AGE(R)S
Asociación Española de
Gerencia de Riesgos y Seguros

Newsletter

Retos ante la nueva legislación de Protección de Datos

Madrid · 21 de febrero de 2017

Bienvenida

D. José Luis Zimmermann, Miembro de la Comisión de Sociedad Digital de la CEOE ha realizado el discurso de bienvenida del acto, agradeciendo la gran acogida del mismo y animando a participar en este foro, sobre la nueva regulación de protección de datos, con la que se abre un nuevo escenario para las empresas.

D. José Luis Zimmermann
CEOE

De izquierda a derecha: Dña. Cristina Fernández-Miranda (Willis Towers Watson), D. Agustín Puente (Agencia de Protección de Datos), D. Juan Gayá (El Corte Inglés), Dña. Irene Robledo (Dac Beachcroft), D. Frederick Albanez (Zurich Spain) y D. José Luis Zimmermann (CEOE)

Intervención de D. Agustín Puente, Director de la Asesoría Jurídica de la Agencia de Protección de Datos

D. Agustín Puente
Agencia de Protección de Datos

D. Agustín Puente transmitió a los asistentes las novedades de la nueva regulación europea aprobada el 25 de mayo de 2016 y de obligado cumplimiento en mayo de 2018.

Explicó el gran cambio de perspectiva que supone el nuevo reglamento, que armoniza en un mismo documento las reglas para todos los estados miembros de la Unión Europea.

El ámbito de aplicación de la nueva legislación establece el concepto de carácter personal similar al anterior, pero con considerandos, es decir, aquellos que singularicen al individuo, entre los que se incluyen las cookies o la dirección IP.

"**Los principios del reglamento no han de cambiar con la evolución tecnológica, sino que deben reinterpretarse adaptándose a los nuevos contextos**".

Dentro del nuevo reglamento hay que destacar la necesidad de obtener el consentimiento explícito para tratar los datos de índole personal. Esto implica una gran novedad ya que hasta ahora bastaba un consentimiento tácito, lo que obligará a realizar un estudio por parte de las empresas, para revisar la manera en la que han obtenido sus datos.

En 2018, este tipo de consentimiento por omisión dejará de tener validez legítima. Ello no significa que los ficheros de prevención del fraude, por ejemplo, dejen de existir, ya que la ley previene el interés legítimo y que es imprescindible para el desarrollo de la actividad de la empresa.

Respecto a los datos personales de menores, el nuevo reglamento establece que se pueden tratar a partir de los 13 años con consentimiento paterno, pero deja a cada país la libertad de adecuarlo a la edad que estime, siempre y cuando supere la edad indicada.

Además se destaca otra novedad frente al derecho a informar, y no sólo como deber. Se establece un alcance más amplio donde D. Agustín Puente recomienda tener dos capas de seguridad: una básica para la mayoría de usuarios y otra con más información para aquellos que deseen conocerla más a fondo, como ya ocurre con las políticas de cookies.

OTRAS NOVEDADES:

El Sr. Puente destacó la importancia del **derecho a la supresión "derecho al olvido"** (artículo 17) en el que se recoge el derecho a la cancelación de los datos personales y el derecho de oposición.

El derecho de portabilidad es otro de los puntos novedosos de este reglamento europeo, estableciendo una nueva regularización para traspasar datos entre . Debiendo realizarse por contrato y siempre y cuando sea automatizado.

El reglamento ya no se configura como un listado de normas que han de cumplirse, sino que el responsable del tratamiento debe prevenir y analizar los riesgos, así como tomar medidas para que no lleguen a producirse. Es necesaria una **actitud más proactiva** que con la regulación anterior.

El artículo 71 y 76 enumeran consideraciones que generan riesgos y para los que han de tomarse medidas. Para ello es imprescindible hacer una evolución de impactos; tener unos códigos de conducta en caso de que los riesgos se lleven a cabo; y tener una figura denominada **Delegado de Protección de Datos** en el caso de que sea una entidad pública, sectores de actividad que tratan datos a gran escala o cuando haya datos sensibles.

Intervención de Dña. Irene Robledo, Abogada especialista en Protección de Datos y Ciber Riesgos en DAC Beachcroft

"El Nuevo Reglamento conllevará una mayor carga de trabajo para las empresas" así comenzaba su exposición Dña. Irene Robledo, debido a la tarea de revisión administrativa que deberán hacer las empresas de los consentimientos tácitos a través de los que se han obtenido datos de terceros.

