MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

Disposición 18/2015

Bs. As., 10/4/2015

VISTO el Expediente N° S04:0005938/2015 del registro de este Ministerio y las competencias atribuidas a esta Dirección Nacional por la Ley N° 25.326 y su Decreto reglamentario N° 1558 del 29 de noviembre de 2001, y

CONSIDERANDO:

Que entre las atribuciones asignadas a esta Dirección Nacional se encuentra la de dictar las normas reglamentarias que se deben observar en el desarrollo de las actividades comprendidas por la Ley N° 25.326.

Que también es facultad de este Organismo, la asistencia y asesoramiento acerca de los alcances de la Ley N° 25.326.

Que es una obligación ineludible de esta Dependencia en su carácter de Autoridad de Aplicación de la citada Ley, velar por el cumplimiento de los principios y obligaciones que la misma impone, como así también por el efectivo goce de los derechos que le otorga a los titulares de los datos personales.

Que una gran parte de los tratamientos de datos personales se llevan a cabo mediante aplicaciones o programas de software, en muchos casos de manera automática o con escasa supervisión de una persona.

Que estos tratamientos de datos personales, automatizados o no, deben ser diseñados y desarrollados de manera tal que se respeten los principios y obligaciones legales, debiendo contemplarse debidamente el resguardo de la privacidad de los titulares de la información personal tratada.

Que como consecuencia de acciones del Gobierno Nacional se ha producido un importante crecimiento en el sector productor de software de la REPÚBLICA ARGENTINA.

Que este crecimiento exponencial ha convertido al País en el primer exportador de software de América Latina.

Que por ello, se estima pertinente aprobar una “GUIA DE BUENAS PRACTICAS EN PRIVACIDAD PARA EL DESARROLLO DE APLICACIONES”, como un documento orientativo que establezca pautas de conducta con relación a la protección de los datos personales y en particular a la aplicación de políticas de privacidad en el campo del desarrollo de aplicaciones.

Que mediante ese documento se apunta a brindar las herramientas necesarias para facilitar que todos los actores involucrados en el desarrollo de aplicaciones contemplen la

protección de datos personales como un aspecto fundamental en el diseño de los programas de software.

Que la aplicación de las recomendaciones aquí aprobadas no sólo redundará en el cumplimiento formal de un régimen legal, sino que se verá reflejado como un valor agregado a la producción de software local y, en última instancia, en una mejor protección de los datos y la privacidad de las personas.

Que ha tomado la intervención que le compete la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de este Ministerio.

Que la presente medida se dicta en uso de las facultades conferidas por los artículos 29, inciso 1, apartados b) de la Ley N° 25.326 y 29, inciso 5, apartados a) y e) del Anexo I del Decreto N° 1558/01.

Por ello,

EL DIRECTOR NACIONAL DE PROTECCION DE DATOS PERSONALES

DISPONE:

ARTÍCULO 1° — Apruébase el documento “GUIA DE BUENAS PRACTICAS EN PRIVACIDAD PARA EL DESARROLLO DE APLICACIONES”, que como ANEXO I forma parte del presente, como un instrumento orientativo en materia de reglas de privacidad y protección de datos personales en el ámbito del desarrollo de aplicaciones.

ARTÍCULO 2° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Dr. JUAN CRUZ GONZALEZ ALLONCA, Director Nacional de Protección de Datos Personales, Ministerio de Justicia y Derechos Humanos.

ANEXO I

GUIA DE BUENAS PRACTICAS EN PRIVACIDAD PARA EL DESARROLLO DE APLICACIONES

1) INTRODUCCION

Las aplicaciones, como programas de software, tienen la capacidad de recabar, usar y transferir información de carácter personal.

Esta información se encuentra protegida por la Ley N° 25.326 (Ley de Protección de Datos Personales - LPDP), que establece ciertos principios y obligaciones que tiene que cumplir cualquier tratamiento de datos.

Esta Ley define al dato personal como cualquier información que pueda referirse a una persona determinada o determinable, así que desde el nombre y apellido hasta una imagen o una grabación de voz, cuando pueda reconocerse a una persona, es un dato protegido.

El principio más importante que establece la Ley es que el dato, sin importar dónde se encuentre almacenado o cómo se esté utilizando, es siempre de propiedad de su titular, el que tiene el derecho a controlar los usos que se le da a su información personal.

