

Temario

- Ley de Protección de Datos Personales.
- Guía de Buenas Prácticas en Privacidad para el desarrollo de aplicaciones.
- Política de Privacidad.
- Términos y Condiciones.
- Material Extra.
- ¿Cómo lo aplico?



Derecho a la intimidad - Evolución

1ª Etapa:

- “La casa de un hombre es su castillo” invocada por líderes de revolución norteamericana para oponerse al poder estatal...
- “Derecho a ser dejado solo”...

2º Etapa:

- Posguerra se reconoce como derecho constitucional y amplía el concepto a la persona y su individualidad.

3º Etapa (**autodeterminación informativa**). Es el derecho de cada uno a:

- controlar los datos que hacen a su persona;
- decidir cuándo y qué información puede ser objeto de procesamiento automatizado.
- controlar la veracidad de la información y el uso que se hace de ella.

Derecho a la Intimidad **HOY Y MAÑANA**

“Lo que pasa dentro de la casa sale por el cable de internet”.

- Big data.
- Huella digital.
- Comercio electrónico.
- Tratamiento automatizado.
- Elaboración de perfiles.
- Inteligencia Artificial (IA).
- IoT / 5G / realidad virtual (¿metaverso?).
- Investigaciones penales.



Protección de Datos Personales

Ley 25326 (año 2000)

- **Ámbito de aplicación:** Tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para **garantizar el derecho al honor y a la intimidad** de las personas, así como también el **acceso a la información** que sobre las mismas se registre.
- **Datos personales:** información de cualquier tipo referida a personas físicas o de existencia ideal **determinadas o determinables**.
- **Datos sensibles:** Datos personales que **revelan** origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Excepciones: interés general por ley o con fines estadísticos sin que puedan identificarse sus titulares. La Iglesia Católica, asociaciones religiosas y organizaciones políticas y sindicales pueden llevar registro de sus miembros.

Protección de Datos Personales

Ley 25326 - Principios Generales

Licitud: cuando se encuentren debidamente inscriptos.

Calidad: deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se obtienen.

Consentimiento: libre, expreso e informado, por escrito. Excepciones: a) acceso público, b) en ejercicio de funciones del Estado u obligación legal, c) Nombre, DNI, CUIT, ocupación, fecha de nacimiento, domicilio -llamados “datos nominativos”-; d) relación contractual, e) operaciones entidades financieras.

Información: a) finalidad y destinatarios, b) existencia del registro y responsable, c) obligación o no de responder cuestionario, d) consecuencias, e) derechos de acceso, rectificación y supresión.

Seguridad y confiabilidad: deber de adoptar medidas técnicas y organizativas y de guardar secreto profesional.

Protección de Datos Personales

Ley 25326 – Cesión

Sólo para el cumplimiento de los fines relacionados con el interés legítimo del cedente y cesionario, con el consentimiento informado de la finalidad e identificación del cesionario.

Es revocable.

Excepciones: a) por ley, b) excepciones al consentimiento, c) entre órganos del Estado dentro de sus competencias, d) datos de salud disociados por razones epidemiológicas, e) procedimiento de disociación.

Cesionario y cedente tienen idénticas obligaciones y responden solidaria y conjuntamente.

Protección de Datos Personales

Ley 25326 – Transferencia Internacional

Prohibida respecto de los países que no proporcionen niveles de protección adecuados, salvo que se hubiere consentido.

“White list” actualizada según Resolución N° 34/19: Estados miembros de la UNIÓN EUROPEA y miembros del espacio económico europeo (EEE), REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE, CONFEDERACIÓN SUIZA, GUERNSEY, JERSEY, ISLA DE MAN, ISLAS FEROE, CANADÁ sólo respecto de su sector privado, PRINCIPADO DE ANDORRA, NUEVA ZELANDA, REPÚBLICA ORIENTAL DEL URUGUAY y ESTADO DE ISRAEL sólo respecto de los datos que reciban un tratamiento automatizado.”).

Actualmente se admite para aquellos que no alcancen un nivel adecuado, que se pueda alcanzar un nivel similar de protección mediante: a) cláusulas contractuales – Disposición N° 60/16 aprueba Contrato Modelo, b) autorregulación para empresas de un mismo grupo económico – Disposición N° 158/18 que adopta “Binding Corporate Rules”.

