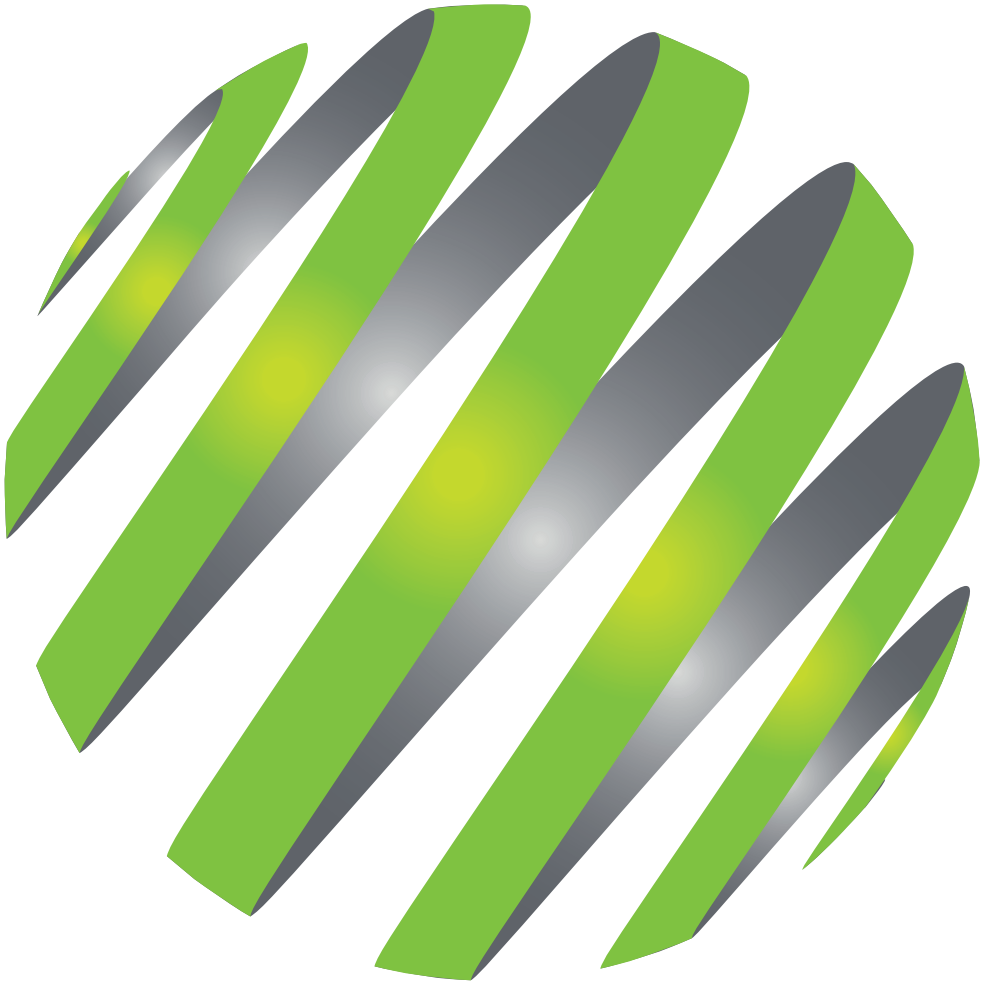
Deloitte.
Legal

Flash Legal Deloitte
Flash Legal 14 de Julio, 2020



Proyecto de Ley en materia de protección de datos personales

Con fecha 30 de junio de 2020 el Poder Ejecutivo remitió al Poder Legislativo un proyecto de ley, que tiene por finalidad aprobar el Protocolo de enmienda del Convenio para Protección de las Personas con Respecto al Tratamiento de Datos de Carácter Personal (el "Convenio Original"). Dicho protocolo modificativo del Convenio Original, fue suscrito el 10 de octubre de 2018.

Se trata de una norma que busca actualizar las disposiciones contenidas en el Convenio Original ante nuevas realidades y fortalecer la protección de datos personales. Asimismo, ratifica la adhesión de Uruguay al modelo de protección de datos personales seguido por los países europeos.

Antecedentes. Estándar Europeo.

El Convenio Original fue aprobado por la Ley 19.030 y contiene principios básicos en materia de protección de datos.

Tal como surge de la exposición de motivos del Poder Ejecutivo, "Con la entrada en vigencia de la mencionada Ley el primero de enero de 2013, Uruguay se convirtió en el primer país no europeo en ser parte del Convenio y su Protocolo Adicional. (...)"

Hoy día Uruguay cuenta con la Ley 18.331 en materia de protección de datos personales (la "LPDP"), la cual fue modificada recientemente por la Ley 19.670, con la finalidad de adecuarla, aún más, a los estándares de la

Unión Europea.

Por Decisión Nº 2012/484/EU, de fecha 21 de agosto de 2012, Uruguay cuenta con el estatus de país adecuado en los términos de la Comisión Europea.

De esta forma, podemos concluir que Uruguay ha seguido la tendencia de la Unión Europea, y es uno de los países de la región con mayor regulación en materia de protección de datos personales.

A través de la enmienda se amplía el objeto del Convenio Original, al aplicar al tratamiento de datos automáticos como no automáticos (el Convenio Original aplicaba solo al tratamiento de datos automáticos), e implica una obligación de los Estados adherentes de aplicar el Convenio al tratamiento de datos dentro de su jurisdicción en los sectores público y privado.

Como vimos, Uruguay ya ha avanzado en la aplicación de los principios recogidos en el Convenio Original y el Reglamento Europeo, por lo que en sustancia, la enmienda al Convenio Original no supone grandes novedades.