Como desarrollador de aplicaciones, tenés la responsabilidad de velar por la privacidad de los datos personales que tus desarrollos utilicen. Debes tener en cuenta cómo tus programas protegerán la privacidad desde el inicio mismo del desarrollo, teniendo una política de uso de los datos clara, transparente, que les permita a los titulares de datos conocer cómo es el tratamiento de datos que tus programas realizan.

La Dirección Nacional de Protección de Datos Personales (DNPDP) es la Autoridad de Aplicación de la LPDP, y desde nuestras funciones de control de cumplimiento de la Ley, apuntamos a instalar una cultura de protección de los datos personales.

Mediante esta Guía intentamos brindarte las herramientas necesarias para que se te facilite contemplar la protección de datos personales en tus desarrollos de software, para que puedas, al mismo tiempo, cumplir con la Ley y generar en tus clientes, usuarios y en los titulares de los datos, confianza en que tus productos respetan la privacidad.

2) PRINCIPIOS DE PRIVACIDAD

a. Consentimiento del titular de los datos

El consentimiento del titular para el uso de su información personal es la única manera en la que el tratamiento de datos sea lícito, salvo que se trate de alguna excepción prevista por la Ley. El consentimiento implica una decisión informada por parte del titular permitiendo el uso de sus datos.

Recaba el consentimiento de los titulares, y al mismo tiempo infórmales que estarás recabando su información y los usos que le darás.

b. Finalidad

Los datos que tus aplicaciones recolecten sólo pueden ser utilizados conforme a la finalidad que originó la recolección. Si la aplicación que desarrollas está destinada a la gestión contable de un comercio, la información personal que se recabe puede utilizarse para llevar la contabilidad, liquidar impuestos, llevar inventarios y todas las finalidades compatibles a una gestión contable, pero no podría utilizarse para llevar adelante una campaña publicitaria, porque se estaría cambiando la finalidad del tratamiento.

c. Calidad de los datos

Los datos personales que tus aplicaciones recaben y almacenen deben ser ciertos, adecuados, pertinentes y no excesivos en relación a la finalidad que motivaron su recolección.

No pueden ser obtenidos por medios desleales o fraudulentos y deben ser destruidos cuando hayan dejado de ser útiles.

Además tenés la obligación de almacenarlos de manera tal que se facilite el ejercicio de los derechos de sus titulares.

d. Seguridad

La seguridad de la información es un aspecto importante de la protección de datos. Evalúa los riesgos de seguridad que tu aplicación puede aparejar, teniendo en cuenta la sensibilidad de la información personal que recolecta y almacena.

Verifica que tu aplicación, si utiliza datos personales, respete las mejores prácticas en seguridad de la información.

e. Confidencialidad

Los datos personales de los que tomes conocimiento por el tratamiento que realices son confidenciales. Está prohibido revelarlos.

Esta obligación alcanza a cualquier persona que intervenga en cualquier etapa del desarrollo e inclusive subsiste aun finalizada la relación contractual.

3) PRIVACIDAD APLICADA AL DESARROLLO

a. Los OCHO (8) pasos básicos para desarrollar resguardando la privacidad

i. Contempla la privacidad en todos los procesos de tu organización.

ii. Desarrolla las aplicaciones con el concepto de “Privacidad desde el Diseño”.

iii. Establece una Política de Privacidad clara y fácilmente accesible por los titulares del dato.

iv. Configura por defecto como “activadas” las opciones de privacidad.

v. Permite a los titulares del dato que elijan y controlen.

vi. Limita la cantidad de datos que recolectas o retienes.

No recolectes o almacenes información personal que tu sistema, aplicación o dispositivo no necesite.

Controla no recolectar o almacenar datos sensibles salvo que estés autorizado a hacerlo.

Establece una política para la eliminación de datos personales que ya no te sean útiles.

vii. Asegura los datos personales recabados.

viii. Asume la responsabilidad. Designa a un "responsable de privacidad" o asume vos mismo la responsabilidad del resguardo de los datos personales que hayas tratado.

b. Privacy by design

"Privacidad desde el diseño" es un enfoque en el que desde el origen mismo del diseño de un sistema, aplicación o dispositivo se contempla la protección de la privacidad.

