

Reflexiones sobre el futuro de la Privacidad en Europa

II Edición del Estudio
de la propuesta de
Reglamento de
Protección
de Datos de la UE

Una iniciativa de:



DPI
Data Privacy
Institute

Copyright y derechos:

DPI (Data Privacy Institute) - ISMS Forum Spain.

Todos los derechos de esta Obra están reservados al **DPI** y a **ISMS Forum Spain**. Los titulares reconocen el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

- a) Que se reconozca la propiedad de la Obra indicando expresamente los titulares del Copyright.
 - b) No se utilice con fines comerciales.
 - c) No se creen obras derivadas por alteración, transformación y/o desarrollo de esta Obra.
- Los titulares del Copyright no garantizan que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores que pudieran detectarse a este nivel
 - El contenido de la Obra no constituye un asesoramiento de tipo profesional y/o legal.
 - No se garantiza que el contenido de la Obra sea completo, preciso y/o actualizado.
 - Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos y demás elementos de propiedad industrial citados en la Obra son de propiedad exclusiva de los titulares correspondientes.
 - Las opiniones contenidas en el presente Estudio, son la suma de las aportaciones de un grupo de expertos en protección de datos, por tanto, no necesariamente reflejan la opinión de DPI-ISMS Forum Spain.

Más información acerca de **DPI / ISMS Forum Spain** se puede consultar a través de su página web oficial: www.ismsforum.es/dpi

ÍNDICE

Carta de Presentación	5
Introducción	7
Alcance y Objetivos	9
Metodología	11
Cap. 1.- Reglamento europeo de Protección de Datos y PYMES.	13
Cap. 2.- Privacy Impact Assesstment y Privacy by design	27
Cap. 3.- Data Protection Officer: perfil, formación, posición, competencias y operativa.	43
Cap. 4.- Reglamento europeo de Protección de Datos, Binding Corporate Rules y Grupos multinacionales.	55
Cap. 5.- La nueva configuración de los Derechos de los interesados.	71
Cap. 6.- Seguridad: Análisis de riesgos, RLOPD y Estándares de Seguridad de la Información.	87
Cap.7.- Accountability: cómo demostrar el cumplimiento de manera continuada y sostenible.	101

En este Estudio han colaborado:

- CDPP** Edgar Ansola Munuera
CDPP Miguel Ángel Ballesteros
Zuriñe Areitio Labanda
- CDPP** Noemí Brito Izquierdo
Ignacio Bruna López Polín
- CDPP** Fernando Campo Guardiola
- CDPP** Francisco Javier Carbayo
- CDPP** Rafael Castejón
- CDPP** José Luis Colom Planas
- CDPP** Concepción Cordón Fuentes
José Martín Dacal Romero
Flora Egea Torrón
- CDPP** Verónica Eguirón Vidarte
Ana Belén Galán
- CDPP** Juan García Galera
Mónica Garrido Vílchez
Ramón González-Calero
David González Calleja
- CDPP** Ana González Romo
- CDPP** Francesc Flores González
Héctor E. Guzmán Rodríguez
- CDPP** Ana Iparraguirre Jiménez
- CDPP** María José Lacunza González
- CDPP** Gustavo Lozano García
Miguel Ángel Lubian
Luis Salvador Montero
- CDPP** Elena Mora González
- CDPP** Raúl Perdigones López
- CDPP** Javier Pérez García
- CDPP** Nathaly Rey Arenas
- CDPP** Soledad Romero Jiménez
Julio San José Sánchez
Francisco Javier Sempere Samaniego
Cristina Sirera Martínez
- CDPP** Carlos Alberto Saiz Peña
María Teresa Torres Cardona
- CDPP** Rafael Velázquez Bautista
- CDPP** Eva Vidal Fernández

Coordinadores:

- CDPP** Francisco Javier Carbayo
- CDPP** Carlos Alberto Saiz

CARTA DE PRESENTACIÓN

Queridos amigos:

Desde [ISMS Forum Spain](#) (Asociación Española para el Fomento de la Seguridad de la Información) seguimos promoviendo las iniciativas y las acciones tangibles, prácticas y útiles que permitan crear y aportar valor a nuestros miembros, a las organizaciones públicas y privadas y a la Sociedad en general.

