ACUERDO POR EL QUE SE APRUEBA EL PROCEDIMIENTO INTERNO PARA LA MEJOR OBSERVANCIA DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS EN EL INMEGEN

CONSIDERANDO

Que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 85 fracción III prevé como parte de las funciones de la Unidad de Transparencia el establecimiento de mecanismos para asegurar que los datos personales sean entregados únicamente al titular o bien, a su representante legal debidamente acreditado, con el objeto de cumplir con los principios prescritos en la Ley como son el de responsabilidad y lealtad así como los deberes de seguridad y confidencialidad; asimismo, constriñe a los sujetos obligados para que el trámite, expedición y modificación de su normatividad interna acorde con dicha disposición jurídica.

Que el Instituto Nacional de Medicina Genómica, como garante del derecho a la protección de datos personales y al acceso, rectificación, cancelación y oposición de éstos, y en cumplimiento a lo previsto en el orden jurídico nacional, es que emite el siguiente:

PROCEDIMIENTO INTERNO PARA LA MEJOR OBSERVANCIA DE LA LGPDPPSO EN EL INMEGEN

DISPOSICIONES GENERALES

1. El presente procedimiento interno es de observancia obligatoria para todas las unidades administrativas que integran el Instituto Nacional de Medicina Genómica, el cual tiene por objeto garantizar el derecho fundamental de las personas a la protección de sus datos personales contenidos en los archivos, registros y en las bases de datos en posesión del Instituto.

DEFINICIONES

2. Además de las definiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para efectos del presente procedimiento se entenderá por:

I. Unidades Administrativas: Aquellas áreas que integran el Instituto y llevan a cabo el tratamiento de datos personales incluyendo la Junta de Gobierno, Comités y/o Cuerpos Colegiados.

II. 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.

III. Datos personales sensibles: 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. 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, creencias religiosas, filosóficas y morales, así como opiniones políticas y preferencia sexual.

IV. Derechos ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición en el tratamiento de datos personales.

V. DDT: Dirección de Desarrollo Tecnológico.

VI. Encargado: La persona física o jurídica distinta a las unidades administrativas, que realizan el tratamiento de los datos personales a nombre del Instituto.

VII. INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

VIII. Instituto: Instituto Nacional de Medicina Genómica.

IX. Ley: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

X. Responsable: La persona que dentro de las unidades administrativas llevan a cabo el tratamiento de datos personales.

XI. Titular: Persona física a quien corresponden los datos personales.

XII. Usuario: Persona física que tiene una sesión en un equipo de cómputo.

3. No podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o, en su defecto, se refiera a los casos establecidos en la Ley.

En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior del menor. Para los casos en que se pueda advertir el tratamiento de datos personales de probables víctimas y testigos, se deberá garantizar la mayor protección de los datos personales, en términos de la normativa aplicable.

4. Todo tratamiento de datos personales deberá llevarse a cabo con plena observancia a los principios y deberes establecidos en Ley y demás disposiciones normativas emitidas por el INAI.

Las limitaciones al derecho a la protección de datos personales se sujetarán a las previstas en los ordenamientos jurídicos aplicables que regulan el derecho de acceso a la información pública y protección de datos personales.

DE LOS PRINCIPIOS

5. Las Unidades Administrativas deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

6. El principio de licitud establece la obligación a cargo del Instituto de recabar y tratar los datos personales en apego y cumplimiento a la legislación mexicana y el derecho internacional, atendiendo las facultades que le son conferidas por mandato legal.

7. El principio de finalidad se refiere a que todo tratamiento de datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

Las finalidades deberán ser determinadas, es decir, deberán especificar el objeto para el cual se tratarán los datos personales; además deberán de ser claras a efecto de que no generen confusión y con objetividad.

Existen dos tipos de finalidades: Las que dan origen y son necesarias serán primarias, en tanto que aquellas que no cumplan con dicha condición, serán secundarias.

8. El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses de los titulares y la expectativa razonable de privacidad, entendiendo ésta última como la confianza que deposita una persona en otra, respecto de que los datos personales proporcionados, serán tratados conforme lo acordado y lo establecido en la Ley.