Desde esta perspectiva, la preocupación por la protección de los datos personales no debe ser analizada posteriormente a la finalización del desarrollo, como si se tratara de un anexo, sino que debe estar presente en todas las etapas del proceso.

La privacidad debe ser considerada en todas las fases del ciclo de vida del sistema, aplicación o dispositivo.

c. Privacy by default

Es un concepto de desarrollo de software que establece que la configuración de la privacidad debe estar activada de manera predeterminada, de manera tal que implique un acto de voluntad del titular desactivar o compartir información personal.

Generalmente los titulares del dato, cuando hacen uso de aplicaciones, no saben cómo configurar la privacidad o no se toman el tiempo para hacerlo, por ello es importante que la aplicación no comparta información personal a menos que el mismo titular configure las opciones de privacidad permitiéndolo.

d. Privacy-Enhancing Technologies (PET)

Se trata de un sistema de medidas, herramientas y aplicaciones que protegen la privacidad de la información mediante la eliminación o minimización de los datos personales. De ese modo se previene el procesamiento innecesario o indeseado de datos personales, sin la pérdida de la funcionalidad del sistema de información.

i. Herramientas de gestión de la privacidad, que permitan al titular elegir y controlar la forma en que sus datos son recolectados y usados.

ii. Herramientas de protección de la privacidad

1. Disociación de datos

Herramientas que apuntan a ocultar la identidad del titular, para que no pueda relacionarse los datos con una persona determinada o determinable. Por ej., las herramientas que ocultan la dirección IP del emisor.

2. Seudonimización

Permiten llevar adelante operaciones sin que se identifique al titular del dato, identificado sólo con un seudónimo.

3. Seguridad de la información

El objetivo principal es impedir el acceso no autorizado a los sistemas, archivos o a las comunicaciones a través de una red.

4. Metadatos

Se utilizan para incorporar etiquetas que le agreguen a los archivos que contengan datos personales información adicional que detalle la fuente, el consentimiento obtenido, cómo puede ser utilizado, así como las políticas de privacidad a las que está sujeto. Además puede incorporarse información que indique la cantidad de tiempo que los datos personales se pueden conservar o si el titular brindó consentimiento para ceder la información a terceros.

5. Encriptación

Utilizada no sólo para almacenar información de forma segura, sino también para asegurar su integridad, transportarla, ya sea mediante soportes físicos como a través de una red, o para generar accesos seguros a datos personales.

e. Aspectos técnicos para aplicaciones

i. Correcta utilización de los permisos

Si se trata de una aplicación móvil, verifica que los permisos que requiere sean los estrictamente necesarios para el funcionamiento adecuado. Las personas guardan en sus dispositivos móviles información muy personal, y una mala administración de los permisos

los dejará vulnerables. Un ejemplo típico del mal uso de los permisos es una aplicación de linterna que requiera acceso a los contactos del titular del dato o a su calendario.

ii. Geolocalización

Si tu aplicación accede a datos de localización, debes notificar y obtener el permiso del titular del dato, incluso si se trata de metadatos de geolocalización de fotos o videos.

4) POLITICA DE PRIVACIDAD

a. Establecimiento de una Política de Privacidad

Uno de los pasos más importantes para respetar la privacidad de los titulares de datos, es desarrollar una Política de Privacidad que explique claramente qué tipo de información se recaba, cómo se usa y con quién la compartes.

Esta política debe ser simple y, en la medida de lo posible, estandarizada, de manera tal que se facilite su lectura y comprensión por parte de los titulares de datos.

Es importante que la política refleje el tratamiento de datos que hace tu aplicación, así que no “cortes y pegues” una política genérica de otra aplicación o desarrollador, sino que trata de desarrollar una que sea comprensiva de las particularidades de tu aplicación.

Ten en cuenta que una Política de Privacidad que no responda al tratamiento de datos que hagas puede generarte inconvenientes con tus clientes, los titulares de datos de la aplicación y hasta los organismos de control, como esta DNPDP.

Un aspecto que no debes olvidar es que si introduces cambios en la Política de Privacidad, deberás notificarlas.

La Política de Privacidad debe cumplir con los siguientes lineamientos:

1. Debe contener una definición del Objeto de la Política de Privacidad (cuál es el objeto tutelado, como, por ejemplo los artículos 1° y 2° de la LPDP y sus principios), alcance (a quienes resulta exigible la política) y su compatibilidad y/o relación con las políticas de protección de la información comercial o cualquier otra política que entre en conjunción con la protección de datos personales.