Es por ello que lanzamos esta nueva acción dentro del [Data Privacy Institute \(DPI\)](#), iniciativa de [ISMS Forum Spain](#), que aglutina a todas las personas y organizaciones que tienen responsabilidades y/o interés en el cumplimiento de la normativa sobre Privacidad y Protección de Datos de carácter personal.

En concreto se trata de la segunda edición del “[Estudio de impacto y GAP con la normativa española de la propuesta de Reglamento General de Protección de Datos de la Unión Europea](#)”, que se desarrolla bajo el título “[Reflexiones sobre el futuro de la Privacidad en Europa](#)”.

Este documento tiene como objetivo principal ser un análisis de determinadas materias y aspectos de la propuesta de nueva regulación, considerando tanto el borrador publicado en enero de 2012 por la Comisión, como el publicado en mayo de 2013 por el Consejo, de modo que se pueda conocer en detalle los aspectos regulados en esta normativa, el análisis en profundidad de sus consecuencias y las propuestas concretas para su actuar conforme disponen los citados borradores.

Esperamos que este Segunda edición del Estudio os resulte de interés y utilidad, pues esas son sus principales finalidades.

Por último, os animamos, como siempre, a ser partícipes de las iniciativas y acciones de [ISMS Forum Spain](#) y del [DPI](#), puesto que vuestra colaboración y el trabajo en red es clave para un resultado mayor y mejor.

Atentamente,
Gianluca D’Antonio
(Presidente)

Carlos Alberto Saiz Peña
(Secretario y Vicepresidente)



INTRODUCCIÓN

Desde el Data Privacy Institute (DPI) de ISMS Forum Spain hemos recogido la sensibilidad de muchos de nuestros socios y su interés por profundizar, aun más tras la publicación de la primera edición del Estudio, en cómo va a influir en España la futura normativa europea en materia de Protección de datos, que vendrá a sustituir a la Directiva 95/46/CE.

De esta manera, hemos desarrollado con mucha ilusión una segunda edición del Estudio sobre la Propuesta de “Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento General de Protección de Datos)”.

Este estudio ha contado con el apoyo, la reflexión y el conocimiento de un amplio grupo de expertos de primer nivel, que no sólo querían exponer y aportar su opinión, sino que antes bien querían compartir su conocimiento y experiencia con el resto de socios y con la Sociedad en general.

Sirva esta introducción para mostrar el agradecimiento de ISMS Forum Spain y del DPI a los participantes en el Estudio por su enorme interés, por su implicación, por el uso e inversión de tiempo libre que sabemos han realizado, por su disposición permanente, y por el magnífico nivel de los resultados alcanzados.

ALCANCE Y OBJETIVOS

El Alcance definido para esta iniciativa se concreta en los siguientes textos:

- Propuesta de “Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento General de Protección de Datos)”, publicada por la Comisión Europea en enero de 2012.
- Propuesta de “Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento General de Protección de Datos)”; publicada por el Consejo de la Unión Europea en mayo de 2013.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento General de Protección de Datos) - Cuestiones clave de los Capítulos I a V, publicada por el Consejo de la Unión Europea en mayo de 2013.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento General de Protección de Datos) - Cuestiones clave de los Capítulos I a V – ADD1, publicada por el Consejo de la Unión Europea en mayo de 2013.

Tales textos se citan de manera individual en cada capítulo o vienen referenciados de manera conjunta como “Propuesta de Reglamento UE de Protección de Datos”.

En cuanto a los Objetivos de la iniciativa, han sido principalmente:

- Proponer un estudio de determinados aspectos y materias de la propuesta de nueva regulación, de cara a realizar un análisis en profundidad, práctico y con aportación de valoraciones y/o acciones a realizar en cada caso.
- Todo ello considerando la actual regulación en España, y de modo principal con relación a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, RLOPD).
- Además, se había de tomar como objetivo el establecer, cuando aplicara el gap con la Directiva 95/46/CE del Parlamento europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE).
- Mostrar no sólo el interés del DPI sobre el proceso de creación normativa, sino su voluntad de crear una opinión propia y experta sobre la evolución de tal proceso y sobre la regulación que se pretenda aprobar.
- Aportar medios y herramientas no sólo a los miembros de ISMS Forum Spain y del DPI, sino a la Sociedad en general, para conocer y comprender la nueva regulación, sus conceptos y requisitos, los retos que plantean determinadas e importantes novedades y el impacto que tendrá en todo tipo de organizaciones, en particular, en las empresas, con independencia de su tamaño.

