POLÍTICAS GENERALES DE PROTECCIÓN DE DATOS PERSONALES

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE BAJA CALIFORNIA

Contenido

Glosario

I. **Áreas o Unidades Administrativas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables o encargadas de los datos personales;

II. **Aviso de privacidad:** Documento a disposición 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 los mismos;

III. **Bases de datos:** Conjunto ordenado de 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;

IV. **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

V. **Comité de Transparencia:** Instancia a que hace referencia el artículo 53 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California;

VI. **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

VII. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

VIII. **Datos personales sensibles:** Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

IX. **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición, al tratamiento de datos personales;

X. **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XI. **Encargado:** Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trate datos personales a nombre y por

cuenta del responsable;

XII. **ITAIPBC:** Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California;

XIII. **LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

XIV. **Lineamientos:** Lineamientos de protección de datos personales en posesión de sujetos obligados del Estado de Baja California

XV. **LPDPPSOBC:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California;

XVI. **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales;

XVII. **Responsable(s):** Los sujetos obligados a que se refiere el artículo 2 de la LPDPPSOBC, que deciden sobre el tratamiento de datos personales;

XVIII. **Titular:** La persona física a quien corresponden los datos personales;

XIX. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales;

XX. **Unidad de Transparencia:** Instancia a la que hace referencia el artículo 55 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California.

Fundamento jurídico

El Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California (en adelante ITAIPBC), elabora el presente documento en observancia a lo que dispone la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 33 fracción I:

> *"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
>
> *I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión."*
>
> *…*

Asimismo, su homóloga Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, establece, en el artículo 15 fracción II que:

> "El responsable debe observar los siguientes mecanismos para cumplir con el principio de responsabilidad:
> *…*
>
> *II. Instrumentar políticas y programas de protección de datos personales, obligatorias y exigibles al interior de la organización del responsable;"*
>
> *…*

Por lo anterior, se emiten las presentes Políticas Generales de Protección de Datos Personales del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California, sin perjuicio de que, en su oportunidad, cada unidad administrativa emita políticas internas para la gestión y tratamiento de los datos personales que recaban en cumplimiento de sus funciones institucionales.

Objetivo

El objetivo de las políticas generales de protección de datos personales es establecer la estructura normativa y operativa en la materia, así como los principios y deberes que deben observar los servidores públicos del ITAIPBC, para estar en aptitud de proteger los datos personales que se encuentren en su posesión y/o deban tratar, con motivo de sus funciones institucionales.

Ámbito de aplicación:

Las políticas de protección de datos personales son de aplicación general y obligatoria para:

I. Todas las unidades administrativas que conforman la organización del Instituto:

- Pleno;
- Unidad de Transparencia;
- Coordinador de Protección de Datos Personales;
- Órgano Interno de Control;
- Secretaría Ejecutiva;
- Coordinación de Administración Procedimientos;
- Coordinación de Asuntos Jurídicos;
- Coordinación de Verificación Seguimiento;

II. Todos los servidores públicos que laboran en el ITAIPBC y que, en el ejercicio de sus funciones obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, accedan, manejen, aprovechen, divulguen, transfieran o dispongan datos personales.

III. Los encargados que, en su caso, traten datos personales a nombre y por cuenta de este Instituto.

En todo tratamiento de datos personales se deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, además de velar por la seguridad y la confidencialidad de los datos, desde el momento de su obtención y hasta su disposición final.

Políticas de protección de datos personales

Del Comité de Transparencia

El Comité de Transparencia de ITAIPBC es la máxima autoridad de materia de protección de datos personales y, le corresponden, entre otras funciones, las siguientes:

-Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales de conformidad con las disposiciones previstas en la LGPDPPSO y la LPDPPSOBC;
-Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;
-Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la LGPDPPSO y la LPDPPSOBC.

De la Unidad de Transparencia

La Unidad de Transparencia lleva a cabo, entre otras, las siguientes funciones:

-Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho de protección de sus datos personales;
-Gestionar las solicitudes para el ejercicio de los derechos ARCO;
-Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.

Del oficial de protección de datos personales

El ITAIPBC cuenta con un oficial de protección de datos personales, con conocimientos en protección de datos personales, cuya principal función es:
-Asistir, asesorar y orientar al Comité de Transparencia, a la Unidad de Transparencia y a las demás áreas del Instituto, sobre el cumplimiento de los deberes y obligaciones en materia de protección de datos personales.

