Intuita
Consultores Jurídicos

Intuita Consultores Jurídicos

Una visión de la nueva Ley de Protección de Datos Personales desde el COMPLIANCE

Enero de 2019

Con esta nota los profesionales de nuestro despacho hemos querido aportar nuestra particular visión de la nueva Ley de protección de datos de carácter personal, aprobada mediante Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, desde el punto de vista del compliance, siendo así que constituye un interesante artículo para profesionales del Sector y para administradores y directivos de cualquier empresa.

Novedades en el ejercicio del derecho de acceso a datos.

A modo de canal de denuncias de los que utilizamos los profesionales en implantaciones de sistemas de prevención de delitos (compliance) –pues no olvidemos que la protección de datos sirve como base a determinadas conductas ilícitas de los tipos penales de descubrimiento y revelación de secretos, suplantación de identidad o daños informáticos –, la nueva norma permite la utilización de canales de protección de datos personales a través de los cuales el responsable cumpla de manera directa, fácil, segura y continua con su obligación respecto del acceso a datos por sus legítimos titulares, mediante una sencilla implementación de un canal directo en su sitio web a través de cuyo acceso los usuarios podrán consultar los datos que están siendo sometidos a tratamiento por parte del responsable de los mismos.

Y, también en relación con el ejercicio del derecho de acceso a datos personales, merece la pena comentar que ejercitar este derecho por los interesados una segunda ocasión en menos de 6 meses permitirá al responsable no atender a esta solicitud, salvo que aquéllos acrediten la existencia de justa causa para este ejercicio reiterativo.

Operaciones de reestructuración societaria.

Una novedad importante y que afecta a uno de los servicios principales de nuestro despacho es la presunción que la norma establece respecto de la licitud de los tratamientos de datos derivados de cualquier operación de modificación en la estructura de sociedades, incluyendo aquéllos tratamientos de datos que con carácter previo fuera necesario realizar para garantizar el buen fin de la operación, como ocurre cuando nuestros profesionales acceden a determinados datos personales necesarios para prestar un servicio de auditoría legal (conocidos como procesos de Due Diligence) en operaciones mercantiles llevadas a cabo por nuestros clientes.

Debemos precisar que para estos supuestos de estudios, auditorías y otras operaciones precontractuales (cartas de intenciones, promesas de compra o venta, acuerdos de confidencialidad, contratos de colaboración, etc) habremos de cumplir también con la obligación se supresión de datos para el supuesto de que finalmente la operación no llegara a concluirse.

Sistemas de denuncias internas

Con esta terminología, la nueva norma viene a utilizar también los clásicos canales de denuncia permitir a las empresas responsables de datos personales que establezcan sistemas anónimos de denuncias a través de los cuales cualquier tercero tenga la posibilidad fácilmente accesible de denunciar una vulneración de la normativa general o sectorial aplicable.

Los empleados y terceros deberán ser informados respecto de la existencia y puesta a su disposición de estos canales de denuncia, de manera que no sólo deben entenderse como una herramienta a su disposición sino también como una obligación exigible para los mismos.

Especial cuidado habremos de mostrar para limitar el acceso a los datos exclusivamente a quienes, dentro de la empresa o de forma externalizada, desarrollen las denominadas funciones de control interno y de cumplimiento, en clara referencia al Compliance Officer, o a los encargados del tratamiento que eventualmente se designen a tal efecto, como pueden ser los delegados de protección de datos (DPD), pero también cualquier otro que asuma el rol de encargado de tratamiento conforme a la prestación de servicios en cuestión. No obstante, deben quedar a salvo de este acceso otras personas, incluyendo la posibilidad de su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o en sede de procedimientos judiciales, cuando proceda.

Vemos una y otra vez las continuas referencias al compliance en esta nueva norma, en la referencia directa al encargado de cumplimiento normativo (Compliance Officer), a los canales de denuncia de ilícitos en general, a la necesaria exigencia y formación a empleados y terceros proveedores o a la adopción de medidas disciplinarias.

Muy importante también es el plazo durante el que podremos conservar los datos tanto de la persona que formula la denuncia como los de los empleados o terceros que puedan verse afectados por la información denunciada y puesta en conocimiento de la empresa, pues este debe limitarse al necesario para poder decidir sobre la iniciación de una investigación sobre los hechos denunciados, con un máximo de 3 meses desde que se comunicaron a través del canal de denucias. A partir de ese momento los datos deben ser borrados del sistema de denuncias, quedando exclusivamente bajo el conocimiento y la utilización del Órgano de cumplimiento.

La contratación de encargados de tratamiento

En nuestro despacho estamos desgraciadamente acostumbrados a que administradores, gerentes y directores nos aseveren que todas aquéllas responsabilidades que habitualmente son delegadas o encomendadas a otros dejan de resultarles exigibles, siendo esta una creencia completamente infundada y exenta de argumentación jurídica para tratar de soportar en el futuro una defensa de la posición de un cliente en juicio.