2. Debes incluir una definición de los términos utilizados en la política (acordes con la LPDP).

3. Debe reflejar los principios de protección de datos personales aplicables al tratamiento de datos que haga la aplicación (acordes con la LPDP, según artículos 3°, 4°, 5°, 6°, 7°).

4. Si compartes o transfieres los datos con un tercero, debes notificarlo en forma destacada en tu política y cumplir con los requisitos de la cesión de datos, contemplados en el artículo 11 de la LPDP.

5. Contemplar la confidencialidad de los datos personales (artículo 10, LPDP), con referencia a los convenios de confidencialidad del personal y terceros que presten servicios, y de cualquier otra persona u organización que puedan entrar en conocimiento de los datos personales que trata la aplicación.

6. Hacer mención a la política de seguridad de los datos personales, y la aplicación de la Disposición DNPDP N° 11/06 (manual de seguridad).

7. Contempla, en el caso que el tratamiento de datos incluya su transferencia al exterior, los requisitos para una Transferencia Internacional de datos personales (aplicando el artículo 12 LPDP y Decreto N° 1558/01). Ten en cuenta que el almacenamiento en la nube se considera una transferencia internacional de datos.

8. En el caso que el uso de la información personal incluya la finalidad de publicidad, debe contemplarse el cumplimiento de las obligaciones específicas para este tipo de tratamiento (artículo 27 LPDP y Decreto N° 1558/01), Disposiciones DNPDP N° 10/08 y 4/09.

9. Prestaciones de servicios de tratamiento de datos por cuenta de terceros (artículo 25 LPDP y Decreto N° 1558/01).

10. Establece el procedimiento para cumplir con los derechos de los titulares de los datos (derechos de acceso, rectificación, supresión y bloqueo, artículos 14, 15, 16 y 27, inc. 3 de la LPDP).

11. Comunica mediante la Política quien es el Encargado de Protección de Datos (a cargo de velar por la correcta y efectiva aplicación de la política y su relación tanto con los titulares de datos como con el órgano de control). Puede ser una persona física o un área dentro de tu organización.

b. Asegúrate que alguien en tu organización sea responsable de pensar acerca de la privacidad.

Al menos una persona en la organización debe velar porque las aplicaciones que desarrolles cumplan con los principios de la protección de datos. Si se trata de un emprendimiento unipersonal, debes encargarte vos mismo de esta función.

Será tarea de esta persona:

- Asegurarse que las aplicaciones y el tratamiento de datos que hagan cumplan con la normativa de protección de datos (Ley N° 25.326, decreto reglamentario, disposición de la DNPDP).

- Revisar y mantener actualizada la Política de Privacidad de la organización, y asegurarse que las aplicaciones que desarrollen la cumplen.

- Responder las consultas vinculadas a la Política de Privacidad, el ejercicio de los derechos del titular del dato y los requerimientos de la DNPDP.

c. Capacitación del personal en privacidad

Todas las personas que trabajen en tu organización deben estar al tanto de las obligaciones que tienen con relación al tratamiento de datos. Es la mejor manera de evitar que por error o desconocimiento hagan incurrir a tu organización en un incumplimiento.

d. Control de terceros con los que se intercambian datos personales

La Ley N° 25.326 establece la responsabilidad solidaria entre quienes intercambian información. Esto es que si a quien le mandas o de quien recibes información personal cometen algún incumplimiento, también te podrían reclamar a ti.

Solamente cede o recibe datos personales de personas u organizaciones confiables y verifica que se encuentren debidamente inscriptos en el Registro Nacional de Bases de Datos de la DNPDP.

5) CONTROL DE LA INFORMACIÓN PERSONAL POR PARTE DE SUS TITULARES

Bríndales a quienes hagan uso de tus aplicaciones y a los titulares de los datos en general el control de su información personal, particularmente cuando se trata de información sensible, íntima o cuando se le den usos que no sean los obvios o comunes.

Los usos que se hagan de los datos personales deben provenir de una elección consciente e informada de sus titulares.

Permite que accedan a la información que almacenes sobre ellos y que puedan rectificar información errónea o desactualizada, o que puedan suprimir información cuando corresponda.