9. La obtención del consentimiento debe ser libre, sin que medie error, mala fe, violencia o dolo, específica, referida a finalidades determinadas que justifiquen el tratamiento; e informada, es decir, que el titular tenga conocimiento del aviso de privacidad previo al tratamiento.

En caso de que se pretenda tratar los datos personales para finalidades distintas de las que se dieron a conocer en el aviso de privacidad al titular y para las cuales se obtuvo el consentimiento, será recabar nuevamente el consentimiento para ello.

10. El consentimiento del titular podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

El consentimiento será tácito al estar a disposición del titular el aviso de privacidad y éste no manifieste su voluntad en sentido contrario. Será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Para tales efectos, tratándose de datos personales de carácter patrimonial, es obligatorio recabar el consentimiento expreso de los titulares, en tanto que para el tratamiento de datos personales sensibles, resulta necesario la obtención del consentimiento expreso y por escrito.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

La carga de la prueba para demostrar la obtención del consentimiento otorgado por los titulares para el tratamiento de datos personales, en todos los casos, recae en el Responsable.

11. No se tendrá obligación de recabar el consentimiento del titular para el tratamiento de sus datos personales en los casos siguientes:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley;

II. Cuando las remisiones o trasferencias que se realicen, sean en ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

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 Instituto;

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 y / 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.

12. El principio de calidad consiste en que los Responsables deberán adoptar las medidas necesarias para mantener exactos (que reflejen la realidad de la situación del titular), completos (cuando no falta ningún dato que se requiera para las finalidades para las que se lleva a cabo el tratamiento), pertinentes (que corresponden a su titular), actualizados (se encuentran al día) y correctos (cuando cumplen todas las características anteriores).

Se presume que los datos personales son correctos, cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales dejen de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

13. Las unidades administrativas, deberán establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos.

14. Para dar cumplimiento al principio de proporcionalidad, los Responsables sólo deberán tratar los datos personales que resulten necesarios, adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Las unidades administrativas deberán realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron, las cuales, deberán contemplarse en el Aviso de Privacidad. Respecto de los datos personales sensibles, se deberá limitar el periodo de tratamiento mínimo indispensable.

Queda prohibida la creación de bases de datos que contengan datos personales sensibles sin que se justifique su creación para finalidades legítimas, concretas y acordes con las funciones establecidas en la normativa.

15. Por virtud del principio de información, las unidades administrativas deben informar a los titulares de los datos personales, las características principales del tratamiento al que serán sometidos. Este principio se materializa a través de la puesta a disposición del Aviso de Privacidad.

El Aviso de Privacidad puede establecerse a través de formatos físicos, electrónicos, de manera verbal o a través de cualquier otra tecnología siempre y cuando garantice el deber de informar al Titular dicho documento.

Cuando los datos personales se obtengan personalmente del titular, el Aviso de Privacidad debe ser facilitado en el momento y a través de los formatos por los que se recaban, salvo que se hubiere facilitado el Aviso de Privacidad con anterioridad.

El aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el Instituto. Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla.

16. Cuando resulte imposible dar a conocer al titular el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, la unidad administrativa podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

17. El aviso de privacidad se pondrá a disposición del titular en dos modalidades: simplificado e integral.

El aviso simplificado deberá contener la siguiente información:

I. La denominación del Área Universitaria;
II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
III. Cuando se realicen transferencias de datos personales que requieran consentimiento, el aviso además deberá indicar:
    a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y
    b) Las finalidades de estas transferencias.
IV. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales, y
V. El sitio donde se podrá consultar el aviso de privacidad integral.

18. El aviso de privacidad en su versión integral, además de la información del numeral 17, contendrá:

I. El domicilio del Instituto;
II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;
V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
VI. El domicilio de la Unidad de Transparencia, y

VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

El Responsable no está obligado a dar a conocer el aviso de privacidad en los siguientes casos:

- Cuando obtenga los datos personales de forma indirecta y éstos se encuentren destinados a fines históricos, estadísticos o científicos.
- Cuando recabe información de personas morales,
- Cuando obtenga datos personales de personas físicas en su calidad de comerciantes y profesionistas,
- Cuando obtenga datos con fines de representación de personas físicas que prestan sus servicios a otras personas físicas o morales, relativos al nombre completo, puesto desempeñado, domicilio físico, correo electrónico, teléfono y número de fax.