Del principio de licitud

Los datos personales se tratan únicamente para finalidades que derivan de una norma jurídica que otorga facultades para ello; el tratamiento de datos personales es legalmente permitido por la normatividad aplicable y, en su caso, por el derecho internacional.

Durante el tratamiento de datos personales, se respetan y salvaguardan los derechos y libertades de los titulares.

Del principio de finalidad

El tratamiento de los datos personales se limita al cumplimiento de finalidades concretas, lícitas, explícitas y legítimas; no se tratan datos personales para finalidades distintas a las que le fueron informadas al titular en el aviso de privacidad; en caso de que los datos personales sean necesarios para llevar a cabo finalidades distintas a las informadas inicialmente, se solicita el consentimiento del titular en un nuevo aviso de privacidad.

Del principio de lealtad

No se utilizan medios engañosos o fraudulentos para obtener, recabar o tratar datos personales.

En los tratamientos de datos personales que se llevan a cabo, no existe dolo, mala fe, violencia o negligencia que afecten los intereses de las personas y, en todo momento se respeta y favorece su expectativa razonable de privacidad.

Del principio de consentimiento

En todos los casos, los datos personales se recaban con el consentimiento de su titular; dicho consentimiento se obtiene de forma libre, específica e informada.

El consentimiento tácito se obtiene después de haber puesto a disposición del titular, el aviso de privacidad, y éste no manifiesta oposición u objeción alguna; asimismo, el consentimiento es tácito, cuando el tratamiento de datos actualiza alguno de los supuestos establecidos en el artículo 11 de la LPDPPSOBC:

I. Cuando una ley así lo disponga, siempre que no contravenga las disposiciones de la Ley General de protección de datos.
II. Cuando las transferencias de datos personales entre responsables, sean sobre facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento;
III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;
VIII. Cuando los datos personales figuren en fuentes de acceso público;
IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o
X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

El consentimiento debe ser expreso, cuando las finalidades para las cuales pretendemos utilizar los datos personales, son distintas a los supuestos del artículo 11 de la LPDPPSOBC.

Cuando el tratamiento implique datos personales sensibles, se debe obtener el consentimiento

expreso y por escrito del titular, a través de su firma autógrafa o electrónica.

El consentimiento de menores de edad o de personas en estado de interdicción o incapacidad, se obtiene a través del padre o de la madre; de la persona que posea la patria potestad; o de un tutor, debidamente acreditados, según sea el caso.

Del principio de calidad

Durante la obtención de los datos personales, se debe revisar que, los mismos, no presenten errores que puedan afectar su veracidad, que sean íntegros en relación a las finalidades para la cuales se recaban y que correspondan con la situación actual del titular.

Una vez cumplidas las finalidades para las cuales fueron recabados los datos personales, se conservan en una etapa de bloqueo hasta el vencimiento del plazo legal de conservación.

El bloqueo también es aplicable cuando se deban determinar posibles responsabilidades respecto de un tratamiento de datos en concreto.

Una vez que prescribe el plazo legal de conservación de los datos, éstos se eliminan y/o suprimen de las bases de datos, atendiendo a estándares de calidad, irreversibles y favorables al medio ambiente.

Del principio de proporcionalidad

Únicamente se recaban datos personales que son necesarios, adecuados, relevantes y no excesivos para el cumplimiento de las finalidades que justifican su obtención.

Cuando se recaban datos personales adicionales (por ejemplo, para generar estadísticas), se le informa dicha situación al titular a través del aviso de privacidad.

Del principio de información

En todos los casos, previo al tratamiento de los datos personales, se pone a disposición del titular el aviso de privacidad simplificado en el que se le hacen saber las características esenciales del tratamiento al que serán sometidos sus datos personales.

El aviso de privacidad integral se encuentra publicado de manera permanente en el portal institucional, en el apartado de “avisos de privacidad”.

Los avisos de privacidad se redactan en un lenguaje sencillo, claro y comprensible, e incluyen todos los elementos que establece la Ley.

Se pone a disposición de los titulares, un nuevo aviso de privacidad, en caso de que se requiera tratar sus datos personales para finalidades distintas o no compatibles con las que se le informaron inicialmente.

Del principio de responsabilidad

Se implementan mecanismos acordes con los recursos y el presupuesto, para cumplir con los principios y deberes establecidos en las leyes de protección de datos personales.

Se destinan recursos humanos y materiales para la implementación de políticas y programas en materia de protección de datos personales.

Se cuenta con un programa de capacitación en materia de protección de datos personales dirigido al personal.