METODOLOGÍA

Para el desarrollo de un Estudio de esta envergadura, como ya ocurrió en la Primera Edición, era necesario adoptar una metodología de análisis y presentación de resultados homogénea, clara y práctica. Y ello no sólo por el número de personas que han invertido tiempo y esfuerzo personal en su elaboración, sino también por los destinatarios y lectores del mismo.

En este sentido, todos los implicados en este Estudio hemos buscado desde el primer momento un resultado útil y de fácil uso, que aportara un valor efectivo a los receptores del documento respecto al conocimiento del contenido e impacto de la Propuesta de Reglamento UE de Protección de Datos.


Se debe tener en cuenta que, a diferencia de la primera edición de este Estudio, la segunda Edición del mismo se ha focalizado en materias y temas específicos, aquellos que entendíamos que podrían generar más interés, más utilidad y/o que suscitaban un mayor número de cuestiones abiertas al debate. Lógicamente, la labor de selección de materias y temas no ha sido fácil, por la diversidad de cuestiones que cabría abordar, pero sí que ha partido de criterios objetivos y se ha desarrollado de manera colegiada en el seno del Comité Operativo del DPI.

Creemos que si realmente queremos tener una aproximación a la regulación en ciernes después del enfoque de la primera edición del citado Estudio, tenemos que dar el salto desde una aproximación basada en el análisis artículo por artículo, hacia una reflexión profunda, fundamentada y crítica sobre ciertos clave de la normativa que se pretende aprobar a nivel comunitario.

Lógicamente, se trataba de una opción ambiciosa, que sin embargo, hemos afrontado con la intención de promover y publicar un Estudio que permitiera entrar en profundidad en las materias y temas sobre los que se ha centrado el foco.

Para poder manejar la elaboración del documento en unos términos razonables, ordenados y estables, se desarrolló una metodología de trabajo específica, bajo las siguientes pautas:

- El Comité Operativo del DPI aprobó la creación de Grupos de trabajo, cada uno bajo la batuta de un Coordinador miembro del propio Grupo.
- Todos los Grupos estarían bajo la supervisión de un Coordinador de Coordinadores, que resolvería o canalizaría las cuestiones sobre bases de elaboración, incidencias, plazos, niveles de calidad, puesta en común, etc. En este sentido, se creó un plantilla-base que establecía únicamente los parámetros formales para encuadrar cada entregable por Grupo.
- Una vez creados los Grupos, cada uno con su tema propio y su Coordinador nombrado (una vez los propuestos aceptaron tal designación), se puso en marcha la elaboración de los borradores de capítulos.
- Cada Grupo tuvo libertad y autonomía tanto para desarrollar su tema, como para articular su operativa (índice de desarrollo, fuentes, pautas de elaboración, reuniones presenciales y/o en remoto, revisiones, etc.).
- Se revisaron todas las aportaciones para verificar el mantenimiento de las pautas de homogeneidad, claridad y precisión que debían regir, en todo caso, el resultado final
- Finalmente, se trasladaron todas las aportaciones a un documento único, que constituye el núcleo central de este Estudio.

The background of the slide features the European Union flag, which consists of a blue field with twelve gold stars arranged in a circle. The flag is partially visible in the upper right corner. A bright, white light source in the lower left corner creates several diagonal rays of light that sweep across the frame towards the upper right. These rays are accompanied by a bokeh effect of out-of-focus white circles of varying sizes, giving the impression of light particles or data points.