Valga como ejemplo, precisamente, lo establecido en esta norma sobre protección de datos en cuanto a las obligaciones que le son exigibles a cualquier responsable de datos personales a la hora de contratar a un encargado para que este lleve a cabo algún tratamiento de datos personales, pues el RGPD obliga al responsable a elegir únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

Esto significa que cualquier empresa que tenga la consideración de responsable sobre determinados datos personales, que venimos a ser todas las empresas que intervenimos en el Mercado, tiene la obligación de asegurarse de que el encargado con el que pretendemos contratar una prestación de servicios que implica de forma directa o indirecta o consecuencial el tratamiento de datos respecto de los que nosotros tenemos la condición de responsables, cumple con las obligaciones que le son exigibles como encargado, lo que pasa por exigirles con carácter previo a contratar con ellos que nos acrediten su diligencia y las medidas con las que cuentan.

Es decir, si contratamos a un encargado de tratamiento, cualquiera que sea su prestación de servicios a nuestra empresa, sin habernos asegurado previamente de que cumple con estas medidas, cualquier responsabilidad derivada de ese tratamiento nos será directamente exigible a nosotros como responsables, como si hubiéramos sido directamente nosotros los culpables del ilícito cometido.

En la mayoría de los casos, esto puede ser tan sencillo como solicitar al eventual encargado de tratamiento que nos acredite el cumplimiento de estas medidas, para lo cual nada mejor que contar con profesionales del Derecho especializados en la materia que lleven a cabo esta pequeña auditoría previa a la contratación de una prestación de servicios que implique tratamiento de datos por parte de terceros.

Contratos con encargados de tratamiento previos a la entrada en vigor del RGPD.

Un detalle por parte del Legislador debe considerarse el haber incluido una Disposición Transitoria Quinta para asegurar la vigencia de los contratos de encargado de tratamiento suscritos con anterioridad al 25 de mayo de 2018 hasta la fecha de vencimiento señalada en los mismos, y hasta el año 2022 si tenían duración indefinida.

"nada mejor que contar con profesionales del Derecho especializados en la materia que lleven a cabo esta pequeña auditoría previa a la contratación de una prestación de servicios que implique tratamiento de datos por parte de terceros"

Ello no obstante, habremos de asegurarnos de que el contrato suscrito con anterioridad a la entrada en vigor del RGPD cumple suficientemente en su redacción y contenido con los requisitos de seguridad y protección de los datos personales de terceros, pues en otro caso estaremos expuestos a riesgos imprevisibles e inciertos.

No obstante, permitiéndolo la norma expresamente, desde INTUITA CONSULTORES JURÍDICOS recomendamos exigir a todos nuestros encargados la modificación y adaptación de sus contratos a fin de que resulten conformes a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de la nueva norma nacional.

El Delegado de Protección de Datos.

Por fin, se potencia esta figura trascendental en el presente y futuro próximo de muchas empresas, regulándose aspectos básicos como los supuestos en los que resulta obligatoria la designación de un DPD o la cualificación de la que debe disponer y sus funciones.

Entre estos sujetos que, por regulación expresa de la norma, deben contar con un DPD, destacamos los siguientes:

- ✓ Los colegios profesionales y sus consejos generales.
- ✓ Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación
- ✓ Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

En cuanto a la cualificación profesional que debe reunir un DPD, debe destacarse que el artículo 35 de la norma española exige que cuenten con conocimientos especializados en Derecho y con la necesaria práctica en materia de protección de datos, debiendo poder acreditarse como no puede ser de otra forma.

Vuelve este a constituir un ejemplo de la diligencia debida por parte del empresario en la contratación de un DPD para su empresa, o en la atribución de las facultades y competencias propias del cargo en alguien que ya forme parte de la plantilla.

Como consecuencia de esta especialización en Derecho y conocimiento jurídico que requiere la normativa, se otorga al DPO un papel particularmente relevante en caso de que se formule por parte de cualquier particular una reclamación ante la Agencia Española de Protección de Datos (AEPD) en contra de nuestra empresa, estando previsto que la propia AEPD pueda dirigirse directamente al DPO para su análisis y posterior remisión a la autoridad de control de las medidas adoptadas en relación con los hechos descritos en la reclamación, todo ello antes de iniciar un procedimiento contra nuestra empresa, como responsable de los datos, o el propio encargado, en su caso.

Para concluir, no debemos olvidar que la nueva normativa también se refiere a los derechos digitales, con especial relevancia para el empresario en cuanto a determinados derechos que se reconocen a los empleados, tales como la conocida desconexión digital. Estos aspectos serán tratados en un artículo independiente por nuestros profesionales.

Intuita

Consultores Jurídicos

Intuita Consultores Jurídicos

www.intuita.es