Se deben revisar periódicamente las políticas y programas de seguridad, a fin de determinar y realizar modificaciones y actualizaciones.

Las propias políticas de protección y de gestión de datos personales deben ser revisadas y actualizadas periódicamente de acuerdo con los avances en la materia.

Se cuenta con procedimientos para atender dudas y quejas de los titulares respecto a solicitudes para el ejercicio de derechos ARCO.

Del deber de confidencialidad

Las personas y servidores públicos que traten datos personales, así como, en su caso, los encargados, deben guardar absoluta discreción sobre la información y los datos personales que generen, posean o deban conocer por razón de su encargo; la obligación de confidencialidad debe subsistir aun después de finalizada la relación entre el servidor público o el encargado, con el responsable.

Del deber de seguridad

Las medidas de seguridad implementas están orientadas a garantizar la confidencialidad, integridad y disponibilidad de los datos personales y la información que obra en los registros y bases de datos.

Medidas de seguridad administrativas:

-Declaración de confidencialidad de los servidores públicos y encargados que tratan datos personales;
-Políticas de gestión de datos personales;
-Identificación de roles y perfiles de los servidores públicos y encargados que intervienen en los tratamientos de datos personales;
-Manuales de los procedimientos y/o procesos específicos donde se tratan datos personales, por ejemplo: gestión de solicitudes ARCO, Recursos de revisión, etc.
-Procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional;
-Programa de sensibilización, formación y capacitación en la materia a todo su personal;
-Prever sanciones por la revelación, uso, acceso, divulgación o cualquier tratamiento no autorizado de datos personales;

-Esquema de derechos y contraseñas de acceso a las bases de datos y áreas críticas donde se encuentran la información;
-Inventario de tratamientos de datos personales;
-Avisos de privacidad;
-Bitácora para registrar y reportar las vulneraciones ocurridas a las bases y datos personales, debe incluir: fecha y lugar en donde se produjo, nombre y cargo del servidor público que notifica la incidencia, nombre y cargo del servidor público encargado de implementar las medidas de seguridad para mitigar la vulneración y, descripción de las acciones llevadas a cabo y las medidas de seguridad implementadas;
-Mecanismos para la identificación, clasificación y borrado seguro de los datos personales;
-Programa de depuración de archivo (de las bases de datos físicas y electrónicas) conforme a los plazos de conservación y parámetros dispuestos la normativa archivística, documentando los periodos de conservación de las bases de datos, del bloqueo (cuando sea necesario) y de supresión de las mismas;
-Bitácora de registro de personal que tiene acceso al archivo físico y a los expedientes, que incluya la finalidad para la cual se consulta tal expediente.
-Documento de seguridad.

Medidas de seguridad físicas:

-Señalamientos de restricción en las áreas críticas donde se resguardan datos personales;
-Restricción de acceso a las áreas críticas solo al personal autorizado;
-Uso de candados en áreas clave.
-Registro de visitas o ingreso de personas ajenas a la organización;
- Política de “escritorio” limpio al ausentarse temporalmente o bien, al finalizar el turno:
    -Dejar el área de trabajo en un estado que no permita a otros usuarios y/o personas no autorizadas, visualizar los datos e información a su cargo;
    -No dejar a la vista documentos que contengan información confidencial;
    -Bloquear el equipo de cómputo con contraseña, o bien, desconectarse y apagar el equipo.
    - Recoger originales de impresoras y fotocopiadoras, revisar la bandeja de entrada y de salida y retirar todos los documentos.
-Supresión de documentos utilizando trituradora, o bien, algún otro mecanismo que no permita su recuperación;
-Cuidar y mantener en buen estado los equipos de cómputo;
-No introducir softwares que no hayan sido validados y autorizados por el personal del área informática.
-Uso de alarmas contra incendios;
-Colocar reguladores de voltaje a los equipos de cómputo;
-Colocar videocámaras.

Medidas de seguridad técnicas:

-Uso de contraseñas personales e intransferibles, que combinen caracteres entre mayúsculas, minúsculas, números y signos, que no sean fáciles o predecibles;
-Realizar copias de seguridad, respaldos;
-Contar con un área especializada en asuntos informáticos para atender fallas y dar mantenimiento a los equipos electrónicos o de cómputo;
-Notificar cualquier falla del equipo de cómputo al área especializada para atenderla;
-Instalar antivirus y dar mantenimiento preventivo a los equipos de cómputo;
-Prohibir del uso de puertos USB por personas ajenas a la organización;
-Crear perfiles de acceso, claves y contraseñas de autenticación del personal que trata datos personales;

-Contratación de cómputo en la nube;
-Uso de un servidor.