Cap. 1
Reglamento
Europeo de
Protección de Datos
y PYMES

ABSTRACT

Teniendo como punto de partida la situación actual (Estado de la situación) del cumplimiento normativo respecto de la LOPD y el RLOPD, veremos, a través de las distintas facetas estudiadas en las siguientes páginas, como las PYMES Europeas y más en concreto en aquello que nos atañe, las PYMES Españolas, se enfrentan ante la Propuesta de Reglamento UE de Protección de Datos, a muy importantes retos, desde el punto de vista del tratamiento reglamentario (la propuesta de Reglamento, Análisis normativo), de cómo se obtienen, se tratan y se preservan los datos personales que, de los distintos titulares (empleados, clientes, proveedores, etc.), están incluidos en los sistemas de información de la empresa.

Así mismo veremos la necesaria adaptación de la organización a las medidas, tanto organizativas como tecnológicas, que deben ser modificadas de acuerdo a la Propuesta de Reglamento UE de Protección de Datos. (La propuesta de Reglamento. TIC's y medidas organizativas).

Analizaremos que fortalezas y debilidades tienen las PYMES frente a la Propuesta de Reglamento UE de Protección de Datos, las ventajas y obstáculos que plantea, que oportunidades presenta, y cuáles pueden ser las estrategias para afrontarlos. (la propuesta de Reglamento, Análisis DAFO, Estrategias).

Y por último veremos cuál puede ser el futuro de la Propuesta de Reglamento UE de Protección de Datos (La propuesta de Reglamento, El futuro, ¿Aprobación? ¿No aprobación?, Evolución) y cómo afectará a las PYMES, teniendo en cuenta, por un lado, los distintos informes de las Comisiones, las negociaciones entre los Estados Miembros y las presiones recibidas, y por otro lado, la ineludible evolución de las TIC's y los Sistemas de Información de las PYMES, dado que, contemplando dicha evolución sólo durante el período de elaboración, presentación, debate, discusión y negociación de la Propuesta de Reglamento, es decir en el corto tiempo de tres años, nos encontramos con nuevos conceptos y "fenómenos" inmersos en la vida empresarial, tales como el almacenamiento y tratamiento de la información en la Nube (Cloud Computing), la capacidad de análisis de ingentes cantidades de "datos" relacionados y no relacionados (Big Data) la "explosión" de los dispositivos móviles, tablets, smartphones, etc., conectándose a los procesos de TI de la organización, conocido como "tráete tu propio dispositivo" (Bring your Own Device , BYOD), o las amenazas y ataques a los sistemas de información y comunicación de las empresas (Flame, Botnets, Malware, DDos, Phising, APT's...).

DESARROLLO

Estado de la situación actual de la Protección de Datos

No podemos soslayar en ningún momento que, aunque en el pensamiento de muchos de los ciudadanos y empresarios parece que la protección de la privacidad está orientada a las grandes empresas, las operadoras de servicios, las multinacionales, su destinatario natural en la Unión Europea son precisamente las PYMES, dada su preponderancia en la demografía empresarial. Conforme a las estadísticas, en el conjunto de la Unión Europea, las PYMES suponen el 99,68 % de las empresas, (99,85 % en el caso de España), y si contemplamos las Microempresas (menos de 10 empleados según la recomendación de la Comisión 2003/361/CE), son el 92,45 % en la Unión Europea y el 95,43 % en España.

Así mismo debemos observar la evolución del cumplimiento, por parte de las empresas y profesionales, de la Protección de Datos en España a lo largo de los 20 años recién cumplidos de la legislación de la materia. De acuerdo a las estadísticas elaboradas vemos como el número de empresas que tiene pendiente el mínimo requisito legal como es el registro de sus ficheros en la Agencia Española de Protección de Datos es abrumador. A 31 de Diciembre de 2012, de acuerdo a los datos de la Agencia, de entidades registradas por Comunidades Autónomas y Provincias se encontrarían pendientes de registrar sus ficheros el 71,91 % de las empresas españolas.