Además debes esforzarte porque la información personal que almacenas sea cierta, adecuada, pertinente y no excesiva con relación a los usos que le das y que motivaron su recolección.

Procura recabar siempre que sea necesario el consentimiento del titular del dato para usar su información personal.

Trata de limitar al mínimo posible y a lo estrictamente necesario la cantidad de información personal que recolectas y utilizas, y destruye de manera segura aquellos datos que te hayan dejado de ser útil.

6) APLICACIONES MÓVILES

Las aplicaciones desarrolladas para dispositivos móviles generalmente tendrán la limitación del tamaño de la pantalla.

Deberás ser creativo para poder mostrar la información de tu Política de Privacidad de una manera que le resulte útil a los titulares de datos con el desafío adicional que genera un espacio pequeño como la pantalla de un teléfono celular.

Algunos consejos que puedes aplicar:

a. Separar la información en distintas capas

Pocas personas estarán dispuestas a leer TREINTA (30) páginas de una Política de Privacidad, y mucho menos en la pequeña pantalla de un celular. Para evitarlo, deberás clasificar la información que brindas en tu Política de Privacidad, separarla en distintas capas y colocar la más importante en las capas superiores. Luego ofrecer hipervínculos para aquellos que quieran profundizar más y conocer los detalles.

b. Proveer al titular del dato un tablero de privacidad

Podría ser útil ofrecer una herramienta de configuración de privacidad, con un diseño atractivo y amigable que le permita al titular del dato elegir fácilmente las opciones de privacidad.

c. Utilizar técnicas para llamar la atención del titular del dato

Debes procurar llamar la atención de tu titular del dato sobre la información importante de tu Política de Privacidad.

Para ello puedes recurrir a una serie de recursos que te brinda la plataforma móvil, como indicaciones visuales o sonoras:

1. Gráficos: utiliza íconos, etiquetas o imágenes que llamen la atención del titular del dato vinculada a un texto que provea más información. Esto puede resultar útil en determinado

momento del uso de la aplicación, como cuando se disponga a utilizar los datos personales del titular del dato: por ejemplo, si se va a geolocalizar una foto, se activa un símbolo que advierte de esto al titular del dato y de ser necesario, se recaba su consentimiento.

2. Colores: Llama la atención de los titulares de datos mediante el uso de colores y la variación de intensidad de los mismos. La intensidad del color puede ser proporcional a la importancia de la decisión o sensibilidad de la información.

3. Sonidos: Otro modo apropiado de llamar la atención del titular del dato es a través de sonidos, cuando sea necesario una decisión del titular del dato o debas proveerlo de información importante acerca del uso de sus datos personales.

7) USO DE APLICACIONES POR NIÑOS

Si tu aplicación puede ser usada por niños o adolescentes, deberás procurar un cuidado especial.

Se trata de un grupo que hace un uso intensivo de la tecnología, que la saben manejar, pero que por su edad pueden carecer de la reflexión crítica necesaria para identificar los peligros que el mal uso de su información personal puede aparejar. Son una población vulnerable, y por lo tanto, será necesario que incorpores salvaguardas especiales para resguardarlos.

- Limita al máximo el tipo y la cantidad de información que sobre ellos recolectas.

- Contempla estrictas medidas de seguridad sobre la información que necesariamente debas recabar.

- Evita compartir información personal de menores con terceros.

- Bríndales información adecuada a su nivel de comprensión sobre el uso responsable de sus datos y alerta sobre los peligros que se relacionan a una mala utilización.

- Siempre que corresponda, obtén el consentimiento de sus padres. Establece mecanismos de resguardos para mantenerlos informados acerca de los usos que se hacen de la información personal de los menores.

8) CONTACTO CON LA DNPDP Y LEGISLACION APLICABLE

La DNPDP es un órgano dependiente del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, con sede en Sarmiento 1118, piso 5°, de la CIUDAD AUTÓNOMA DE BUENOS AIRES.

En la página web de la DNPDP (www.jus.gov.ar/datospersonales) podrás encontrar toda la

normativa de protección de datos personales, que incluye la LPDP, su decreto reglamentario y todas las disposiciones del Director Nacional de Protección de Datos Personales, así como mucha información adicional sobre privacidad y protección de datos.