De la relación con encargados

En caso de establecerse contratos de colaboración con encargados para la realización de tratamientos de datos personales, éstos deben adherirse al cumplimiento de los principios y deberes en materia de protección de datos personales, a través de la suscripción de cláusulas que lo describan claramente.

La actuación de los encargados respecto de los tratamientos de datos personales se limitará a los términos que fije el responsable. Tales acuerdos no deben contravenir las Leyes, General y Estatal de protección de datos personales.

Del tratamiento de datos personales de menores de edad

En el tratamiento de datos personales de menores de edad, en todo momento se debe privilegiar su interés superior, atendiendo las disposiciones de la "Ley para la protección y defensa de los derechos de niñas, niños y adolescentes del Estado de Baja California" las reglas de representación previstas en la legislación civil y demás ordenamientos aplicables.

Del ejercicio de derechos ARCO

En todo momento el titular de los datos personales o su representante pueden solicitar el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales que se encuentren en posesión del responsable.

El ejercicio de derechos ARCO de menores de edad, de personas en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, y de personas fallecidas, está sujeto a las reglas de representación establecidas en el capítulo V de la LPDPPSOBC y en el título tercero de los Lineamientos de protección de datos personales en posesión de sujetos obligados del Estado de Baja California.

La solicitud de derechos ARCO no debe imponer mayores requisitos a los establecidos en el artículo 31 de la Ley Estatal y 93 de los Lineamientos:

1. Nombre del titular de los datos personales;
2. Nombre del representante legal (en su caso);
3. Domicilio o medio para recibir notificaciones, pudiendo ser su correo electrónico;
4. Descripción clara y precisa de los datos personales objeto de la solicitud, salvo que se trate del derecho de acceso;
5. Descripción del derecho que se quiere ejercer; y
6. Los documentos que acrediten la identidad del titular y, en su caso, la identidad y personalidad de su representante.

Las personas con discapacidad y los hablantes de lengua indígena deben poder ejercer sus derechos ARCO en igualdad de circunstancias.

La Unidad de Transparencia debe entregar un acuse de recibo al solicitante.

El procedimiento para el ejercicio de los derechos ARCO no excede los requisitos, plazos condiciones y términos establecidos en el título tercero de la LGPDPPSO y el Capítulo V de la LPDPPSOBC, así como en el título tercero de los Lineamientos.

Los medios disponibles para presentar una solicitud para el ejercicio de derechos ARCO son los siguientes:

-escrito enviado al correo electrónico: transparencia@itaipbc.org.mx,
-escrito presentado físicamente en la Unidad de Transparencia del Instituto, ubicada en: Avenida Carpinteros y Calle H, número 1598, Colonia Industrial, Mexicali, Baja California cp. 21010, o bien, en las oficinas ubicadas en Calle Rufino Tamayo #9970, Zona Urbana Río Tijuana, en Tijuana Baja California cp. 22320;
-formato electrónico disponible en el portal institucional, en el menú “Datos Personales”, submenú “solicitud para el ejercicio de derechos ARCO”;
-a través de la Plataforma Nacional de Trasparencia:
https://www.plataformadetransparencia.org.mx/web/guest/inicio

Al momento de presentar la solicitud, el titular de los datos personales, así como su representante, en su caso, deberán anexar copia simple de los documentos que acrediten su identidad y personalidad.

Los medios aceptables para acreditar la identidad y personalidad del titular y del representante, en cada caso, son los siguientes:

Titular:

- INE o, cédula profesional (excepto electrónica) o, pasaporte vigente o, cartilla del servicio militar o, licencia de conducir o, credencial expedida por autoridad de seguridad social.

Representante legal:

- INE o Cédula profesional +
- Identificación oficial del titular de los datos +
- Carta poder simple firmada ante dos testigos +
- Copia de identificación de ambos testigos.

Al momento de recibir la solicitud, se entrega el ACUSE en el que consta la fecha de recepción de la misma.

En caso de que la solicitud no cuente con todos los elementos necesarios, en un plazo de 5 días hábiles se requiere la información faltante al solicitante, por medio de una prevención.

Se otorgan 10 días al solicitante para subsanar la prevención; en caso de no hacerlo, la solicitud, se tiene por no presentada conforme a la Ley.

En caso de que el Instituto se declare incompetente para dar trámite a la solicitud, se le notifica al solicitante en un plazo no mayor a 3 días hábiles.

