

HAY QUE ADAPTAR MODELOS PROACTIVOS BASADOS EN LA PREVENCIÓN

# Retos y oportunidades en materia de protección de datos para 2017



## MARIA SUÁREZ PLIEGO

Socia y Responsable del Área de Tecnología y Privacidad de Suárez de la Dehesa Abogados

**D**urante el año 2016 se han producido importantes novedades legislativas en materia de protección de datos que afectarán a la transformación digital de las empresas en las que el 'Dato' y el data governance cobran un valor importantísimo, teniendo que evaluar las políticas de protección de datos implantadas para adaptarlas a la nueva regulación.

Las principales novedades se centran en el Paquete Europeo de Protección de Datos que entró en vigor en mayo de 2016, compuesto por el Reglamento Europeo de Protección de Datos (RGPD)<sup>i</sup> y la Directiva sobre transmisión de datos en el ámbito policial y judicial<sup>ii</sup>, y en el nuevo marco para las transferencias internacionales de datos.

acreditar el cumplimiento de las obligaciones establecidas en el RGPD; o los principios de 'Privacy by design y Privacy by default', que consisten en la adopción de políticas internas y otras medidas para que desde el diseño y/o por defecto se cumplan las obligaciones en materia de protección de datos.

- Inclusión de nuevos derechos de los interesados: el Derecho de supresión o 'el derecho al olvido', o el Derecho a la portabilidad de los datos a otro Responsable del tratamiento; lo que implicará la revisión de los procedimientos establecidos para garantizar el ejercicio de los Derechos ARCO.

- Introducción de nuevas obligaciones para los Responsables del tratamiento entre las que destacan: (1) la realización de una evaluación de impacto, que evalúe el riesgo inherente al tratamiento y determine las medidas apropiadas para mitigarlo; (2) el nombramiento de un delegado de Protección de Datos o DPO (por sus siglas en inglés) con capacidad para tomar decisiones, autónomo e independiente; o (3) la necesidad de que los Estados miembros establezcan mecanismos que garanticen la compensación de los daños y perjuicios derivados de las vulneraciones en esta materia; lo que implicará la necesidad de incluir la protección de datos en los nuevos desarrollos de negocio.

- Reforzamiento del principio de seguridad de la información, al establecerse como obligación notificar en un plazo de 72 horas las brechas de seguridad a la Autoridad de Control, a los interesados y demás agentes intervinientes en el tratamiento de los datos y, en lo que respecta a las medidas de seguridad, a adoptar la novedad que introduce el Reglamento en relación con las establecidas en el Real Decreto 1720/2007, consistente en la necesidad de realizar con carácter previo a establecer cuáles son las medidas técnicas y organizativas que deben establecerse en materia de seguridad de la información, un análisis de los riesgos inherentes al tratamiento de datos; lo que implicará evaluar los riesgos y analizar si las medidas de seguridad implantadas son las adecuadas.

## Reglamento Europeo de Protección de Datos

En relación al Reglamento Europeo de Protección de Datos (en adelante, RGPD), que será aplicable a partir del próximo 25 de mayo de 2018, en escasos dos años, las empresas tendrán que revisar sus políticas de protección de datos y de seguridad de la información, así como sus procesos, para adaptarse a las nuevas exigencias, so pena de multas administrativas superiores a las que nos enfrentábamos hasta ahora (pasando de los 600.000 euros como máximo a los 20 millones de euros o, tratándose de una empresa, a una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior).

## ¿Cuáles son los principales cambios?

- Reforzamiento de los principios de los que derivan las obligaciones en materia de protección de datos. El principio de información introduce nuevos aspectos de los que deberá ser informado el interesado previamente al tratamiento de sus datos; o el principio de consentimiento, que deberá solicitarse de forma expresa y separada respecto de cada una de las finalidades, no siendo posible recabarlos de manera tácita ni de forma global y general.

- Introducción de nuevos principios, como el de 'accountability', consistente en la necesidad de



## MIREIA PARICIO ZARAGOZA

Abogada de Suárez de la Dehesa Abogados

## Directiva sobre transmisión de datos personales entre los Estados Miembros en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial

Esta Directiva, cuyo plazo máximo de transposición es el 6 de mayo de 2018, asegurará un nivel uniforme de protección de la privacidad de víctimas, acusados, testigos y demás personas implicadas en la prevención, investigación o enjuiciamiento de infracciones penales, o de la ejecución de las correspondientes sanciones penales, fortaleciendo los derechos de los interesados, así como las obligaciones y los límites de las autoridades competentes cuando traten datos de carácter personal con los precitados fines.

