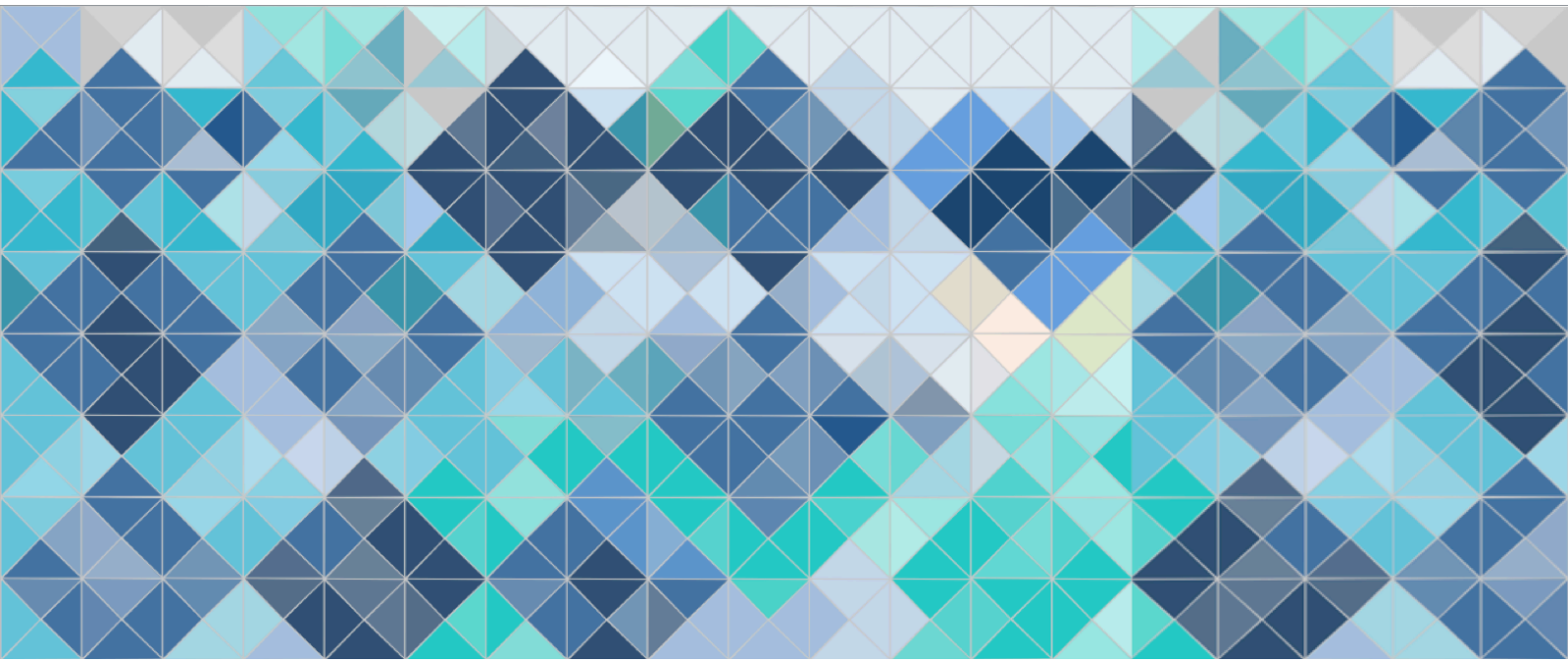
Novedades Reglamento UE Protección de datos

Resumen de la ponencia de Ramón Miralles
Junio 2014



Diagonal 640 1C - 08017 BARCELONA 934940748 http://ribasyasociados.com

ribasyasociados

TABLA DE **CONTENIDOS**

ANTECEDENTES - **INTRODUCCIÓN**

En junio de 2014 el despacho de abogados RIBAS Y ASOCIADOS organizó un ciclo de desayunos de trabajo en los que RAMÓN MIRALLES, Coordinador de Auditoría y Seguridad de la información en la Autoridad Catalana de Protección de Datos, expuso las novedades de la propuesta de Reglamento UE de Protección de Datos y anticipó los puntos que probablemente formarán parte de la nueva norma.