(ver Disposición 18/15! Almacenamiento en la nube se considera una transferencia internacional de datos)

Protección de Datos Personales

Ley 25326 – Tratamiento Automatizado

ARTÍCULO 20. — (Impugnación de valoraciones personales).

1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

Autoridad de Aplicación y normativa complementaria

Agencia de Acceso a la Información Pública – Dirección Nacional de Protección de Datos Personales. Rol activo para *aggionar* la ley:

- Disposición N° 10/15 y modif– condiciones de licitud para la recolección y uso imágenes digitales de personas con fines de seguridad.
- Resolución N° 40/18 - Política Modelo protección de datos personales para organismos públicos. Recomienda designación de agente de planta permanente como “delegado de protección de datos personales”.
- Resolución N° 47/18 – Medidas de seguridad para tratamiento y conservación de datos personales en medios informatizados y no informatizados.
- **Resolución N° 4/19 - Criterios Orientadores de mejores prácticas para aplicación de la LPDP** (C1: acceso a datos recolectado por video vigilancia; C2: explicación lógica sobre decisiones basadas en tratamiento automatizado de datos, C3: Disociación de datos; c4: datos biométricos son datos sensibles si pueden resultar potencialmente discriminatorios; C5: Consentimiento: mecanismos de validación eficaces y transferencia entre organismos públicos; **datos personales de niños, niñas y adolescentes**).

Guía Buenas Prácticas en Privacidad para el desarrollo de aplicaciones - Disposición N° 18/15

- 1) introducción.
- 2) principios de la privacidad.
- 3) privacidad aplicada al desarrollo.
- 4) política de privacidad.
- 5) control de la información personal por parte de sus titulares.
- 6) aplicaciones móviles.
- 7) uso de aplicaciones por niños.

1) introducción.

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

- **Consentimiento.** El consentimiento del titular para el uso de su información personal es la única manera en la que el tratamiento de datos es lícito, salvo que se trate de alguna excepción prevista por la Ley.
- **Finalidad.** Los datos que tus aplicaciones recolecten solo pueden ser utilizados conforme con la finalidad que originó la recolección.
- **Calidad.** Los datos personales que tus aplicaciones recaben y almacenen deben ser ciertos, adecuados, pertinentes y no excesivos en relación con la finalidad que motivó su recolección.
- **Seguridad.** La seguridad de la información es un aspecto importante de la protección de datos. Evaluá los riesgos de seguridad que tu aplicación puede aparejar, teniendo en cuenta la sensibilidad de la información personal que recolecta y almacena.
- **Confidencialidad.** Los datos personales de los que tomes conocimiento debido al tratamiento que realices son confidenciales.

3) privacidad aplicada al desarrollo (los “8 pasos”).

- contemplá la privacidad en todos los procesos de tu organización.
- desarrollá las aplicaciones con el concepto de “privacidad desde el diseño” .
- establecé una política de privacidad clara y fácilmente accesible por los titulares del dato.
- configurá por defecto como “activadas” las opciones de privacidad.
- permití a los titulares del dato que elijan y controlen la configuración de privacidad.
- limitá la cantidad de datos que recolectás o retenés.
- asegurá los datos personales recabados.
- designá a un “responsable de privacidad” o asumí vos mismo la responsabilidad del resguardo de los datos personales que hayas tratado.

4) 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 compartís.**
- 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 refleje el tratamiento de datos que hace tu aplicación, así que **no “cortes y pegues”** una política genérica de otra aplicación o desarrollador.
- Incumplir puede generar inconvenientes con tus clientes, los titulares de datos de la aplicación y hasta los organismos de control.

4) política de privacidad (cont.)

La Política de Privacidad debe cumplir con los siguientes lineamientos:

- Definir el **objeto** de la Política de Privacidad, **alcance**, y su **compatibilidad** y/o relación con las políticas de protección de la información comercial.
- Incluir una **definición** de los términos utilizados en la política.
- Reflejar los **principios** de protección de datos personales.
- Si se **comparten o transfieren datos con un tercero**, debe notificarse y cumplir con los requisitos.
- 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.

4) política de privacidad (cont.)