La Sra. Robledo ha expuesto la importancia de que los responsables de tratamiento revisen también los contratos que tienen con los encargados de tratamiento para que se adapten a los nuevos requisitos exigidos por el Reglamento.

Asimismo, ha destacado, al igual que el Sr. Puente, la importancia del Derecho al Olvido en internet, que ya se recogía en la LOPD como derecho de cancelación.

Respecto al nuevo Derecho a la Portabilidad de los datos ha querido puntualizar que, para que estos puedan trasladarse de una empresa a otra, a petición del interesado, deben encontrarse almacenados en un formato común y compatible, así como que no deben ser excesivos para la finalidad para la que se recogieron.

Dña. Irene Robledo
Dac Beachcroft

Impacto del Reglamento en materia de Ciber Riesgos

1. Las **sanciones por incumplimiento aumentan** y serán proporcionales, aunque disuasorias.
2. Cuando exista una **violación de la seguridad** de los datos, esta ha de **comunicarse a la Agencia Española de Protección de Datos en un plazo de 72 horas**, así como a los interesados sin demoras injustificadas, siempre que la violación pueda afectar a los derechos y libertades de los mismos. No será necesario notificar la violación si los datos se encontraban encriptados y no se ha tenido acceso a las claves para desencriptarlos.

Además, el nuevo Reglamento recoge la posibilidad de que los afectados por un incumplimiento del Reglamento puedan reclamar indemnizaciones por daños y perjuicios a través de **organizaciones sin ánimo de lucro** que promuevan **reclamaciones masivas**.

Intervención de D. Frederick Albanez, Partners Zurich España

D. Frederick Albanez
Zurich Spain

El Sr. Albanez ha expresado la importancia de tener una **cultura de privacidad en el entorno empresarial**, lo que facilitará el cumplimiento de l nuevo reglamento, así como que no hemos de relajarnos porque nuestra legislación haya sido de las más restrictivas de la Unión Europea.

Para lograr el correcto cumplimiento del reglamento es muy importante la figura del Delegado de Protección de Datos, reformando o creando en los casos que no haya, el puesto y dotándolo de medidas para el correcto cumplimiento normativo actual.

D. Frederick Albanez, apunta la importancia de **poder compartir ficheros con el nuevo derecho de portabilidad** y sugiere una solución similar a la ya existente para intercambio de información entre corredores y aseguradoras (EIAC). Este ejemplo puede ser una solución para que aquel que lo desee pueda ejercer su derecho de portabilidad

Además, ha apuntado que aquellas empresas que no estén ya trabajando para cumplir el nuevo reglamento han de ponerse a ello de manera urgente. “En Zurich llevamos trabajando ya dos años y lo que nos queda” ha afirmado el Sr. Albanez.

Intervención de Dña. Cristina Fernández-Miranda, Special Risk Director de Willis Towers Watson

Dña. Cristina Fernández-Miranda ha remarcado la importancia de este año, 2017, para llevar a cabo la transición y adecuarse al reglamento europeo, así como la importancia de **ser proactivo y adelantarse**.

La Sra. Fernández-Miranda ha expuesto que la **valoración de los riesgos** a hacerse a través de una **metodología existente que cuantifique** y mida los riesgos. **Para las pymes**, mayoría del negocio empresarial español, bastará con **una reflexión documentada sobre los riesgos**, pero que puedan poner a disposición de la Agencia de Protección de Datos cuando ésta lo requiera.

Es imprescindible tomar medidas de control previas a la puesta en marcha del reglamento, para ello hemos de realizar **evaluaciones de impacto**, continuar con las auditorías bianuales para evaluar el impacto que un cibersiniestro puede ocasionar en la compañía y valorar si una parte ha de delegarse a las empresas aseguradoras y sus pólizas de ciberriesgos.

Dña. Cristina Fernández-Miranda
Willis Towers Watson

"**Cuando se produce una violación de seguridad es un hecho que puede ser muy costoso para la empresa**" ha explicado la representante de Willis Towers Watson, quien ha remarcado que para ello existen las **pólizas de ciberriesgos** que cada vez tienen más peso y que cubren, no sólo la notificación a terceros afectados por el robo de datos, sino los costes de envíos de documentación, el montaje de call centers para dar atención a todas las reclamaciones, los costes de abogados, daños materiales a activos digitales, gastos de primera respuesta, pérdida de beneficios e incluso **multas y sanciones como consecuencia de un fallo de seguridad**, que se recogen en el Reglamento General de Protección de Datos, pudiendo llegar a ser hasta de 20 millones de euros o el 4% de la facturación mundial de la organización.