Desde la foto del estado de cumplimiento actual por parte de las empresas españolas, nos enfrentamos a los posibles escenarios que se pueden plantear ante la Propuesta de Reglamento UE de Protección de Datos. Durante el período de negociación del mismo y la elevación de informes de las distintas Comisiones (Consejo, SEPD, CDR, LIBE, CES...), han quedado patentes las diferentes opiniones y controversias que suscita la Propuesta de Reglamento UE de Protección de datos con el número de enmiendas presentadas, más de 4.000, y la presión ejercida por los distintos grupos de interés (lobbies) empresariales (sobre todo los correspondientes a EEUU), instituciones y Estados Europeos. Esta situación nos indica el tremendo interés que despierta la Propuesta de Reglamento UE de Protección de Datos y la preocupación de su alcance, y de cómo afectará a la actividad de las empresas, como por ejemplo, las limitaciones que algunos grupos de presión estiman que impondrá el Reglamento a la competitividad y evolución de las empresas europeas frente a las estadounidenses y otras no comunitarias, no limitadas por dicha reglamentación.

Este nivel de presión, las enmiendas presentadas y las reticencias de varios de los Estados Miembros (Gran Bretaña, Checoeslovaquia, Polonia ...) han impedido la votación de la Propuesta de Reglamento que se ha ido aplazando en varias convocatorias, introduciéndose además el parámetro temporal, de urgencia, dada la vigencia de la actual legislatura parlamentaria que finaliza en mayo del 2014.

Por otro lado, los eventos e "incidencias" internacionales de los últimos meses relativos a la privacidad y las tecnologías de la información y la comunicación, en concreto, toda la controversia suscitada por las filtraciones del ex empleado de la NSA, Edward Snowden, referen-

tes al programa PRISM, han disparado las exigencias sobre los criterios de privacidad a nivel mundial, dando lugar a un importante número de interpelaciones, peticiones de información y explicaciones entre las Presidencias de los distintos Estados, incluidas las de la propia Comisión Europea. Aunque de una manera transversal, todo esto probablemente incidirá en el proceso de negociación y aprobación de la Propuesta de Reglamento.

La propuesta de Reglamento. Análisis normativo

A lo largo de este sub-apartado, se tratará de destacar las principales novedades y retos a los que se enfrenta la PYME desde el punto de vista del cumplimiento normativo. Para ello se destacarán las principales variaciones entre la normativa vigente y la Propuesta de Reglamento UE de Protección de Datos, sus principales novedades y obligaciones.

VARIACIONES.

Sin duda la gran variación con respecto a la situación actual es la desaparición de la obligación de notificar los tratamientos de datos a la Autoridad de Control, medida que se ha demostrado que no aporta mejoras a la Protección de Datos y que ha logrado un respaldo unánime por todos los actores implicados en la reforma. Pero que desaparezca la obligación de notificar los tratamientos de datos personales no significa que desaparezca la obligación de detectarlos, analizarlos y controlarlos, para poder dar cumplimiento a las nuevas obligaciones que se establecen en la nueva normativa y que iremos viendo a continuación, como puede ser la rendición de cuentas o *accountability*, el deber de documentar el cumplimiento de las obligaciones en materia de Protección de Datos o el establecimiento de los principios de transparencia y privacidad por diseño y por defecto.

En lo que respecta al ejercicio de los derechos A.R.C.O. (acceso, rectificación, cancelación u oposición), se amplía y unifica el plazo para su resolución en un mes para todos los casos y se establece la posibilidad de ejercicio por vía electrónica, lo que provocará un abaratamiento de costes.

Se refuerzan los deberes de información y obtención del consentimiento, sobre todo en los casos de tratamiento de datos de menores, lo que redundará en mayor confianza por parte de clientes y consumidores.

Está por ver la variación en la adopción de medidas de seguridad en los tratamientos, puesto que deberán ser desarrolladas en una fase posterior por la institución que finalmente tenga atribuida esa competencia (Comisión Europea o Consejo Europeo de Protección de Datos) o por los Estados Miembros como en la actualidad.

NOVEDADES.

Se introducen las figuras de la Privacidad por diseño y por defecto de manera que se garantice que todas las fases de los tratamientos de datos personales cumplen con la normativa vigente y que sólo se tratan los datos necesarios e imprescindibles para la finalidad para la que se obtuvieron. El establecimiento de estos mecanismos y controles por parte de la PYME limitará los riesgos derivados de los tratamientos y por ello la posibilidad de incumplimiento y posterior sanción. Independientemente de que se establezca posteriormente en el desarrollo normativo de las medidas de seguridad la obligación de realizar auditorías periódicas para todos

o ciertos tipos de tratamientos, la plena adopción de estos principios requerirá el establecimiento de controles periódicos, ya sean internos o externos, que valoren y determinen el grado de cumplimiento de los mismos.

