Guía de Protección de Datos Personales para empresas (en especial micro, pequeñas y medianas empresas MIPYMES)

Autor
URCDP

Fecha de creación
07/03/2024

Tipo de publicación
Guías

Resumen

Esta guía orienta sobre la Protección de Datos Personales a micro, pequeñas y medianas empresas (MIPYMES)

A quiénes está dirigida esta guía

En Uruguay, la protección de datos personales es un derecho humano, reconocido en el artículo 1° de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data.

En el mundo actual, la protección de datos personales es un valor agregado para las empresas que la consideran en su gestión diaria, y para las personas que la integran.

Las empresas que resguardan debidamente los datos personales que gestionan son más valoradas por las personas, y reducen su exposición ante eventuales ataques informáticos, y a posibles reclamos de quienes se hayan visto afectados por revelaciones indebidas de su información personal. Por ello, la protección de datos se encuentra estrechamente vinculada a otros temas centrales en la vida de las empresas como la gestión de riesgos o la gestión de calidad.

La puesta en práctica de medidas que tiendan a proteger adecuadamente los datos personales implican una actividad de análisis por parte de las empresas que pueden generar costos económicos asociados a la contratación eventual de especialistas, la adquisición de sistemas o desarrollos que permitan resguardar la información, la capacitación de personal, entre otros.

Esta guía tiene por objetivo facilitar el cumplimiento de las normas de protección de datos en el marco de las actividades empresariales, teniendo en cuenta recomendaciones ya emitidas por la Unidad Reguladora y de Control de Datos Personales (URCDP), el uso de herramientas que facilitan la gestión en la materia, incluso gratuitas, modelos de cláusulas, cursos virtuales, entre otras.

Además, se propone una serie de acciones que las empresas deben adoptar para el cumplimiento de las obligaciones en esta materia, y se pone a disposición las definiciones más importantes de la protección de datos personales. Esta guía puede complementarse con la Guía General en Protección de Datos Personales en Uruguay, donde se desarrollan con mayor extensión algunos de los conceptos que se detallan a continuación.

Conceptos relevantes

Cuando nos referimos a “datos personales”, debemos considerar que éstos se definen en forma amplia, como toda información que identifique o haga identificable a una persona (nombre, apellido, imagen, voz, número de cuenta bancaria, domicilio, origen racial o étnico, etcétera). La ley identifica a la persona con la denominación “titular del dato”; por ejemplo, desde esta perspectiva son “titulares de datos”: clientes, empleados, proveedores, entre otros.

En este marco, la gestión de la información de los titulares de los datos para finalidades propias (gestión de clientes, contacto de proveedores, etcétera) convierten a la empresa en un “responsable de tratamiento”. Si esa gestión de información se encarga a un tercero (como por ejemplo estudios contables, estudios jurídicos, *call centers*), ese tercero se denomina “encargado de tratamiento”. La distinción entre responsable y encargado de tratamiento es importante porque la responsabilidad en uno y otro caso es diferente según la normativa aplicable.

La gestión de información, desde que esta se recolecta hasta que se elimina, pasando por su conservación, comunicación, almacenamiento y todas las restantes etapas de la vida de un dato, se define por la ley como “tratamiento de datos”. Cuando los datos se almacenan de forma lógica, ya sea en formato digital o papel (una libreta de direcciones, una planilla de cálculo, etcétera), nos encontramos ante una “base de datos”.

Conocimiento del estado de situación en la empresa

La primera acción que debe realizar toda empresa, es -además de conocer la existencia de la normativa- entender el alcance de las obligaciones que conlleva, y realizar un análisis del estado de situación que permita su adecuado cumplimiento.

Algunas preguntas iniciales pueden ayudar a proveer un diagnóstico preliminar del estado de situación de la empresa en esta materia.

En el desarrollo de acciones para el cumplimiento de la ley, contar con el asesoramiento de personas de distintos perfiles que conozcan de la materia se en la empresa o de ella, permitirá alcanzar mejores resultados aunque ello no es imprescindible para el cumplimiento de ciertas obligaciones formales y acciones específicas, que pueden ser realizadas por las propias empresas a través de las herramientas, modelos y sugerencias que se proponen en esta Guía.