Agradecemos a Ramón Miralles su participación como ponente en este ciclo de reuniones de trabajo y sus aportaciones en el posterior debate, que fue muy enriquecedor para los asistentes.

En este documento se resumen los principales puntos de su ponencia.

ORIGEN Y **PROCEDIMIENTO LEGISLATIVO ORDINARIO**

25 DE ENERO DE 2012

La Comisión Europea presenta una propuesta legislativa dirigida a reformar el marco jurídico del derecho a la protección de datos en Europa, con la finalidad de actualizar las previsiones de la vigente Directiva 45/96 CE sobre protección de datos, adecuando la regulación especialmente a los avances y usos tecnológicos ocurridos durante los últimos años (ej. big data, cloud computing, redes sociales, smartphones, etc.).

12 DE MARZO DE 2014

El Parlamento examina la propuesta de la Comisión (en primera lectura) y aprueba una serie de enmiendas, dando lugar así a la postura del Parlamento respecto de la regulación propuesta; la votación fue favorable por una amplia mayoría (621 votos a favor, 10 en contra y 22 abstenciones), por lo que puede considerarse que el Reglamento ya no es un proyecto de futuro sino una realidad próxima que debería materializarse con su aprobación definitiva a finales de 2014 o, como máximo, a principios de 2015.

PRÓXIMOS **PASOS**

En una tercera fase la propuesta llega al Consejo Europeo (con representación de cada Estado miembro) para su primera lectura, y podrá aceptar la posición del Parlamento, quedando adoptado el acto legislativo, o por el contrario enmendar la propuesta, en cuyo caso sería devuelta al Parlamento para una segunda lectura.

Una vez aprobado, el Reglamento será de aplicación directa, en todos los estados de la Unión Europea a los 2 años desde su fecha de entrada en vigor (vigésimo día siguiente al de su publicación en el Diario Oficial de la Unión Europea)

Este Reglamento está considerado por las instituciones europeas como uno de los pilares del mercado único digital europeo, que debería estar ultimado, al menos conceptualmente, en el 2015.

ÁMBITO DE **APLICACIÓN**

El Reglamento será de aplicación directa a todos los Estados miembros.

Todas las empresas que traten datos de carácter personal y dispongan de un establecimiento en un Estado miembro deberán aplicarlo, aunque las operaciones materiales de tratamiento de la información se lleven a cabo fuera de la Unión Europea.

Del mismo modo, las empresas no establecidas en Europa se verán obligadas a adecuarse a dicho Reglamento cuando su oferta de bienes y servicios vaya dirigida a personas residentes en la UE.

OBJETIVO DEL REGLAMENTO

El objetivo del Reglamento es alcanzar un mayor nivel de protección de los datos de carácter personal, especialmente en el medio digital, alineando la gestión de la protección de datos con el resto de actividades ordinarias y cotidianas que conforman la estructura organizativa y las reglas de negocio de las empresas, a lo que se une la obligación de ofrecer una mayor transparencia respecto del tratamiento de datos que llevan a cabo, en base a informar más y mejor sobre las operaciones de tratamiento.

Se reduce la carga formal y burocrática en pro de una gestión más ejecutiva y práctica.

PRINCIPIOS RECTORES

Los principios rectores de la protección de datos previstos en la vigente normativa de protección de datos se mantienen (ej. proporcionalidad, seguridad, calidad, minimización, etc.) pero se incluyen otros nuevos como el principio anglosajón "*accountability*" o "rendición de cuentas", que se refiere a que el responsable del tratamiento deberá garantizar y ser capaz de acreditar de forma previa y recurrente que cumple con las disposiciones recogidas en el Reglamento.

Este Reglamento incluye la previsión de mecanismos de coherencia. El objetivo es crear un cuerpo normativo común para los países de la UE, que además deba ser aplicado de forma armonizada por todas las Autoridades de Control existentes.

Sin perjuicio de lo anterior, como su propio redactado indica, el Reglamento es un cuerpo normativo de mínimos por lo que sectorialmente, a través de las propias Autoridades de Control o instituciones europeas, podrá producirse una ampliación de su contenido y regulación en aspectos eminentemente operativos.

