Protección de datos personales

Mediante Decreto número 64/020 de fecha 17/02/020 se reglamentó la Ley 19.670 de 15/10/018 que establece nuevas disposiciones en materia de protección de datos personales.

La protección de datos personales consiste en el amparo a las personas de sus datos personales registrados en cualquier soporte que los haga suceptibles de tratamiento, ante la posible utilización de terceros no autorizados.

El tratamiento de datos refiere a operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permiten el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

El responsable del tratamiento de los datos es la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso de la misma.

Ambito territorial de aplicación

La normativa se aplica para los casos en que el responsable o encargado del tratamiento de la base de datos se encuentre en estado uruguayo independiemtemente de la forma jurídica adoptada para ello.

En ciertos casos también es de aplicación para cuando el responsable o encargado se encuentra en el extranjero:

- Si las actividades de tratamiento de datos están relacionadas con la oferta de bienes o servicios dirigidos a habitantes de la República.
- Si están relacionadas con el análisis del comportamiento de los habitantes de la República, incluyendo las destinadas a la elaboración de perfiles.
- Lo disponen normas de derecho internacional público o un contrato.
- En el tratamiento se utilizan medios situados en el país, tales como redes de información y de comunicación, centros de datos e infraestructura informática en general.

Medidas de seguridad

El responsable y el encargado de tratamiento, deben adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales, asi como deberán en el ejercicio de una responsabilidad proactiva deberán preveer la privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación

Si ocurre un incidente de seguridad que afecte los datos personales se debe iniciar el procedimiento previsto para minimizar el impacto de ese incidente dentro de las 24 horas de constatado el mismo y debe ser comunciado dentro de las 72 horas a la Unidad Reguladora y de Control de Datos Personales, dicha comunicación deberá contener información relevante, tal como la fecha cierta o estimada de la ocurrencia de la

vulneración, su naturaleza, los datos personales afectados, y los posibles impactos generados.

También debe ser comunicado en un lenguaje claro y sencillo a los titulares de los datos que hayan sufrido una afectación significativa en sus derechos.

Las medidas adoptadas deben ser documentadas, revisadas periódicamente y evaluadas en su efectividad.

Contenido mínimo de la documentación de las medidas

La documentación de las medidas deberá contener, como mínimo:

- la forma, medios y finalidad del tratamiento,
- los procedimientos orientados a dar cumplimiento a las normas de protección de datos,
- la planificación de mecanismos para responder a vulneraciones de seguridad, y
- el rol del delegado de protección de datos cuando corresponda.

Esta documentación deberá estar disponible ante la solicitud efectuada por la Unidad Reguladora y de Control de Datos Personales.

En forma previa al inicio del tratamiento, el responsable y el encargado del tratamiento en su caso, deberán realizar una evaluación de impacto en la protección de datos personales. Si el tratamiento ya se había iniciado, el responsable y el encargado en su caso, deberán realizar esta evaluación en un plazo de 1 año a contar de la publicación de la norma reglamentaria en el Diario Oficial **(Fecha de publicación en el DO: 21/02/2020)**.

Si de la evaluación surge un riesgo potencial y significativo para los derechos de los titulares de los datos se debe dar aviso a la URCDP, estableciendo cuales son las medidas a adoptar y en que plazo.

Delegado de protección de datos personales

La Ley 19.670 establece la designación de un delegado, que es aquella persona que tiene como funciones asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales, supervisar el cumplimiento de la normativa sobre dicha protección en su entidad, proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en la materia.

Quienes deben designar un delegado de protección de datos personales son:

- las Entidades Públicas, estatales o no estatales,
- las privadas total o parcialmente de propiedad estatal,
- las Entidades Privadas que traten datos sensibles como negocio principal,
- las que realicen tratamiento de grandes volúmenes de datos, más de 35.000 personas.

El delegado puede ser un dependiente de la empresa o también la empresa puede contratar a alguien externo, debe contar con conocimientos en Derecho, especializados en materia de protección de datos personales, los que deberán acreditarse y debe guardar absoluta confidencialidad sobre los datos a los cuales tiene acceso debido a su condición de tal ya que para el desempeño de sus tareas se le debe brindar pleno acceso a las bases de datos personales y a las operaciones de tratamiento.

Actuará con autonomía técnica y no recibirá instrucciones en el desempeño de sus funciones específicas como delegado de protección de datos.

En un plazo de 90 días debe ser comuncado a la URCDP el nombramiento del delegado al igual que el cese o renuncia de este si ocurriere.

Sanciones

La Unidad Reguladora y de Control de Datos Personales fijará criterios para el cumplimiento, auditoría y evaluación de las medidas establecidas en la Ley N° 18.331 de 11/08/008 y el presente decreto

Las sanciones pueden por incumplimiento son:

- Observación.
- Apercibimiento.
- Multa de hasta 500.000 UI (quinientas mil unidades indexadas).
- Suspensión de la base de datos respectiva por el plazo de cinco días.
- Clausura de la base de datos respectiva.

La sanción va a depender de la gravedad y reiteración de la falta cometida.