- En su caso cumplí con los requisitos para una **Transferencia Internacional** de datos personales. Tené en cuenta que el almacenamiento en la nube se considera una transferencia internacional de datos.
- En el caso de 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).
- Tené en cuenta lo que establece el artículo 25 LPDP y Decreto N° 1558/01 en relación con las **prestaciones de servicios de tratamiento de datos por cuenta de terceros**.
- Establecí 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).
- Comunicá quién es el **Encargado de Protección de Datos**.

5) control de la información personal por parte de sus titulares.

- Brindales 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.
- Permitiles **acceder** a la información que almacenes sobre ellos y dáles la posibilidad de **rectificar** información errónea o desactualizada, o de **suprimirla**, cuando corresponda.
- Procurá recabar, siempre que sea necesario, el **consentimiento** del titular del dato para usar su información personal.

6) aplicaciones móviles.

Algunos consejos que podés aplicar:

- Separar la información 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.
- Proveer al titular del dato un **tablero de privacidad**, con un diseño atractivo y amigable, que le permita elegir fácilmente las opciones de privacidad.
- Utilizar técnicas para **llamar la atención** del titular del dato, a través de recursos que te brinda la plataforma móvil, como indicaciones visuales o sonoras.

7) uso de aplicaciones por niños.

- Limitá al máximo el tipo y la cantidad de información que recolectás sobre ellos.
- Contemplá estrictas medidas de seguridad sobre la información que necesariamente debas recabar.
- Evitá compartir información personal de menores con terceros.
- Brindales información adecuada a su nivel de comprensión sobre el uso responsable de sus datos y alertalos sobre los peligros que se relacionan con una mala utilización.
- Siempre que corresponda, obtené el consentimiento de sus padres.
- Establecé mecanismos de resguardo para mantenerlos informados acerca de los usos que se hacen de la información personal de los menores.

Términos y condiciones - Nociones básicas

¿Qué son los términos y condiciones de una aplicación o de una página en Internet?

- Son las **cláusulas legales** que establecen la forma en la que podés usar la información y acceder a los contenidos de una página web o aplicación.
- **Establecen lo que el dueño de la página o aplicación hará con tus datos personales y con los datos que generés.**
- Son condiciones unilaterales y tenés que aceptarlas para poder usar los servicios de la página web (contrato de adhesión).
- **Cuando aceptas los términos y condiciones das tu consentimiento para que la empresa almacene, procese, analice o utilice tus datos para distintos fines.**



Términos y condiciones - Contenido

¿Qué cuestiones deben informarse en los términos y condiciones?

- **Datos de identificación:** se debe informar los datos del profesional o la empresa titular de la página web.
- **Derechos de propiedad intelectual e industrial:** se debe informar quién es el titular de los elementos que componen la página web así como el tipo de licencias de uso que se da a los usuarios.
- **Pasos a seguir para contratar:** se debe informar cuáles son los pasos que debe seguir para adquirir los productos o servicios y se le debe indicar sus derechos y obligaciones.
- **Producto o servicio objeto de contratación:** se debe establecer de forma clara y precisa cuál es el producto o servicio que puede contratar el usuario a través de la web.
- **Precios, duración y formas de pago:** se debe indicar si los precios incluyen impuestos o si la compra tiene cargos adicionales; cuál es el tiempo de duración; formas y condiciones de pago, y cuáles son las consecuencias en caso de mora o incumplimiento.

Términos y condiciones - Contenido (cont.)

- **Reglas de conducta:** en el caso que sea necesario registrarse, se deben establecer las condiciones específicas de uso, los derechos y las responsabilidades si su conducta no es acorde con las reglas de comportamiento.
- **Responsabilidades:** tienen que establecer de forma precisa las responsabilidades que se asumen, así como las limitaciones de responsabilidad.
- **Garantías:** dar a conocer las garantías que tiene por la adquisición de un producto o servicio.
- **Legislación aplicable y sistema de solución de conflictos:** dar a conocer las normas que serán de aplicación a la relación contractual, así como el sistema extrajudicial de solución de conflictos o los tribunales competentes para resolver las controversias que surjan.
- **Otros:** en caso de que se realicen ofertas y promociones deben incluirse las condiciones específicas que regirán las ofertas o promociones. Si se ofrece al usuario un servicio de post-venta, se deben informar las condiciones que regulan el servicio post-venta.

Términos y condiciones - Lenguaje Claro

¿Por qué es importante que los términos y condiciones estén redactados en **lenguaje claro**?