LA FIGURA DEL DPO - DELEGADO DE PROTECCIÓN DE DATOS

SUPUESTOS EN LOS QUE SERÁ OBLIGATORIO TENER UN DPO

La propuesta de Reglamento determina la obligatoriedad del DPO en los siguientes casos:

- Tratamiento de datos de más de 5.000 personas durante 12 meses consecutivos
- Tratamiento de categorías especiales de datos (ej. hospitales)
- Tratamiento de datos de localización (ej. geolocalización);
- Tratamiento que consista en la monitorización del interesado (ej. navegación);
- Tratamiento de datos de menores y empleados a gran escala
- Administraciones Públicas.

RÉGIMEN QUE SE APLICARÁ AL DPO

- El DPO será el punto de enlace entre la Autoridad de Control y el responsable o encargado tratamiento, aunque la responsabilidad por el incumplimiento de la normativa recaerá siempre sobre la empresa (responsable o encargado de tratamiento)
- El DPO podrá ser interno (el mandato mínimo será de 4 años) o externo (el mandato mínimo será de 2 años), y podrá representar a varias empresas simultáneamente. Además, no necesariamente deberá residir en Europa.
- En cualquier caso el DPO deberá contar con los recursos humanos y materiales necesarios para desarrollar sus funciones de forma adecuada.
- Ha de ser una persona física y su identidad y datos de contacto deberán ser comunicados a la Autoridad competente y al público en general.
- El cargo de DPO no reviste exclusividad por lo que el profesional podrá desarrollar otras funciones y competencias, siempre que le permitan garantizar los principios de independencia (no parece por tanto que esta función pueda ser asignada, por ejemplo, al Responsable de Seguridad) y deber de secreto que rigen su actividad.
- Deberá estar presente en la toma de decisiones sobre los procesos que vayan a implicar el tratamiento de datos personales, y disponer de una interlocución directa con la Dirección Ejecutiva, si bien no es necesario que pertenezca a ella.

PERFIL DEL DPO

El DPO ha de ser un profesional conocedor de la materia (legislación y buenas prácticas) y capacitado para desarrollar todas las funciones que describe el Reglamento (ej. supervisión, información, asesoramiento, formación, comunicación al Comité de empresa sobre el tratamiento de datos de los empleados, auditorías, seguridad, etc.), aunque por el momento no se detalla la obligación de acreditar una formación determinada.

No obstante, muy probablemente se establecerán mecanismos de acreditación, ya sean a nivel europeo o local, respecto de la formación o capacitación requerida.

DEBER DE INFORMACIÓN Y CONSENTIMIENTO

La información que sobre los tratamientos han de proporcionar los responsables a las personas afectadas, deberá ser más extensa, clara y comprensible.

Del mismo modo deberá incluirse en los avisos legales información sobre la identidad y datos de contacto del Delegado de Protección de Datos.

El tratamiento de datos llevado a cabo por un responsable o encargado deberá estar legitimado y únicamente lo estará:

- si el afectado ha prestado su consentimiento para ello
- si una ley así lo autoriza
- si hay un interés legítimo por parte del responsable o encargado en ese tratamiento concreto (debe ponderarse el interés del responsable en tratar los datos con el derecho del afectado a la protección de sus datos u otros derechos y libertades), o
- si hay un interés vital en el tratamiento de los datos (en caso de estar en riesgo la vida de los interesados).

En relación al consentimiento para el tratamiento de datos, el Reglamento no detalla unos requisitos concretos, limitándose a establecer que este consentimiento deberá ser informado y explícito. Además, como ocurre en la actualidad, la carga de la prueba recaerá siempre sobre el responsable o encargado del tratamiento.

ICONOS INFORMATIVOS NORMALIZADOS

El Parlamento ha propuesto normalizar las políticas de información a los afectados (como se hace en otros sectores como el alimenticio o el farmacéutico), a través de iconos visualmente informativos que deberán utilizar todos los responsables a los que pueda afectarles el Reglamento (ej. iconos para representar si el responsable cifra los datos, los trata con una finalidad distinta a la principal que motivo su recogida, o si los vende o alquila a terceros).