1 ¿Conoce la existencia de una ley de protección de datos personales?

Si la respuesta es no, debo tener presente que la Ley N° 18.331, de 11 de agosto de 2008, establece un derecho de todas las personas a la protección de sus datos personales, y obligaciones que todas las empresas privadas y todos los organismos públicos deben cumplir. Existe además un organismo público que controla su cumplimiento, la Unidad Reguladora y de Control de Datos Personales (URCDP), la que puede fiscalizar e imponer sanciones.

Para conocer más de la Ley, y de la protección de datos en general, puede acceder a Curso en línea sobre la Ley de Protección de Datos Personales (versión 2016) y a otra información en el portal web de la URCDP.

2 ¿Mis asesores y proveedores de sistemas y desarrollos conocen de la existencia de la ley?

Es importante que los profesionales que asisten a las empresas, y aquellos que les brindan soporte técnico tengan un conocimiento completo de la normativa aplicable.

Consultar con profesionales y proveedores de la empresa (abogados, escribanos, contadores, técnicos) a fin de que éstos puedan asesorar debidamente a la empresa cuando sea necesario.

3 ¿Se procedió a inscribir las bases de datos?

Esta es una de las obligaciones de las empresas, y es relevante porque toda la gestión de la información, para ser lícita, depende de esta inscripción. Las bases de datos dependen de los fines para las cuáles se crean, como veremos luego, y se pueden tener tantas bases como finalidades. En general, en las empresas pequeñas encontramos bases de clientes, empleados, proveedores, y videovigilancia (las imágenes también son datos personales), lo que no excluye que puedan existir otras.

La inscripción de la base de datos es un procedimiento sencillo que en general puede realizarse completamente en línea, sólo requiere contar con usuario gub.uy y completar un formulario electrónico. Se accede a través del Sistema de Gestión de la URCDP.

4. ¿Se consideró la forma de almacenar y resguardar la información de clientes, empleados, proveedores y otras personas?

La seguridad de la información y la protección de datos personales, si bien son diferentes, sirven al propósito del cuidado de la información. Tener fichas de clientes sin medidas de seguridad o tener, por ejemplo, una planilla con esa información en una computadora al alcance de todos generan situaciones de riesgo innecesarias.

Establecer contraseñas de acceso en caso de sistemas, asesorarse en su caso con profesionales informáticos para establecer medidas de seguridad, en ciertos casos adoptar medidas físicas de seguridad (como por ejemplo cerrar con llaves u otras medidas).

5. ¿La empresa usa servicios para gestionar la información a través de internet?

El empleo de servicios a través de internet para cumplir con partes del negocio (por ejemplo, almacenar información) es cada vez más común, y se enmarca en general dentro del concepto de “nube”.

Usar este tipo de servicios puede significar que los datos se estén transfiriendo fuera del país, y si el país de destino no es adecuado a los estándares uruguayos, puede requerirse una autorización especial de la URCDP. En ese caso, puede realizarse una solicitud a través del sistema de la Unidad

6. ¿Los empleados conocen la normativa?

Es importante que los integrantes de la empresa conozcan la normativa. No sólo por tratarse de un derecho y porque existen obligaciones, sino además porque las personas que se vinculan con la empresa tienen derechos específicos que pueden ejercer, y debe responderse en un plazo de 5 días hábiles desde su ejercicio.

Resulta importante que se solicite a los empleados que conozcan las normas como por ejemplo accediendo a Curso en línea sobre la Ley de Protección de Datos Personales (versión 2016) o a otras. alternativas de capacitación disponibles que pueden consultarse en la web de la URCDP (gub.uy/urcdp) o al correo infourcdp@datospersonales.gub.uy.

