POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES
DE LA FISCALÍA GENERAL DE JUSTICIA EN EL ESTADO DE NUEVO LEÓN

La Fiscalía General de Justicia del Estado de Nuevo León, con el firme propósito de cumplir con las disposiciones normativas contenidas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y las demás normas generales aplicables en materia de protección de datos personales, ha tenido a bien elaborar políticas internas para garantizar a las y los titulares el tratamiento adecuado de sus datos de dicha naturaleza.

Lo anterior de conformidad con el artículo 35, fracción II de la Ley de la referida Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, para que todo el personal adscrito a la Institución actúe en todo momento conforme a las disposiciones jurídicas aplicables, en términos del presente instrumento.

I. Objetivo

Establecer la mecánica interna para el acopio, uso, resguardo y protección de los datos personales en posesión de las y los servidores públicos de la Fiscalía General de Justicia, en el ejercicio de sus funciones para cumplir de manera cabal con lo establecido en la materia por las normas generales aplicables, así como los tratados internacionales en la materia.

II. Alcance

Las presentes políticas internas de protección de datos de datos personales van dirigidas y deberán ser observadas por todo el personal de la Fiscalía General de Justicia del Estado. En los casos de datos obtenidos en ocasión del desarrollo de una investigación, las y los responsables deberán darle el tratamiento armónico conforme a los diversos ordenamientos procesales del sistema de justicia penal las garantías y en armonía con los imperativos que se desprenden de las garantías del debido proceso.

III. Glosario

1. **Fiscalía:** Fiscalía General de Justicia en el Estado de Nuevo León.
2. **Dirección General:** La Dirección General Jurídica y de Transparencia.
3. **Unidad:** Cualquier área administrativa de la Fiscalía, que trata o tiene acceso a los datos personales, de forma física o mediante cualquier otro sistema.
4. **Encargado**: La o el servidor público que trata datos personales, o cualquier otra persona física o moral ajena a la Fiscalía que, de manera individual o juntamente con otros, trata datos personales por cuenta de la Fiscalía.
5. **Responsable:** La o el servidor público titular del área que decide el tratamiento de los datos personales.
6. **Titular:** Persona física a quien pertenecen los datos personales que son objeto de tratamiento, o persona moral que proporcione datos que se equiparen de manera análoga.
7. **Políticas**: Políticas y Programas de Protección de Datos Personales.
8. **Remisión:** Comunicación de datos personales entre un responsable y un encargado del tratamiento de forma interna.
9. **Transferencia:** Comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta de la o del titular, por parte del responsable o del encargado.
10. **Aviso de privacidad:** Documento a disposición de la o del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos**.**
11. **Bases de datos:** Conjunto ordenado que contiene entre otras cosas, datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
12. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

13. **Datos personales sensibles:** Son aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, datos genéticos o datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual**.**
14. **Ley de Protección:** Ley de Protección de Datos Personales del Estado de Nuevo León.
15. **Subresponsable.** Las y los servidores públicos adscritos a la Fiscalía, que ejecutan las decisiones del Responsable sobre el tratamiento físico o automatizado de los datos personales.
16. **Disociación.** Procedimiento mediante el cual los datos personales no pueden asociarse a la o al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de este.
17. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
18. **Consentimiento:** manifestación de la voluntad libre, específica e informada de la o del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

IV. Identificación

Las y los servidores públicos de la Fiscalía, al recibir o usar, por cualquier medio, información relativa a una persona, deberán identificar si la misma constituye un dato personal, de acuerdo con la información contenida en el Glosario del actual instrumento.

V. Clasificación de datos personales y su nivel de seguridad

Una vez que la o el servidor público de la Fiscalía ha identificado que tiene en su poder información que constituye un dato personal, debe hacer la clasificación correspondiente de éste, para proceder, de inmediato, a ubicarlo en el nivel de seguridad que le corresponda y, así, adoptar las medidas de protección pertinentes hacia el interior de su unidad, atendiendo a la información que a continuación se inserta:

1. NIVEL DE SEGURIDAD BÁSICO: Obligatorio para todos los soportes documentales, físicos, como electrónicos, a fin de proteger la información de naturaleza privada, concerniente únicamente a las y los Titulares.

Dentro de este nivel de seguridad se encuentra la siguiente clasificación de datos personales:

1.1 **Datos de identificación**. Información concerniente a una persona física que permite diferenciarla de otras, en una colectividad. En esta categoría pueden ubicarse: nombre, estado civil, firma autógrafa y electrónica, Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), número de cartilla militar, lugar y fecha de nacimiento, nacionalidad, fotografía, edad, entre otros.

1.2 **Datos de contacto**. Información que permite mantener o entrar en contacto con su titular. En esta categoría, pueden clasificarse: domicilio, correo electrónico, teléfono fijo, teléfono celular, entre otros.