Establecimiento del principio del One Stop Shop, mediante el cual los ciudadanos y los Responsables de tratamiento podrán dirigirse a la Autoridad de Control de su país de residencia, evitando el tener que realizar cada trámite en un país diferente, con el consiguiente ahorro de tiempo y dinero.

Adopción del principio de transparencia mediante el cual los responsables de tratamiento deberán aplicar políticas transparentes y ser fácilmente accesibles en lo que respecta a los tratamientos previstos y modo de ejercicio de derechos. A mayor transparencia, mayor confianza por parte del cliente o consumidor.

Instauración del denominado “derecho al olvido”, que deberá ser tenido en cuenta no sólo por las PYMES de corte tecnológica o de comunicación, sino también por las PYMES con gran actividad e interacción con sus seguidores en redes sociales.

Instauración del derecho a la portabilidad de datos cuando los datos se traten en vía electrónica y en un formato estructurado y comúnmente utilizado. Cabe advertir que para las PYMES a veces será una obligación y otras será un derecho (contratación de un servicio de Cloud Computing).

Finalmente cabe destacar la promoción de los Códigos de Conducta y las certificaciones en materia de Protección de Datos, lo que fomentará las buenas prácticas en esta materia, facilitará la percepción del nivel de cumplimiento en protección de datos por parte de terceros y afectados y posibilitará el cumplimiento de los principios de la Privacidad por diseño y por defecto.

OBLIGACIONES.

Documentar para poder demostrar el cumplimiento de sus obligaciones en materia de protección de datos. Esta obligación nos facilitará la prueba de cumplimiento ante una inspección de oficio o a raíz de denuncia por parte de la Autoridad de Control.

Una novedad y a la vez una obligación es la notificación de las violaciones de datos personales a la Autoridad de Control competente, si demora y como máximo en un plazo de 24 horas desde que se produce. Esta notificación puede extenderse a los propios afectados cuando se cumplan los supuestos contemplados en la normativa.

Otra novedad que genera a su vez una obligación es la de realizar una evaluación de impacto previa al inicio de determinados tratamientos.

La obligación de solicitud de autorización previa a la Autoridad de Control aumenta los supuestos en los que es preceptiva. Además de para transferencias internacionales de datos a países que no tengan reconocido un nivel adecuado de protección, será necesaria para iniciar un tratamiento que haya obtenido un resultado desfavorable en la declaración de impacto previa y para tratamientos con riesgos específicos que serán enumerados en una lista de operaciones que emitirá la Autoridad de Control. Este requisito dará seguridad jurídica a las PYMES ya que una vez obtenida la autorización y si se cumple con las obligaciones que establezca la Autoridad de Control no cabrá sanción por denuncia de un afectado por el tratamiento.

Finalmente una de las nuevas obligaciones que mas eco ha tenido es la creación de la figura del Delegado de Protección de Datos o DPO. Aunque el umbral para su nombramiento cambia en las diferentes versiones de la Propuesta de Reglamento UE de Protección de Datos (Comisión o Consejo), el que se pueda establecer para determinados tratamientos (datos especialmente protegidos y determinados tipos de tratamientos) puede conllevar que para algunas PYMES resulte obligatorio proceder a la contratación de estos profesionales, que posibilitarán un tratamiento conforme a la Normativa Europea de Protección de Datos y difuminarán por ello la posibilidad de incumplimiento.

Entrada en vigor y desarrollo posterior.

En lo que respecta a la entrada en vigor de la futura normativa, tenemos que tener en cuenta dos variables:

Por un lado la entrada en vigor de la Propuesta de Reglamento UE de Protección de Datos se establece a los veinte días a contar desde su publicación en el Diario Oficial de la Unión Europea y la fecha de aplicación será a los dos años de la fecha mencionada anteriormente.