19. El principio de responsabilidad o rendición de cuentas consiste en la obligación de velar por el cumplimiento de los principios estableciendo los mecanismos necesarios para su aplicación así como velar y responder por el tratamiento de los datos personales que se encuentran bajo su custodia o posesión.

DE LOS DEBERES

20. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe de los mismos, cada unidad administrativa deberá establecer, mantener y revisar las medidas de seguridad y controles de carácter administrativo, físico y técnico para la protección de los datos personales que los protejan contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y garanticen su confidencialidad, integridad y disponibilidad, conforme a las Disposiciones Complementarias que emita el Comité de Transparencia.

Las medidas de seguridad administrativas constituyen el conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información así como la concienciación, formación y capacitación del personal en materia de protección de datos personales.

Las medidas de seguridad físicas refieren el conjunto de acciones y mecanismos ya sea que empleen o no la tecnología, destinados para entre otras cosas, prevenir el acceso no autorizado.

Por medidas de seguridad técnicas, se tomarán al conjunto de actividades o controles con resultado medible, que se valen de la tecnología para asegurar que el acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados en cumplimiento de funciones.

Será responsabilidad de la unidad de desarrollo tecnológico proponer al Comité de Transparencia, el proyecto de disposiciones Complementarias de carácter técnico en materia de seguridad, que resulte viable para la protección de los datos personales que se encuentren en posesión del Instituto a través de sus unidades administrativas.

21. Las medidas de seguridad deberán considerar:

I. El riesgo inherente y sensibilidad de los datos personales tratados;

II. El desarrollo tecnológico y las posibles consecuencias de una vulneración para los titulares;

III. Las transferencias de datos personales que se realicen;

IV. El número de titulares de datos personales;

V. Las vulneraciones a datos personales ocurridas en los sistemas de tratamiento, y

VI. El riesgo por el valor potencial cualitativo o cuantitativo que pudieran tener los datos personales tratados por una tercera persona no autorizada para su posesión.

22. A fin de establecer y mantener la seguridad de los datos personales, el Instituto deberá considerar las siguientes acciones: i) elaborar un inventario de datos personales y de los sistemas de tratamiento, ii) determinar las funciones y obligaciones de las personas que traten datos personales; iii) contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales; iv) establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva; v) realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resulten necesarias para la protección de los datos personales; vi) elaborar un plan de trabajo para la implementación de medidas de seguridad faltantes, derivadas del análisis de brecha; vii) llevar a cabo revisiones o auditorías; viii) capacitar al personal que efectúe el tratamiento y ix) realizar un registro de los medios de almacenamiento de los datos personales.

23. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar contenidas en un sistema de gestión a cargo del responsable de seguridad de datos personales designado en cada unidad administrativa.

24. El Instituto elaborará un documento de seguridad de datos personales que contenga lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

VII. El programa específico de capacitación.

26. Cuando ocurra una vulneración a la seguridad, la unidad administrativa analizará y anotará sus causas en una bitácora e implementará acciones preventivas y correctivas para mejorar las medidas de seguridad y el tratamiento de los datos personales mediante un plan de trabajo para evitar se repita.

27. Además de las vulneraciones de seguridad que señale la normatividad aplicable, se considerarán como tales, al menos, las siguientes:

I. La pérdida o destrucción no autorizada;

II. El robo, extravío o copia no autorizada;

III. El uso, acceso o tratamiento no autorizados, o

IV. El daño, la alteración o modificación no autorizada.

28. En cada acceso a un sistema de datos personales, el responsable de seguridad de la unidad administrativa deberá registrar y guardar como mínimo en una bitácora:

I. Datos completos del responsable, del usuario o del encargado;

II. Modo de autenticación del responsable, del usuario o del encargado;

III. Fecha y hora en que se realizó el acceso, o se intentó el mismo;

IV. Sistema de datos personales accedido;

V. Operaciones o acciones llevadas a cabo dentro del Sistema de datos personales, y

VI. Fecha y hora en que se realizó la salida del Sistema de datos personales.

29. Las medidas de seguridad implementadas para la protección de las bases de datos personales se someterán a una auditoría del área de desarrollo tecnológico, para el monitoreo, revisión y evaluación, interna o externa y anual, para verificar el cumplimiento de la Ley.