DERECHOS **ARCO**

Se mantienen los derechos de acceso, rectificación, cancelación y oposición pero se definen nuevas especialidades (ej. en el derecho de oposición se incluye la posible oposición a la elaboración de perfiles).

La mención específica al derecho al olvido que aparecía en el redactado inicial del Reglamento ha sido suprimida, pero su contenido y finalidad esencial se mantienen.

Lo mismo sucede con el derecho a la portabilidad cuya mención expresa desaparece pero su funcionalidad se mantiene, en base al derecho del interesado a la obtención de los datos. Se entiende como un derecho de acceso amplificado en el que el interesado, siempre que hubiera facilitado sus datos personales y estos se traten electrónicamente, puede exigir al responsable del tratamiento que se los proporcione en formato electrónico interoperable, para poder facilitárselos o transferirlos a un nuevo proveedor/ responsable, cuando sea técnicamente viable y materialmente posible.

CONTRATO DE **ENCARGADO DEL TRATAMIENTO**

El Reglamento establece la necesidad de formalizar a través de un contrato la relación jurídica con aquellos proveedores que traten datos personales por cuenta del responsable del tratamiento, estableciendo que en ese contrato podrán establecer libremente sus respectivos papeles y tareas en relación a los requisitos del Reglamento.

En la última versión del Reglamento se incluyen algunas de las cuestiones que deberá prever el contrato, tal y como ahora se establece un contenido mínimo para este tipo de contratos, regulado en el artículo 12 de la LOPD. Básicamente se mantienen los requisitos descritos en dicho artículo.

MEDIDAS DE **SEGURIDAD**

No se detallan los niveles ni las medidas de seguridad, pero se describen una serie de objetivos en el tratamiento de datos, tales como la integridad, disponibilidad, seguridad, reacción ante incidencias, planes de contingencia o control continuado.

Se trata de un modelo preventivo que pretende proteger no solo los datos personales objeto de tratamiento, sino los sistemas que los albergan y tratan.

Deben implantarse aquellas medidas técnicas y organizativas que se consideren necesarias a partir de la realización de un análisis de los riesgos inherentes al tratamiento de datos que quiera realizarse. En función del referido análisis deberán adoptarse las medidas de seguridad necesarias para minimizar el riesgo derivado del tratamiento de los datos.

Las auditorías sobre las medidas de seguridad se realizarán en función y con la periodicidad que marque el modelo de seguridad de la información adoptado.

Por otra parte, el responsable y el encargado del tratamiento, en determinadas circunstancias (ej. cuando del análisis de riesgos se derive esta necesidad, cuando se traten datos sensibles, cuando se traten datos de más de 5.000 personas, o en general, siempre que una empresa reúna los requisitos para disponer de un DPO), deberán realizar una evaluación del impacto que sobre la protección de datos tendrá el tratamiento que pretendan llevar a cabo (es uno de los instrumentos relacionados con el concepto anglosajón de *"privacy by design",* que junto con la privacidad por defecto han sido incorporados al Reglamento).

TIPOLOGÍAS DE DATOS

Al desaparecer los niveles, desaparecen las tipologías concretas de datos, limitándose el Reglamento a identificar las denominadas “categorías especiales de datos”. En éstas, además de los ya conocidos datos especialmente sensibles (ej. salud, vida sexual, creencias religiosas, etc.), se incluyen nuevas tipologías como los datos genéticos o biométricos.

Las medidas de seguridad a aplicar a este tipo de datos vendrán definidas por el análisis de riesgos realizado, que deberá tener en cuenta esa mayor sensibilidad de los datos, y en conciencia se identificarán unos requisitos de protección más exigentes respecto de otro tipo de datos.

FICHEROS Y DOCUMENTO DE SEGURIDAD

Con carácter general desaparece la obligación de notificar ficheros ante la Autoridad de Control, y de elaborar formalmente un Documento de Seguridad, si bien en la práctica los documentos en materia de seguridad deberán elaborarse en función del modelo de seguridad adoptado.