Bajo la opinión de Dña. Cristina Fernández-Miranda es muy importante que se tienda a la **homogeneización de las normativas**, puesto que los ataques pocas veces vienen de la puerta de al lado, sino que la mayoría proceden de otras partes del mundo. Cuanta más regulación universal haya, más claros serán los riesgos.

Conclusiones

Antes de finalizar la jornada, D. Juan Gayá, Gerente de Riesgos de El Corte Inglés, Miembro de la Junta Directiva de AGERS y moderador de la jornada, abrió la ronda de prenguntas de las que se pueden extraer las siguientes conclusiones:

- El **derecho a la portabilidad** como gran novedad del reglamento europeo 2016 establece que los datos serán transferibles entre responsables cuando el propietario de los mismos así lo requiera siempre y cuando tengan un formato de uso común y puedan ser leído de manera mecánica.

- Las **violaciones de seguridad** que comprometan datos de terceros **han de comunicarse** tanto a la Agencia de Protección de datos, con un máximo de 72h, como a los interesados en un corto plazo.

- **El nuevo reglamento no recoge normas** sino que establece que sea el propio gestor de datos quien identifique cuáles son sus riesgos y cómo ha de mitigarlos.

- **Las sanciones se incrementan** pudiendo llegar a ser hasta de 20 millones de euros o el 4% de la facturación mundial de la organización.

- **El deber a informar pasa a ser un derecho imprescindible** cuando se pidan datos personales.

- **El derecho al olvido o de cancelación** invierte su procedimiento, siendo la empresa que requiera los datos quien ha de explicar por qué los quiere mantener.

- **El consentimiento para recabar información de un tercero ha de ser claro** y no puede estar pre marcado.

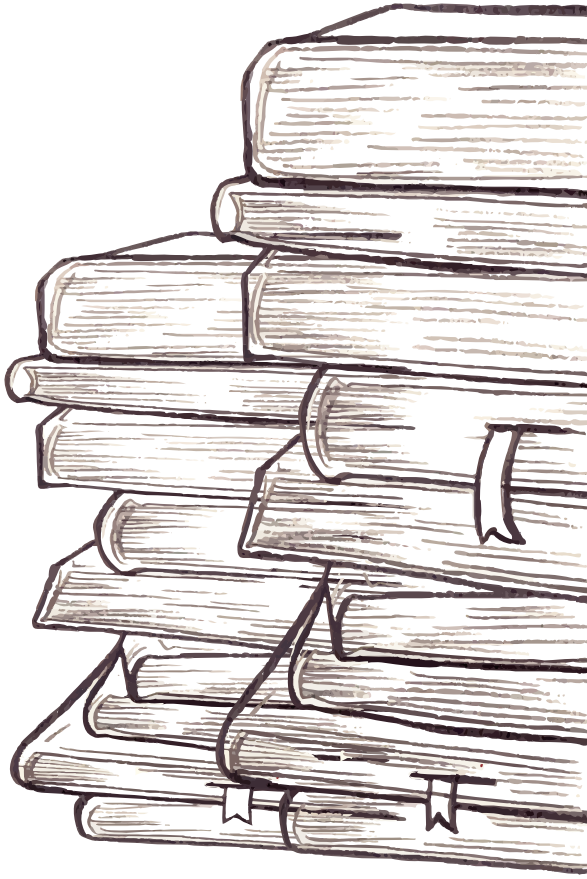
- **Los consentimientos tácitos** con los que se recogieron datos en el pasado, en el 2018 dejarán de tener base legal.

Documentación anexa - links

- Entrevista sobre el nuevo reglamento a Dña. Irene Robledo (Dac Beachcroft) en la revista de AGERS "Observatorio Gerencia de Riesgos" nº 4 (diciembre 2016) – Pág. 26

- La AEPD analiza la incidencia del nuevo Reglamento europeo de Protección de Datos sobre las pymes

- El Reglamento de protección de datos en 12 preguntas



HERBERT SMITH FREEHILLS

MAPFRE

AIG Bring on Tomorrow

AON

AXA CORPORATE SOLUTIONS redefining / standards

DAC beachcroft

GENERALI

grupo addvalora

MARCH JLT

QBE

ventiv TECHNOLOGY

Willis Towers Watson

XL CATLIN

ZURICH

CHUBB

HIGHDOME PCC

INTERNATIONAL SOS

LLOYD'S

Swiss Re Corporate Solutions