ECIJA | La Concepción 191, Providencia,
Santiago de Chile · Tel: +56 2 25738521
www.ecija.com

NOTA INFORMATIVA - Aplicación en Chile del RGPD

¿Cuándo tiene mi empresa que cumplir con la normativa europea?

El ecosistema de la privacidad vive desde el 25 de mayo de 2018 el mayor cambio normativo de su historia en la Unión Europea, tras la plena aplicación del Reglamento General de Protección de Datos (RGPD). El alcance de esta norma, de vital importancia, traspasa las fronteras del continente europeo, **obligando a las empresas situadas fuera del mismo y que presten servicios a empresas o personas que se encuentren en la Unión Europea.**

Estos aspectos adquieren una mayor relevancia en los casos en que se presten servicios a empresas europeas, donde la industria chilena deberá garantizar aspectos relacionados con el ámbito legal, organizativo y de seguridad, máxime teniendo en cuenta que estos factores pueden ser decisivos en la contratación final.

En caso de incumplimiento de dicha normativa, se podrán imponer **sanciones económicas** importantes, **que pueden llegar hasta los 20 millones de euros (aproximadamente 14.763.200.000 de pesos chilenos) o el 4% de la facturación global de las empresas.**

Estos aspectos coinciden con el reconocimiento del derecho a la protección de datos constitucionalmente y la tramitación del proyecto de ley de modificación de la actual normativa chilena en la materia, cuestiones que ponen de manifiesto la necesidad de adaptar procesos, tratamientos y servicios a un sistema garantista y respetuoso con la privacidad.

En este sentido cabe recordar la reforma constitucional mediante la que se modifica el numeral 4, del artículo 19, en el siguiente sentido: "El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

En paralelo, deben tenerse en cuenta los movimientos normativos que se están produciendo en la región, donde **determinados países ya han anunciado sus modificaciones normativas** (como los casos de Argentina y Uruguay), la adaptación de sus actuales normas (como es el caso de México) o la tramitación de nuevas normativas (como es el caso de Ecuador), así como las propias recomendaciones de la Organización de Estados Americanos, enfocadas hacia una ley marco y estándares en materia de privacidad y protección de datos.

Así las cosas, una empresa tendrá la obligación de adaptarse a las exigencias del RGPD cuando oferte servicios o bienes a personas que se encuentren en la Unión Europea o presten servicios a empresas o responsables de tratamientos obligadas por el RGPD.

Prestaciones de servicios a empresas obligadas por el RGPD: una de las principales cuestiones que incluye la nueva norma europea hace referencia a las diligencias que deben adoptarse a la hora de contratar prestaciones de servicios con terceros. Estos proveedores, que actúan como encargados de tratamiento, tal y como les denomina la normativa, deben garantizar cuestiones en relación con la seguridad de los datos, los estándares aplicados, la obligación de comunicar las brechas de seguridad que puedan producirse, aportar garantías desde la óptica legal, así como los compromisos de sus equipos en relación con las responsabilidades que puedan generarse del tratamiento de datos persoanles.

Cumplimento de obligaciones legales: en determinados casos las empresas pueden verse sujetas a realizar tratamientos o comunicaciones de datos en aquellas situaciones en las que sean obligadas por ley o sean requeridos por jueces y tribunales.

Interés legítimo: existen supuestos en los que la ponderación de derechos, de empresa y ciudadanos, pueden conllevar los tratamientos de los datos en base a este concepto, aspectos que podrían darse en tratamientos como la videovigilancia o, en casos tasados, para el envío de comunicaciones comerciales.

Protección de intereses vitales de la persona: estaríamos aquí ante el tratamiento de datos personales en un contexto de emergencia humanitaria, como sería el caso de un terremoto o aspectos sanitarios, en los que por la gravedad de la situación se hace inviable la obtención del consentimiento analizado.

Es importante recordar que, en tanto los tratamientos que realizan para estas empresas europeas, se puedan realizar en territorio chileno, podrían conllevar una **transferencia internacional de datos,** aspectos de los que deberemos que informar en el momento de la contratación y suscribir las correspondientes adendas.