7. ¿Se cuenta con procedimientos para la respuesta de ejercicio de derechos?

odas las personas pueden ejercer los derechos de información, acceso, rectificación, actualización, inclusión, supresión e impugnación de valoraciones personales que están previstos en la Ley, en forma, de principio, gratuita.

Como se verá luego, el plazo para dar respuesta a estas solicitudes es breve (5 días hábiles) por lo que es recomendable tener un canal específico e informado a las personas, y un responsable dentro de la empresa que conozca el procedimiento y pueda responderlas dentro del plazo.

Obligaciones de los responsables y encargados de tratamiento

Los responsables y encargados de tratamiento deben cumplir con un conjunto de obligaciones, enmarcadas en principios definidos en la Ley. Existen obligaciones formales expresamente establecidas, como la inscripción de bases de datos, la designación de delegados de protección de datos (en determinados casos) y la comunicación de vulneraciones de seguridad (cuando éstas ocurren). Además, existen criterios para realizar el tratamiento de datos personales y para asegurar que las personas puedan ejercer adecuadamente sus derechos.

En el siguiente cuadro, se presentan distintas acciones que deben seguir los responsables y encargados para cumplir con los principios que establece la ley. Esto no excluye otras acciones que puedan adoptarse en cada caso concreto.

Acciones a seguir por los responsables

Acciones	Cuando corresponde	A tener en cuenta	Forma de realizarlo - Herramientas disponibles
Inscripción de base de datos	Siempre que se cuente con bases de datos.	Plazo: 90 días desde el inicio de actividades.	A través del Sistema de Gestión de la URCDP.
Actualización de base de datos	En los casos expresamente indicados y cuando ya exista una Base de Datos registrada.	Solo se deberá actualizar si: a) existe una alteración del 20% de los datos indicados en la solicitud; b) si existen modificaciones estructurales (agregado o supresión de un campo, cambio de la finalidad, alternación significativa de la información).	A través del Sistema de Gestión de la URCDP.
Definición de la finalidad	Siempre.	Se trata del para qué se recolectan los datos, qué va a realizar el responsable de la base de datos con ellos. Los datos que se obtienen no pueden ser utilizados para finalidades distintas o incompatibles con las que motivaron su obtención y no pueden conservarse datos si dejaron de ser necesarios.	Un ejemplo sobre la información de clientes puede ser: ¿se recolectan sus datos para ofrecerles publicidad? ¿para darles un beneficio particular?, ¿para hacer un registro de ventas?. Estas preguntas permitirán definir la finalidad y en consecuencia las categorías y la cantidad de datos que se van a solicitar.
Análisis de los datos recolectados o almacenados	Siempre.	Corresponde realizar una verificación en forma previa a recolectar los datos, para determinar si son verdaderos, ecuánimes, adecuados, imparciales, no excesivos y si se ajustan a la finalidad para los que se recolectaron.	La forma más sencilla es analizar los datos personales que la empresa solicita y determinar si son estrictamente necesarios para esa finalidad (por ejemplo, si se trata de datos de proveedores no se necesita conocer su estado civil).

