresa a usuarios autorizados e identificados en el

Manual Interno de Seguridad, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel y el uso de módems y las descargas de datos.

g) Verificar semestralmente la correcta aplicación del procedimiento de copias de

respaldo y recuperación de datos.

h) Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.

i) Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas

j) Realizar una auditoría, interna o externa, para verificar el cumplimiento de las

medidas de seguridad en materia de protección de datos, al menos cada año.