En caso de que el Instituto sea parcialmente competente respecto de la solicitud, se le notifica dicha respuesta al solicitante, en un plazo no mayor a 20 días hábiles.

De advertirse que la solicitud corresponde a un derecho distinto, se le notifica al solicitante en un plazo de 3 días hábiles.

Una vez cumplidos todos los requisitos de la solicitud, dentro de los 20 días hábiles contados a partir del día siguiente al de recibida, se le informa al solicitante si, la misma, es procedente o improcedente.

Una vez que se determina la procedencia de la solicitud y, previo a hacer efectivo el ejercicio del derecho de que se trate, el titular y/o su representante deberán presentar los documentos de identificación originales directamente en las oficinas del responsable.

La reproducción de los datos personales en copias simples o certificadas es gratuita cuando no excede de 20 hojas.

En caso de no recibir respuesta o bien, en caso de inconformidad con la respuesta otorgada, el titular podrá interponer el Recurso de Revisión.

El procedimiento para ejercer los derechos ARCO se encuentra disponible para consulta de los titulares, en el portal de internet del Instituto, en el menú “Datos Personales”, submenú “Procedimiento para el ejercicio de derechos ARCO”.

De la portabilidad de datos personales

En lo referente al derecho de portabilidad, se observará lo dispuesto en los ¨Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales¨.

De las transferencias de datos personales

En caso de que se deban transferir datos personales nacional o internacionalmente, previo a la transferencia se deberá obtener el consentimiento del titular y, en cada caso, se deberá informar al receptor de los datos, el aviso de privacidad, para que éste se limite a tratarlos conforme a las finalidades que ahí se describan.

Las transferencias se formalizarán mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, a excepción de las siguientes:

I. La transferencia sea nacional, y se realice en virtud del cumplimiento de una disposición legal;
II. La transferencia sea internacional y se encuentre prevista en una Ley o tratado suscrito y ratificado por México;
III. La transferencia sea internacional y se realice a petición de un organismo internacional competente cuyas facultades sean homologas y las finalidades sean análogas respecto de aquellas que motivaron el tratamiento de los datos.

En las transferencias nacionales, el receptor asumirá el carácter de responsable de los datos personales.

En las transferencias internacionales, el receptor deberá obligarse a proteger los datos personales conforme a los principios y deberes y demás obligaciones similares o equiparables a las previstas en la legislación nacional y estatal.

No se requerirá consentimiento del titular cuando:

I. La transferencia esté prevista en la LGPDPPSO, la LPDPPSOBC u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;
II. 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. La transferencia sea legalmente exigida para la investigación y persecución de un delito, o la procuración y administración de justicia;
IV. La transferencia sea precisa para el ejercicio, defensa o reconocimiento de un derecho, siempre que la autoridad competente la requiera;
V. La transferencia sea necesaria para un diagnóstico médico o la gestión de servicios sanitarios siempre que se acrediten;
VI. La transferencia sea necesaria para el cumplimiento de una obligación jurídica entre el sujeto obligado y el titular;
VII. La transferencia sea necesaria por virtud de un contrato celebrado entre el sujeto obligado y un tercero, en beneficio del titular
VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente Ley, o,
IX. Cuando sea necesaria por razones de seguridad nacional.

De las vulneraciones de seguridad

En caso de ocurrir una pérdida, destrucción, robo, extravío, copia, uso, acceso o tratamiento no autorizados, o bien, un daño, alteración o modificación no autorizada de datos personales, que afecten de manera significativa los derechos patrimoniales o morales de los titulares, se debe dar aviso a estos últimos en cuanto se confirme la existencia de la vulneración, a fin de que tomen acciones al respecto.

El aviso debe contener, cuando menos, lo siguiente:
-La naturaleza del incidente;
-Los datos personales comprometidos;
-Las recomendaciones al titular para que adopte medidas para proteger sus intereses;
-Las acciones correctivas realizadas de forma inmediata;
-Los medios donde puede obtener más información al respecto.

En caso de ocurrir una vulneración, se debe elaborar una bitácora registrando la fecha en la que ocurrió, el motivo, y las acciones correctivas implementadas de forma inmediata y definitiva.

De las sanciones

Serán causas de sanción por incumplimiento de las obligaciones establecidas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad;

VIII. No establecer las medidas de seguridad en los términos de Ley;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley General;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos en contravención a lo que dispone el artículo 5 de la Ley General;
XIII. No acatar las resoluciones emitidas por el Instituto, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.