Acciones	Cuando corresponde	A tener en cuenta	Forma de realizarlo - Herramientas disponibles
Revisión de los datos personales	Siempre.	Además de la verificación previa, se debe contar con un proceso para la revisión y actualización permanente de la información personal.	Resulta conveniente establecer parámetros de revisión de datos personales, y un procedimiento que permita rectificar la información que perdió vigencia o .eliminar fácilmente la que dejó de ser necesaria.
Elaboración de cláusulas de consentimiento	Siempre que se use como base el consentimiento.	El consentimiento debe ser libre, previo, expreso, informado y documentado, y tiene ciertos requisitos para ser válido. El correcto armado de cláusulas de consentimiento es vital para asegurarse que los datos pueden ser tratados dentro de la ley.	Se encuentra disponible un modelo de cláusulas de consentimiento que deberán adaptarse al caso concreto.
Uso de datos personales en páginas web	Siempre que trate información personal en la web.	Si se recolecta información personal a través de páginas web, se deben establecer cláusulas de consentimiento específicas y una política de privacidad.	Se encuentran disponibles modelos de política de privacidad y de cláusulas de consentimiento. Estos modelos deben adaptarse al caso concreto.
Uso de aplicaciones de mensajería para el contacto con los clientes	Siempre que se establezcan canales de contacto a través de aplicaciones de mensajería.	Debe tenerse en cuenta que el uso de estas aplicaciones puede significar la recolección de datos personales, no sólo por parte de la empresa, sino también del proveedor de la aplicación, por lo que es importante que las personas conozcan esta situación, y darles la posibilidad de contactarse a través de mecanismos alternativos.	Se encuentran disponibles recomendaciones específicas en el documento sobre "Consideraciones respecto al uso de aplicaciones de mensajería"
Poner en práctica medidas de seguridad de los datos personales	Siempre.	El primer aspecto a considerar es poner en práctica medidas de seguridad físicas y lógicas para la protección de los datos personales que se traten Ejemplos de estas medidas son guardar en lugares seguros bases físicas, establecer accesos diferenciados para bases de datos en formato digital, utilizar herramientas informáticas adecuadas, contratar servicios de nube de proveedores confiables.	En el documento sobre el "Marco de Ciberseguridad" se podrán encontrar un conjunto de medidas al respecto.

Acciones	Cuando corresponde	A tener en cuenta	Forma de realizarlo - Herramientas disponibles
Comunicar vulneraciones de seguridad	Cuando se produzcan vulneraciones de seguridad.	Se deben realizar diversas comunicaciones cuando sucede alguna vulneración de seguridad en las bases de datos que contienen datos personales de los titulares, dentro de un plazo de 24 horas a la Unidad, y por los medios puestos a disposición por ésta.	La comunicación se puede realizar a través del Sistema de Gestión de la URCDP. Por más información se encuentra disponible la "Guía de comunicación de vulneraciones de seguridad"
Mantener reserva de la información personal	Siempre.	Se debe mantener la reserva de la información personal de terceros obtenida por el vínculo con la empresa, sin limitación de tiempo. La sanción en caso de incumplimiento es de carácter penal.	Sin perjuicio de que se trata de una obligación legal, resulta conveniente incluir esta previsión en los contratos con el personal y con otros terceros que puedan trabajar para la empresa.
Privacidad por diseño y por defecto	Siempre.	Siempre que se vaya a desarrollar un nuevo tratamiento de datos personales se deben incorporar medidas de privacidad por diseño y por defecto, que implica poner en práctica en todo el ciclo de vida de los datos mecanismos que protejan estos datos.	Los artículos 7° y 8° del Decreto N° 64/020, de 17 de febrero de 2020 dan algunos ejemplos (tales como el uso de técnicas de disociación, seudonimización y minimización de datos, mecanismos para asegurar el ejercicio de los derechos de los titulares, documentación de los consentimientos, etcétera).
Evaluaciones de impacto	En los casos expresamente previstos por la normativa (tratamiento de datos sensibles, de personas vulnerables, especialmente protegidos, de más de 35.000 personas, cuando se transfieran datos personales a países no adecuados, cuando se traten datos biométricos, entre otros).	Las evaluaciones de impacto tienen como objetivo determinar los posibles riesgos para las personas en el tratamiento de su información personal y tomar medidas para mitigar esos riesgos.	Para saber cómo realizar una evaluación de impacto puede consultarse la "Guia para la realización de Evaluaciones de Impacto" de la URCDP y Agencia de Acceso a la Información Pública de Argentina.
Designación de delegado de protección de datos	Sólo corresponde obligatoriamente si se tratan datos sensibles como negocio principal (origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e información referente a la salud o a la vida sexual) o si se tratan datos de más de 35.000 personas. También se puede designar en forma voluntaria como una medida de responsabilidad proactiva.	En el primer caso, puede tratarse de un laboratorio, un consultorio médico, una organización que nuclee personas de determinado origen étnico, entre otros. En el segundo caso, deberá considerarse toda la información que se gestiona en las distintas bases de datos de la empresa, y determinar si se excede o no el límite de 35.000 personas establecido por la reglamentación.	En caso de corresponder la designación, el delegado debe tener determinadas características y cumplir las funciones indicadas en la normativa y comunicarse su designación a través del Sistema de Gestión de la Unidad

Derechos de los titulares de los datos personales

Así como se establecen principios, la Ley también regula los derechos de los titulares de datos personales. La obligación principal de las empresas es brindar canales que permitan el ejercicio de estos derechos de forma sencilla, y asegurarse de dar la respuesta que en cada caso corresponda en un plazo de 5 días hábiles de recibida la solicitud.