1.3 **Datos laborales**. Información concerniente a una persona física, relativa a su empleo, cargo o comisión; desempeño laboral y experiencia profesional, generada a partir de procesos de reclutamiento, selección, contratación, nombramiento, evaluación y capacitación. Dentro de esta categoría, podemos identificar, entre otros: puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, fecha de ingreso y salida del empleo.

2. NIVEL DE SEGURIDAD MEDIO: Obligatorias para los soportes documentales, físicos, como electrónicos, relativos a los procesos jurisdiccionales o administrativos seguidos en forma de juicio, información financiera, datos patrimoniales, así como aquellos que se permita obtener evaluación de personalidad o perfiles de cualquier tipo, en el presente, pasado o futuro, que haga reconocible a las y los Titulares.

Dentro de este nivel de seguridad se encuentra la siguiente clasificación de datos personales:

2.1. **Datos académicos**. Información concerniente a una persona física que describe su preparación, aptitudes, desarrollo y orientación profesional o técnica, avalada por instituciones educativas; como lo son: trayectoria educativa, títulos, cédula profesional, certificados, reconocimientos, entre otros.

2.2. **Datos patrimoniales o financieros**. Información concerniente a una persona física, relativa a sus bienes, derechos, cargas u obligaciones susceptibles de valoración económica; como pueden ser: bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, número de tarjeta de crédito, número de seguridad, entre otros.

2.3. **Datos jurisdiccionales o administrativos**. Información relativa sobre personas que sostienen un proceso seguido en forma de juicio ante cualquier Tribunal Jurisdiccional u órgano administrativo.

3. NIVEL DE SEGURIDAD ALTO (DATOS SENSIBLES): Aplicables a los soportes documentales relativos a los datos personales clasificados como sensibles,

así como a los que contengan datos recabados para fines de seguridad, prevención, investigación y persecución de delitos que permitan identificar a las y los Titulares.

Dentro de este nivel de seguridad se encuentra la siguiente clasificación de datos personales:

3.1. **Datos biométricos**. Información sobre una persona física, relativa a imagen del iris, huella dactilar, palma de la mano u otros análogos.

3.2. **Datos sobre características físicas**. Información sobre una persona física relativa a su fisonomía, anatomía, rasgos o particularidades específicas; tales como: color de la piel, del iris o del cabello, señas particulares, estatura, peso, complexión, cicatrices, tipo de sangre, entre otras.

3.3. **Datos ideológicos**. Información sobre las posturas ideológicas, religiosas, filosóficas o morales de una persona.

3.4. **Datos sobre opiniones políticas**. Opinión de una persona en relación con un hecho político o sobre su postura política en general.

3.5. **Datos sobre afiliación sindical.** Pertenencia de una persona a un sindicato y la información que de ello derive.

3.6. **Datos de salud.** Información concerniente a una persona física, relacionada con la valoración, preservación, cuidado, mejoramiento y recuperación de su estado de salud físico o mental, presente, pasado o futuro, así como su información genética.

3.7. **Datos sobre vida sexual.** Información de una persona física, relacionada con su comportamiento, preferencias, prácticas o hábitos sexuales, entre otros.

3.8. **Datos de origen étnico o racial**. Información concerniente a una persona física, relativa a su pertenencia a un pueblo, etnia o región que la distingue por

sus condiciones e identidades sociales, culturales y económicas, así como por sus costumbres, tradiciones y creencias.

VI. Principios que regulan el tratamiento de los Datos Personales

Las y los servidores públicos de la Fiscalía que efectúen manejo de datos personales deberán, en todo momento, observar los principios de calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, trasparencia, y temporalidad.

VII. Responsabilidades y deberes

La o el responsable deberá adoptar los mecanismos de seguridad idóneos y necesarios al interior de la unidad a su cargo, sobre el tipo de datos personales que se hallen en los soportes documentales que maneje (físicos o electrónicos).

Soporte documental físico: Documento donde conste gráficamente plasmado el dato personal de los titulares; es resguardado físicamente en la unidad a cargo del responsable.

Soporte documental electrónico: Sistema de base de datos electrónica en donde se almacenan los datos personales del titular.

Las y los subresponsables deberán tratar los datos personales conforme a lo establecido en las presentes políticas internas y conforme a los lineamientos e indicaciones que para tal efecto le traze el responsable, cuidando siempre el cumplimiento de la legislación aplicable en la materia.

La o el responsable deberá mantener un régimen o sistema de vigilancia interno, que permita supervisar que las y los subresponsables y encargados, en su caso, cumplan con las

presentes políticas y con los lineamientos instruidos para el tratamiento que estime adecuado de los datos en posesión de su unidad, para evitar la transferencia ilegal, vulneración o pérdida de éstos.