AUDITORÍA DE CONTROL DEL CUMPLIMIENTO NORMATIVO

Habrá una auditoría bienal obligatoria para todas las empresas que afectará a todo el conjunto de obligaciones relacionadas con la protección de datos, no sólo a las medidas de seguridad.

NOTIFICACIÓN DE INCIDENCIAS

Será obligatorio notificar “sin demora injustificada” a las Autoridades de Control las incidencias que puedan afectar a la seguridad de los datos (*data breach*), y con carácter general deberán comunicarse también a los afectados.

La obligación de comunicar la incidencia a los afectados puede quedar exceptuada si se acredita ante la Autoridad de Control que existen medidas de seguridad que garantizan la confidencialidad de los datos, y que por tanto el potencial impacto negativo sobre los datos ha sido neutralizado. Por ejemplo, ante la pérdida de un dispositivo si se acreditara que los datos afectados estaban cifrados.

No comunicar la incidencia a la Autoridad de Control podrá ser constitutivo de infracción por lo que sería sancionable.

SELLO EUROPEO DE PROTECCIÓN DE DATOS

Uno de los principios básicos del Reglamento es el de generar confianza en el tratamiento de datos y para ello se crea este sello de protección de datos.

Es voluntario y a priori certifica tratamientos concretos, no a compañías en la globalidad de sus tratamientos.

Su vigencia será de 5 años y la tasa para su obtención deberá ser razonable y armonizada en todos los países de la UE.

Las empresas podrán solicitarlo a las Autoridades de Control que lo otorgarán mediante un proceso previo de certificación realizado por profesionales acreditados. Serán las propias Autoridades de Control las que deban definir los mecanismos para acreditar a dichos profesionales encargados de la certificación, así como los requisitos y procesos que deban aplicar para emitir los certificados. Una vez obtenida la certificación, la Autoridad de Control concederá el sello.

Disponer del sello podrá evitar una posible sanción económica ante la declaración de infracción por la Autoridad de Control, siempre que no sea el resultado de un incumplimiento intencionado o negligente por parte del responsable o encargado del tratamiento.

TRANSFERENCIAS INTERNACIONALES

Se mantiene un régimen jurídico similar al actual debiendo:

- obtenerse el permiso de la autoridad nacional de protección de datos
- informarse a la persona afectada antes de comunicar los datos.

Se introducen algunos elementos de simplificación del proceso. No será necesaria la autorización si se ofrecen garantías adecuadas en un documento jurídico vinculante:

- si las empresas disponen de unas *binding corporate rules*
- si la Autoridad de Control ha aprobado unas cláusulas tipo incluidas en el contrato modelo que utilice el responsable o
- si importador/exportador han obtenido el sello Europeo de protección de datos para ese tratamiento concreto.

Las transferencias internacionales autorizadas con anterioridad a la entrada en vigor del Reglamento serán válidas pero deberán regularizarse en un plazo de 2 años.

INFRACCIONES Y **SANCIONES**

Desaparece la graduación de sanciones (leve, grave y muy grave).

Podrá haber apercibimiento en caso de un incumplimiento no deliberado siempre que se trate del primero que comete el responsable o encargado del tratamiento.

Podrá obligarse al infractor a realizar auditorías sobre un aspecto concreto durante un periodo determinado (esto hace prever que la auditoría deberá llevarse a cabo por un profesional independiente/externo)

Las multas podrán llegar hasta 100.000.000€ o bien el 5% del volumen de negocios mundial (si es superior a esos 100 millones).

Podrá graduarse la sanción en función de la proactividad o disponibilidad que ofrezca el responsable por subsanar la incidencia o infracción, el Reglamento recoge una serie de circunstancias atenuantes y agravantes que servirán de criterio para la determinación de las sanciones.

Las administraciones públicas también podrán ser sancionadas económicamente.

INFORMACIÓN Y **ENLACES**

Propuesta de Reglamento de 2012

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

Página de seguimiento de la evolución de la propuesta

http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011(COD)

Mercado único digital

http://www.europarl.europa.eu/aboutparliament/es/displayFtu.html?ftuId=FTU_5.9.4.html

Ramon Miralles

https://www.linkedin.com/in/ramonmiralles