Derechos de los titulares de datos personales

Derecho	¿Qué se debe tener en cuenta?	¿Cómo se cumple y facilita su ejercicio?	¿Qué plazo hay para cumplir?
Derecho de información	El titular del dato personal debe saber para qué van a ser utilizados sus datos, antes de que sean recolectados, o si lo solicita expresamente.	Cuando recolecto datos del titular debo informarle con qué fin se recolecta, dónde puede ejercer sus derechos, qué sucede si no da su consentimiento, si se utilizan medios automatizados, si se van a realizar comunicaciones o transferencias internacionales. Si se perfilan personas por medios automatizados deben informarse los criterios de valoración, los procesos aplicados y la solución tecnológica o el programa utilizado. Puede la empresa además tener a disposición esta información en forma permanente en su sitio web.	Si se recolecta del titular, se debe dar la información previamente. Si es por una solicitud de éste, se debe otorgar la información en 5 días hábiles.
Derecho de acceso	El titular de datos personales, acreditando su identidad, puede solicitar toda la información que posea la empresa de su persona	Se debe entregar la información al titular, en forma gratuita cada seis meses, sin exigir fundamentación.	5 días hábiles desde la solicitud.
Derechos de rectificación, actualización, inclusión y supresión.	El titular de datos personales, acreditando su identidad, puede solicitar la rectificación, actualización, inclusión o supresión de su información personal.	Si se acredita el error o inexactitud de la información se debe rectificar, actualizar o incluir esa información. Si corresponde la supresión debo realizarla, y si no corresponde se debe informar las razones de la negativa.	5 días hábiles desde la solicitud.
Derecho a la impugnación de valoraciones personales	El titular de datos personales tiene derecho a no verse sometido a un tratamiento automatizado de datos (como por ejemplo el uso de perfiles) que finalice en una decisión que lo afecte. Tendrá derecho además a obtener información sobre los criterios de valoración utilizados, y el programa o la solución tecnológica aplicada.	En caso de uso de sistemas que automáticamente perfilan a las personas según su historial de crédito, laboral, etc., debo considerar que si ello implica una decisión que afecta al titular, debo proveer información completa en caso de requerirse, y el titular tiene además la posibilidad de dirigirse al Poder Judicial e impugnar esa decisión.	5 días hábiles desde la solicitud.

En función de lo mencionado, la empresa debe tener en cuenta, para el ejercicio de todos los derechos, las siguientes consideraciones:

- Establecer canales predeterminados para recibir las solicitud de los titulares de los datos (ejemplo: un correo electrónico específico), asignado su control a una persona determinada, e informarlo a los titulares de los datos (por ejemplo en la política de privacidad del sitio web).
- Utilizar formularios predeterminados
- Contar con la información personal de cada persona ordenada, de forma de acceder fácilmente a ella ante una solicitud.
- Recordar que el plazo para habilitar el ejercicio del derecho es de 5 días hábiles.
- Recordar que el ejercicio de todos los derechos corresponde exclusivamente al titular del dato, acreditando debidamente su identidad, o mediante representante debidamente autorizado.

Modelos

1. Política de privacidad
2. Modelos de cláusulas

Guías

Guía general de protección de datos personales en Uruguay

Guía de evaluación de impacto de la protección de datos

Guía de cumplimiento de obligaciones por entidades extranjeras

Guía para la gestión, documentación y comunicación de vulneraciones de seguridad en datos personales