No obstante, es importante recordar cuáles son las principales directrices u obligaciones que impone la legislación uruguaya en materia de protección de datos personales, a todo aquel que trate datos personales (salvo las exclusiones establecidas por la LPDP). Al final del presente informe, analizaremos también las más recientes obligaciones en materia de protección de datos personales y que fueron reglamentadas por el Decreto 64/2020.

Principales obligaciones en materia de Protección de Datos Personales en nuestro país.

Típicamente, las empresas tratan, como mínimo, base de datos de empleados, proveedores y clientes. Así, respecto de esas bases, es necesario cumplir con las siguientes obligaciones:

- Las bases de datos deben estar registradas ante la Unidad Reguladora y de Control de Datos Personales ("URCDP"). Es importante destacar que no solo las bases de datos personales escritas deben registrarse, sino también las bases de datos de audio, video, etc., (como las grabaciones de video vigilancia).

- Los datos personales deben ser recolectados con el consentimiento libre, previo, expreso e informado del titular del dato (el que deberá, además, documentarse), salvo excepciones. En la obtención de tal consentimiento, es necesario que el responsable del tratamiento revele cierta información al titular del dato, lo que hace a la transparencia en el tratamiento. En ese sentido, la norma exige que se le informe al titular del dato: el uso (finalidad) que se le dará al dato, el nombre y dirección del responsable del tratamiento, los destinatarios de los datos, etc.

- El uso de los datos debe ser proporcional a los fines para los cuales se obtuvieron, y deben poder actualizarse.

- Los datos personales no deben ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

- Se deben adoptar medidas para garantizar la seguridad y confidencialidad de los datos personales.

- Se deben almacenar los datos de modo tal que permitan el ejercicio del derecho de acceso de su titular.

- Se deben utilizar los datos de forma reservada, estando prohibida toda difusión de la misma a terceros (salvo excepciones).

- Permitir el ejercicio de los derechos de acceso, rectificación, actualización, inclusión o supresión por parte del titular del dato.

- Los datos personales objeto de tratamiento sólo podrán ser comunicados a terceros para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

Ese consentimiento no es necesario en los casos establecidos en la LPDP y su decreto reglamentario.

Si la transferencia es al exterior, hay que considerar exigencias adicionales (ej.: contar con el consentimiento inequívoco del titular del dato para tal transferencia o que la misma se haga a un país considerado seguro desde el punto vista de la protección a los datos personales, entre otras consideraciones).

Adicionalmente, si el envío involucra datos protegidos por secreto bancario, hay que adoptar medidas adicionales, considerando la normativa bancocentralista.

Nuevas obligaciones.

A comienzos de año se emitió el Decreto 64/2020 (publicado el 21 de febrero de 2020 en el Diario Oficial) que reglamentó los arts. 37 a 40 de la Ley 19.670. A través de dichas normas se pasa a exigir a quienes traten datos personales, evidencia de las medidas adoptadas para cumplir con la LPDP, considerando el tipo de datos que se tratan, los tratamientos que se hacen, los riesgos asociados y los efectos de su materialización.

Esto implica contar con políticas y procedimientos documentados en materia de protección de datos personales y con el contenido indicado por la norma ("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.").

En algunos casos (cuando se manejen grandes volúmenes de datos, esto es, datos de más de 35.000 personas, o datos sensibles; se aplique analítica predictiva; o se envíen datos a países que no cumplan con los estándares requeridos por la URCDP en materia de protección de datos personales, entre otros), se debe realizar una evaluación de impacto en la protección de datos personales. Dicha evaluación tiene como principal objeto identificar los riesgos a los que se exponen los datos personales durante el tratamiento, con la finalidad de establecer controles que tiendan a mitigarlos o eliminarlos; siendo la finalidad última, cumplir con la LPDP.

El decreto establece el plazo de 1 año a contar de la publicación del mismo en el Diario Oficial (esto es, a partir del 21 de febrero de 2020) para que lo sujetos obligados realicen las respectivas evaluaciones de impacto.

Algo similar ya se exige a las entidades supervisadas por el BCU cuando procesan datos de sus clientes a través de terceros.

También se reglamentan otros deberes como la privacidad por diseño o la privacidad por defecto, lo que implica adoptar una serie de medidas organizativas (capacitación, sensibilización, etc.) y a nivel de sistemas o aplicativos (medidas técnicas como disociación de datos, encriptado, etc.).

Para ciertos casos (entidades públicas o de propiedad estatal; o entidades privadas que traten datos sensibles o manejen datos de más de 35.000 personas) se exige a las empresas contar con un delegado de protección de datos personales, que será la persona que vele por el cumplimiento de la LPDP. Dicha persona puede ser dependiente de la empresa o tercerizada, física o jurídica; siendo en todo caso necesario que cuente con competencias en derecho y en particular, sobre derecho a la protección de datos personales. Se otorgó un plazo de 90 días a contar de la publicación del decreto en el Diario Oficial para que las entidades obligadas a tener un delegado de protección de datos personales, lo designaran y comunicaran a la URCDP.

En materia de seguridad de los datos, los responsables o encargados de tratamiento deben velar por que tales datos cumplan los requerimientos de integridad, disponibilidad y confidencialidad. Esos estándares tampoco son nuevos en materia de seguridad de la información. La novedad es que ante cualquier vulneración a la seguridad de los datos, responsables y encargados de tratamiento deberán iniciar procedimientos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de conocido el incidente, asimismo deberá ser comunicado a la URCDP en un plazo máximo de 72 horas de conocida la vulneración, con los riesgos reputacionales que ello podría aparejar.

Para algunas licencias financieras, ese tipo de evento también debe ser reportado al BCU.

Contactos

Dr. Javier Domínguez
Gerente de Deloitte Legal
javdominguez@deloitte.com

Dra. María José Graziani
Abogada de Deloitte Legal
mgraziani@deloitte.com