Sobre el impacto de otras obligaciones específicas de la nueva norma europea, podemos resaltar:

Obligación de comunicar una brecha de seguridad

En caso de que se produzca una brecha de seguridad, se debe notificar a la autoridad de control en un plazo máximo de 72 horas, por lo que deberán llevarse a cabo análisis sobre los subcontratistas, medidas de seguridad o espacios cloud con los trabajamos, de cara a tener la información, cuasi en tiempo real de cara a cumplir con los plazos, en los que estemos obligados a ello, o debamos de facilitárselo a nuestros clientes. En todo caso, esta obligación de notificar brechas de seguridad puede ser doble, en tanto deberemos informar a la autoridad de control y, en determinados casos, a los propios usuarios, si no hemos adoptado medidas como el cifrado o la brecha afecta a información especialmente protegida.

Obligación de realizar una Evaluación de Impacto

Será necesario llevar a cabo una Evaluación de Impacto (PIA, por sus siglas en inglés) cuando el tipo de tratamiento implique, por su naturaleza, un alto riesgo para los derechos y libertades de las personas naturales. Esta obligación afectaría por ejemplo al tratamiento de datos especialmente sensibles (raza, salud, religión, orientación sexual, antecedentes penales, etc); elaboración de perfiles y/o segmentación (página web que analiza a través de cookies el comportamiento de un usuario que esté en la UE para luego proporcionarle publicidad personalizada); o la monitorización sistemática de usuarios (aplicación de móvil que geolocaliza a usuarios que se encuentren en la UE). En todo caso, debemos tener en cuenta que estas evaluaciones de impacto, no sólo incluyen la evaluación de aspectos técnicos o de seguridad, si no de otras facetas del tratamiento, como impacto en las personas, aspectos jurídicos, planificación de marketing, intervención de terceros, licitud de los tratamientos, entre otros.

Obligación de designación de un representante en la Unión Europea

En determinados casos, atendiendo a las tipologías de tratamientos que se realicen, propios o por cuenta de terceros, las empresas deberán nombrar a un representante para que actúe en la UE, cuando traten datos personales de forma habitual, o cuando haciéndolo de manera esporádica sean datos especialmente sensibles. El representante podrá establecerse en cualquiera de los países de la Unión Europea en donde se encuentren los interesados y cuyos datos personales sean tratados. Se encargará fundamentalmente de atender las solicitudes de las Autoridades de Control y de los propios interesados.

Obligación de adoptar la privacidad desde el diseño y la privacidad por defecto

Quizás el cambio más novedoso, parte de la concepción de la nueva norma de la privacidad como eje de los tratamientos, el análisis de los riesgos y la mayoría de edad de las empresas para tratar datos personales, aspectos, todos ellos, que tienen un mayor impacto en una sociedad globalizada donde internet es el medio de comunicación y trabajo, y el avance las nuevas tecnologías influyen de manera absoluta en las relaciones empresariales y la generación de nuevos modelos de negocio.

En este sentido, ambos principios parte de las premisas de proteger los datos personales desde el momento inicial en que una empresa planifica cualquier desarrollo tecnológico que implique el tratamiento de datos. En este supuesto estaría incluido el desarrollo de una web de comercio electrónico, o la creación de una app, y se deberán tratar los datos imprescindibles, garantizando de tal forma que sólo serán objeto de tratamiento aquellos datos que sean necesarios para cumplir con los fines específicos para los cuales se recogieron.

Desde ECIJA, gracias al liderazgo en el sector jurídico en estas materias y su presencia internacional, estamos ayudando a las empresas a cumplir con las nuevas exigencias legales, mediante la adopción de sistemas que garanticen el cumplimiento y capacidad de acreditarlo y que sean conciliables con el avance tecnológico y el desarrollo de negocio

Para más información:

Javier Sabido
Abogado – Socio
jsabido@ecija.com

Franz Ruz
Abogado - Socio
fruz@ecija.com
www.ecija.com