El informe de la auditoría identificará las deficiencias de las medidas de seguridad y propondrá las medidas preventivas, correctivas y/o complementarias necesarias.

30. Si se detectan vulneraciones significativas a derechos patrimoniales o morales, la unidad administrativa deberá informar sin dilación alguna al titular de los datos personales y a la Unidad de Transparencia, la cual a su vez notificará al INAI. La persona afectada definirá las medidas para la defensa de sus derechos.

31. La unidad administrativa deberá establecer controles o mecanismos que tengan por objeto que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo. Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

DE LOS DERECHOS ARCO Y DE SU EJERCICIO

32. Para ejercer los derechos ARCO en posesión de las unidades administrativas, el titular de los datos, deberá acreditar su identidad. En caso del representante legal, además deberá acreditar la personalidad con la que actúe.

El ejercicio de los derechos ARCO por persona distinta a su titular y al representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

33. Para el caso de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapaces por Ley, se atenderá conforme a las normas de representación prevista en las disposiciones legales civiles aplicables.

Cuando se trate de datos personales de fallecidos, la persona que acredite su interés jurídico y cumpla con los demás requisitos que establezca la Ley, podrá solicitar al Instituto a través de las unidades administrativas, el ejercicio de los derechos ARCO.

34. El titular tiene los siguientes derechos:

I. Acceder a sus datos personales que obren en posesión del Instituto y conocer la información relacionada con las condiciones y generalidades de su tratamiento;

II. Solicitar la rectificación o corrección de sus datos personales, cuando considere que éstos sean inexactos, incompletos o no se encuentren actualizados;

III. Solicitar la cancelación de sus datos personales en los archivos, registros, expedientes y sistemas del Instituto, a fin de que ya no estén en su posesión y dejen de ser tratados por éstas, siempre y cuando las disposiciones aplicables lo permitan,

IV. Oponerse al tratamiento de sus datos personales o exigir que cese en el mismo

VI. Solicitar la portabilidad de sus datos personales.

35. Los trámites que realicen las unidades administrativas respecto a la solicitud, el acceso, la rectificación, la cancelación, oposición y portabilidad de los datos personales, serán gratuitos. El titular deberá cubrir los gastos de reproducción y envío, de conformidad con las tarifas establecidas.

La entrega de información no tendrá costo cuando la información sea de hasta veinte fojas o bien, el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales.

36. Las solicitudes para el ejercicio de los derechos ARCO deben presentarse mediante la Plataforma Nacional de Transparencia, o directamente ante la Unidad de Transparencia, en escrito libre, formato, vía correo electrónico o cualquier otro medio aprobado por el Instituto.

Al presentarse una solicitud de ejercicio de derechos ARCO ante la Unidad de Transparencia, ésta la registrará y capturará en la Plataforma Nacional de Transparencia, a más tardar al día siguiente de su recepción y enviará el acuse de recibo al solicitante, por el medio que éste haya señalado para recibir notificaciones. En el acuse se indicará la fecha de recepción, el folio que le corresponda y los plazos de respuesta aplicables.

Cuando la solicitud se presente por medios electrónicos a través de la Plataforma Nacional de Transparencia, las notificaciones se realizarán automáticamente por el propio sistema. En el caso de que la solicitud se presente por otros medios, en los que el solicitante omita señalar el domicilio o medio para recibir notificaciones y la información sobre los datos personales; o no haya sido posible practicar la notificación, se notificará por estrados en la oficina de la Unidad de Transparencia.

37. La solicitud para el ejercicio de los derechos ARCO deberá contar al menos con los requisitos señalados en el artículo 52 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En caso de que la solicitud de ejercicio de derechos ARCO no satisfaga alguno de los requisitos y la Unidad de Transparencia no cuente con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las

omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO.

38. El ejercicio de los derechos ARCO no procederá en los casos que señala la Ley.

39. El procedimiento de solicitud para el ejercicio de los derechos ARCO se sujetará a lo previsto en el Procedimiento para ejercer los derechos ARCO emitido por el Instituto.

RESPONSABLE Y ENCARGADO

40. Las unidades administrativas fungen como responsables de los datos personales y podrán encomendar el tratamiento de datos personales a una tercera persona que se denominará encargado. El encargado no decidirá el alcance y contenido de ese tratamiento, limitando su actuación a las instrucciones del Instituto, en términos de los instrumentos consensuales que suscriban con las unidades administrativas.