El tratamiento de datos personales por parte de la o del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera, con las excepciones legales que correspondan.

Bajo esas condiciones, su actuar estará circunscrito a la luz de los siguientes compromisos:

a) Asegurar que los datos personales en su poder sean ciertos, adecuados, pertinentes y proporcionales; no excesivos, en relación con el ámbito y la finalidad para la que fueron recabados.

b) Garantizar la secrecía y la no difusión de los datos personales en su poder. Por lo que, exclusivamente, podrán permitir a la persona titular el acceder a los mismos, o en su caso, a la o al responsable, a fin de cumplir con las finalidades del tratamiento.

c) Recabar el consentimiento de las y los titulares al momento de recabar los datos personales, poniendo de su conocimiento el aviso de privacidad que corresponda.

d) Verificar que los datos personales recabados y tratados tengan fines determinados, explícitos y legítimos, sin que los mismos puedan ser tratados posteriormente con fines distintos para los que fueron obtenidos.

e) Informar a la o al titular de los datos, sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado relacionados con éstos.

f) Verificar que el tratamiento de datos personales se realice sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza de la o del titular.

g) Asegurar que los datos personales recabados u obtenidos no sean utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

h) Tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con la finalidad o finalidades, para lo cual se obtuvieron.

i) Verificar que la información relacionada con el tratamiento de datos sea accesible y fácil de entender, y siempre a disposición de la o del titular.

j) Asegurar que se cumpla el ciclo de vida o la temporalidad vinculada a la finalidad para la cual fueron recabados y tratados los datos personales.

k) Destruir, cancelar o suprimir los datos personales, una vez concluida su finalidad o porque éstos hayan dejado de ser necesarios, pertinentes o lícitos.

l) Establecer y mantener todas las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

IX. Transferencias y remisiones de datos personales

La Fiscalía, por medio de las y los responsables, realizará solamente las transferencias y remisiones de datos personales necesarias y adecuadas para el cumplimiento de sus atribuciones legales, conforme a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León y demás marco normativo aplicable en la materia.

Para realizar transferencias de datos personales, que no se lleven a cabo de acuerdo a las funciones legalmente establecidas para la Institución, resulta indispensable que se documente en instrumentos jurídicos, con cláusulas contractuales especiales para tal efecto, o mediante la celebración de convenios de colaboración, entre otros, que permitan demostrar el alcance del tratamiento de los datos personales, así como las obligaciones correlativas asumidas por los contratantes.

En cualquiera de los casos mencionados, la transferencia de datos debe observar lo informado en el aviso de privacidad que corresponda y, en su caso, cumplir con lo establecido en el contrato que se hubiere firmado al respecto.

La transferencia de datos sensibles debe contar con el consentimiento expreso de la o del titular.

No se requiere el consentimiento de la o del titular, ni la celebración de instrumentos jurídicos, para la transferencia de datos personales, en los siguientes supuestos que establece la ley:

I. Cuando la transferencia esté prevista en la referida Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por el México;

II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y la o el titular;

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés de la o del titular, por el responsable y un tercero;

VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento de la o del titular para el tratamiento y comunicación de datos personales, conforme a lo dispuesto en el artículo 23 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León; o,

IX. Cuando la transferencia sea necesaria por razones de seguridad.

X. Capacitación

La Fiscalía, a través de la Dirección General, en coordinación con el Instituto de Formación Profesional, llevará a cabo cursos, pláticas y capacitaciones dentro del programa anual, para que el personal de la Fiscalía tenga las herramientas y conocimientos técnicos necesarios para cumplir con el tratamiento adecuado en el manejo de datos personales.

XI. Supervisión y auditoria de las políticas y uso de datos personales

El Órgano Interno de Control, conforme a las competencias que le son propias, vigilará y supervisará el tratamiento de datos personales que llevan a cabo las y los responsables en sus unidades, pudiendo realizar auditorías internas para verificar el cumplimiento de las políticas internas y la legislación aplicable.

Si la Dirección General detectara el acopio o tratamiento inadecuado de datos personales, dará vista a la Visitaduría General y a las instancias que resulten competentes, para que se proceda a efectuar la investigación correspondiente y, en su caso, se apliquen las sanciones a que haya lugar.

XII. Avisos de privacidad

La totalidad de las unidades que conforman la Fiscalía, que traten datos personales, deberán contar con el aviso de privacidad que atienda los extremos de sus funciones.

Los avisos de dicha naturaleza deben ser difundidos a través de la página oficial de la Institución, por lo que deberán ser cargados en el siguiente enlace electrónico: https://fiscalianl.gob.mx/privacidad/. También deberán estar disponibles en forma física para que las y los usuarios de la Fiscalía que acuden a solicitar los servicios brindados estén informados del tratamiento que se le brindará a sus datos personales.