- La normativa legal exige que tengas conocimiento de las condiciones de contratación de un producto o servicio.
- Por eso, una redacción incompleta o inadecuada de los términos y condiciones puede dar lugar a una sanción por parte de un ente público.
- **Las condiciones tienen que estar escritas en forma clara, es decir, evitando una redacción ambigua u oscura, ya que el usuario debe conocer y entender las reglas a las que se somete.**

Registro y Autenticación con redes sociales

- Pérdida de control sobre los datos personales, cuando el servicio accede a determinados datos del perfil social del usuario.
- Utilización de los datos obtenidos de la red social para finalidades distintas de las consentidas por el usuario.
- Acceso de las redes sociales a una mayor información sobre nuestro uso de las aplicaciones o comportamiento por Internet, lo que facilita el seguimiento y perfilado.
- Ante una brecha de seguridad del servicio no se verá afectada la contraseña del usuario, pero sí puede verse afectada mucha información del perfil social de usuarios, incluidos datos sobre sus intereses y perfilado para publicidad comportamental.
- En caso de perder el control sobre la cuenta de la red social (robo de credenciales), se pierde también el control del resto de servicios donde nos hemos registrado con esa cuenta, que podrían también verse comprometidos.
- **Se deben brindar las garantías adecuadas para que no se materialicen riesgos como la pérdida del control sobre los datos personales, ya que podría dar lugar a flujos de datos que acaben siendo utilizados para el seguimiento o el perfilado de las personas.**

Material Extra – Anteproyecto para una nueva Ley de Protección de Datos Personales

- Desde el 12 de septiembre hasta el 11 de octubre se habilitó la instancia de consulta pública sobre la propuesta de actualización de la Ley.
- Documentos recibidos en las mesas de debate: 7.
- Documentos de referencia:
 - Antecedente 2018 - Proyecto de Ley de Protección de Datos Personales (perdió estado parlamentario).
 - Ley N° 27.483 de aprobación del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
 - Reglamento General de Protección de Datos (RGPD) - Unión Europea.
 - Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos (RIPD).
 - Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones de la OEA.
 - Recomendación sobre la Ética de la Inteligencia Artificial - UNESCO.
 - Leyes de Protección de Datos de Brasil y Ecuador.
- Se presentaron más de 140 aportes y opiniones de la ciudadanía, organizaciones de la sociedad civil, universidades e investigadores, sector privado y sector público nacional e internacional.
- La próxima etapa es el análisis de todos los aportes y opiniones, a fin de consolidar un informe que permita avanzar en una versión definitiva del anteproyecto para la actualización de la Ley de Protección de Datos Personales.

<https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales>

¿Cómo lo aplico a la APP para clubes de barrio?

- Registrar la base de datos en <https://www.argentina.gob.ar/registrar-bases-de-datos-personales-privadas>
- Corroborar que los datos que se solicitan sean adecuados, pertinentes y no excesivos en relación al ámbito y finalidad, y deben ser destruidos cuando dejen de serlo.
- Indicar en la política de privacidad: la finalidad, los destinatarios, la existencia de la base de datos, el carácter obligatorio o facultativo del dato, la consecuencia de la negativa o inexactitud y el derecho de acceso, rectificación y supresión.
- En el caso del sexo deberá ser optativo.
- Es necesario el consentimiento expreso en virtud del datos sensible que se solicita. Para los menores la Resolución de la Agencia remite al CCyC y el consentimiento podría prestarse a partir de los 13 años. Es aconsejable que sea a partir de los 16 y considerando la madurez y entendimiento sobre el acto a realizar eventualmente exigirse el consentimiento de quien ejerza la responsabilidad parental.

Fuentes

- <http://www.jus.gob.ar/media/3075908/guiabpsoftware.pdf>
- <https://www.argentina.gob.ar/justicia/convoenlaweb/situaciones/porque-es-importante-leer-los-terminos-y-condiciones-de-una-pagina-en-internet-o-aplicacion>
- <http://lenguajeclaroargentina.gob.ar/wp-content/uploads/2019/08/Gu%C3%A1Da-SAIJ-de-lenguaje-claro.pdf>
- <https://www.aepd.es/es/prensa-y-comunicacion/blog/riesgos-privacidad-iniciar-sesion-cuentas-rrss-otras-aplicaciones>

¡Gracias!

Mariano Cervellini
marianocer@protonmail.com