De esta normativa destacamos la obligación de cumplir con el derecho de información de los interesados a los que deberá informarse sobre los riesgos, reglas, salvaguardias y derechos aplicables en relación con el tratamiento de sus datos personales, así como del modo de hacer valer sus derechos de acceso, rectificación, supresión y limitación de su tratamiento.

## Transferencias internacionales a EEUU

Otra normativa que merece especial mención es la Decisión de la Comisión Europea, de 12 de julio de 2016, por la que se aprueba el nuevo acuerdo denominado Escudo de privacidad o 'Privacy Shield' entre los EEUU y la Unión Europea<sup>iii</sup> para la transferencia internacional de datos al otro lado del Atlántico, tras haberse anulado la Decisión Safe Harbour (o Puerto Seguro) por el TJUE en fecha 6 de octubre de 2015 (Asunto C-362/14).

Con ello, las empresas españolas (y europeas) tienen un nuevo mecanismo para la transferencia de los datos personales de cuyo tratamiento son responsables a un importador situado en los Estados Unidos, además de poder utilizar como mecanismos adicionales las cláusulas contractuales tipo o cláusulas ad hoc o la adopción de Reglas Corporativas Vinculantes o 'Binding Corporate Rules' (BCR) por un grupo multinacional de empresas, las cuales garantizan el nivel adecuado de protección de los derechos de los interesados.

Esta Decisión consiste en un sistema de auto-certificación, por el que las firmas estadounidenses interesadas se adhieren al Escudo de Privacidad UE-EEUU, comprometiéndose a cumplir los Principios de Privacidad establecidos para proteger los datos de los ciudadanos europeos.

Las principales novedades que incorpora el Escudo de Privacidad UE-EEUU, respecto al invalidado Puerto Seguro, son:

- Fortalecimiento de los principios de privacidad e incremento de la transparencia de las políticas de privacidad de las empresas autocertificadas.
- Mayor seguimiento y control por parte del Departamento de Comercio de EEUU y la Comisión Federal de Comercio (FTC), que velarán porque las empresas estadounidenses autocertificadas cumplen los principios del nuevo marco, so pena de ser sancionadas y eliminadas de la lista del Escudo de la privacidad, teniendo que devolver o suprimir los datos personales que hayan obtenido en el marco de dicho régimen.
- Obligación de las empresas de facilitar mecanismos de resolución de las reclamaciones de los ciudadanos, rápidos y gratuitos, de manera que los particulares puedan presentar una reclamación directamente a la organización estadounidense autocertificada, a un órgano independiente de solución de conflictos designado por la organización o a las autoridades nacionales de protección de datos.
- Garantiza que las posibles injerencias indiscriminadas basadas en situaciones excepcionales de seguridad nacional se limiten a lo estrictamente necesario y proporcionado.

## Conclusión

A la vista de estas novedades, y teniendo en cuenta los principales retos a los que se enfrentan las empresas como la digitalización para el tratamiento masivo de datos o Big Data, los nuevos tipos de tratamiento de datos que permiten las nuevas tecnologías (por ejemplo la geolocalización a través del smartphone o el análisis de la salud con aplicaciones específicas), los riesgos que ello conlleva desde el punto de vista de la privacidad, o del carácter global de las Tecnologías de la Información, hoy nos enfrentamos a un nuevo panorama al que debemos adaptarnos con modelos proactivos basados en la prevención, dejando atrás los viejos modelos de cumplimiento.

En este nuevo marco, a nivel regulatorio, el principal reto que las organizaciones asumirán será la adaptación al nuevo RGPD que implicará la obligación de revisar y adaptar sus políticas de protección de datos, así como las de seguridad de la información, siendo preciso colaborar con expertos en la materia. Muestra de ello es la publicación por el Grupo de Autoridades Europeas de tres guías sobre la adaptación al RGPD, relativas al derecho a la portabilidad de los datos, a la figura del delegado de Protección de Datos y a los criterios para identificar la autoridad de control principal. ■

## NOTAS

i REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

ii DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

iii DECISIÓN DE EJECUCIÓN (UE) 2016/1250 DE LA COMISIÓN de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EEUU