41. Son obligaciones de los encargados del tratamiento de datos personales, además de las asentadas en los instrumentos consensuales que al efecto se suscriban: i) tratar únicamente los datos personales conforme a las instrucciones, ii) abstenerse de tratar los datos personales para finalidades distintas a las instruidas, iii) implementar las medidas de seguridad conforme a la Ley y las demás disposiciones aplicables, iv) guardar confidencialidad respecto de los datos personales tratados, v) suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica o bien, por instrucciones siempre que no exista una previsión legal que exija la conservación de los mismos y vi) abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación o cuando así lo requiera la autoridad competente.

COMUNICACIÓN DE DATOS PERSONALES

42. La transferencia de los datos personales que lleven a cabo las unidades administrativas se sujetará al consentimiento de su titular, salvo en los supuestos previstos en la Ley y el presente procedimiento.

43. Para la transferencia de datos personales se deberá observar lo siguiente:

I. Tener el consentimiento del titular de los datos personales para ese propósito;

II. Formalizar, mediante la suscripción de instrumentos consensuales con los encargados, el alcance del tratamiento de los datos personales, obligaciones y responsabilidades de las partes, las cuales deberán ser acordes a la Ley y demás disposiciones legales aplicables, y

III. Comunicar el aviso de privacidad al receptor de esos datos, quien deberá atender lo establecido en el mismo.

44. Las remisiones de datos personales entre las unidades administrativas y el encargado no requerirán ser comunicadas al titular ni contar con su consentimiento.

ACCIONES PREVENTIVAS EN LA PROTECCIÓN DE DATOS PERSONALES

45. Las Áreas Universitarias adoptarán y desarrollarán esquemas de mejores prácticas en materia de acciones preventivas conforme a las Normas Complementarias sobre

medidas de seguridad técnicas, administrativas y físicas que expida el Comité de Transparencia.

46. Para el tratamiento de datos personales, las unidades administrativas se limitarán a los supuestos y categorías de datos que resulten necesarios y proporcionales a las funciones establecidas y a la naturaleza y funciones de las propias unidades administrativas. Los datos personales obtenidos deberán ser almacenados en bases de datos creadas para ese propósito y ser objeto de medidas de seguridad de nivel alto para garantizar la integridad, disponibilidad y confidencialidad de la información.

DEL COMITÉ DE TRANSPARENCIA Y UNIDAD DE TRANSPARENCIA

47. El Comité de Transparencia es el órgano técnico especializado en materia de protección de datos personales y máxima autoridad en materia de protección de datos personales en el Instituto, cuyas funciones se encuentran previstas en el artículo 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

La Unidad de Transparencia es el vínculo entre el sujeto obligado y el particular, responsible del acceso a la información pública además de ser la encargada de attender las solicitudes de información pública y derechos ARCO que le formulen, cuyas funciones se encuentran previstas en el artículo 85 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

DE LAS INFRACCIONES Y SANCIONES

48. Los funcionarios, empleados y personas físicas que presten su servicio en el Instituto, serán responsables por el incumplimiento de las obligaciones de protección de datos personales, de conformidad con la Ley y la Normativa aplicable.

Cuando el Comité de conozca que un funcionario o empleado del Instituto incumplió con alguna de las obligaciones establecidas, lo informará al Órgano Interno de Control, para que, de existir una posible responsabilidad administrativa, se inicie el procedimiento que corresponda.

49. Las unidades administrativas facilitarán el acceso a las bases de datos al INAI para los procesos de supervisión, vigilancia y verificación que se inicien de oficio o por denuncia del titular.

ACUERDO

PRIMERO. Se aprueba el Procedimiento Interno para la Mejor Observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en el Inmegen.

SEGUNDO. Se instruye a la Unidad de Transparencia para que, realice las gestiones necesarias a efecto de que el presente Acuerdo se publique en el portal de Internet del Instituto.

TERCERO. El presente Acuerdo entrará en vigor al día siguiente de su publicación en la dirección electrónica del Instituto.

Así lo acordó, por unanimidad, el Comité de Transparencia, en sesión ordinaria celebrada el veintiséis de enero del dos mil veintidós.