Por otro lado como ya se ha destacado a lo largo de esta exposición, hay aspectos de la nueva normativa que requerirán un desarrollo normativo posterior mediante la figura de actos delegados. En la primera propuesta estos actos delegados eran atribuidos a la Comisión Europea, aunque documentos posteriores le retiran competencias a favor de los Estados Miembros o el Consejo Europeo de Protección de Datos. Al existir un periodo de carencia de dos años, se antoja en principio tiempo más que suficiente para que la Institución o Instituciones que finalmente tengan atribuidas esas competencias, elaboren y dicten esos actos delegados de desarrollo normativo.

La propuesta de Reglamento. TIC's y medidas organizativas

RETOS Y OBLIGACIONES

Las PYMES españolas, tras la aprobación de la Propuesta de Reglamento UE de Protección de Datos, deberán afrontar una serie de retos y obligaciones en materia de seguridad que hasta el momento no habían sido contemplados.

Actualmente la aplicación de las medidas de seguridad se basa en el "principio de seguridad de datos" establecido en el artículo 9 de la LOPD, que impone al Responsable del fichero, y en su caso, al Encargado del tratamiento, adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas están claramente definidas en el Título VIII del RLOPD, existiendo tres niveles de seguridad (básico, medio y alto), definidos en el art. 80 RLOPD, que se aplican en función del tipo de datos que contenga el fichero y la finalidad del tratamiento que se vaya a llevar a cabo con dichos datos.

En el cuadro adjunto se describen los principales retos y obligaciones a los que deberán enfrentarse las PYMES una vez aprobado la Propuesta de Reglamento UE de Protección de Datos.

RETOS	OBLIGACIONES
Ausencia de medidas concretas para cumplir con las obligaciones exigidas en la Propuesta	<p>Todo dependerá del resultado de la preceptiva evaluación de riesgos que habrá que realizar y, como novedad, de las técnicas existentes y los costes asociados a su implementación (art. 30).</p> <p>No obstante, la Comisión (art. 30.3) estará facultada para adoptar actos delegados de conformidad a fin de especificar los criterios y condiciones aplicables a las medidas técnicas y organizativas, incluida la determinación de cuáles son las técnicas existentes, para sectores específicos y en situaciones de tratamiento de datos específicas.</p> <p>Se deberán tener en cuenta las soluciones de “Privacidad desde el diseño” y la “Protección de datos por defecto”, conceptos completamente novedosos hasta ahora.”</p>
“Principio de responsabilidad” o rendición de cuentas	<p>El artículo 22 indica que el responsable del tratamiento, en nuestro caso la PYME, adoptará políticas e implementará medidas apropiadas para asegurar y poder demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con la Propuesta de Reglamento UE de Protección de Datos. Entre estas obligaciones se encuentra la implementación de los requisitos en materia de seguridad de los datos (art. 30), que afecta tanto al Responsable del tratamiento como al Encargado del tratamiento.</p> <p>En el artículo 22.4 se indica explícitamente que la Comisión estará facultada, entre otras cosas, para considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.</p>
Verificación del cumplimiento	<p>El artículo 22.3 especifica que se deberán implementar mecanismos de verificación, que en determinados casos (cuando “no sea desproporcionado”, un parámetro que, en principio y hasta que la Comisión no se pronuncie, resulta cuando menos ambiguo) serán llevados a cabo por auditores independientes internos o externos.</p> <p>Es razonable pensar que muchas de las PYMES optarán por contratar profesionales externos que cubran esta obligación en caso de no disponer de ese perfil en plantilla.</p> <p>Las PYMES, incluso, tendrán la posibilidad de obtener una certificación, sello o marca de protección de datos (art. 39) que avale su cumplimiento de cara a los clientes.</p>
Evaluación de impacto relativa a la protección de datos	<p>Para ciertos tratamientos de datos que entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines, será necesario realizar una evaluación de impacto relativa a la protección de datos (art. 33).</p> <p>La Comisión considerará la adopción de medidas específicas para las microempresas y pequeñas y medianas empresas (art. 33.6).</p>

EVOLUCIÓN

El Documento de Seguridad actual (art. 88 RLOPD) parece que en cierta medida se conserva, debiendo revisarlo al completo para que cumpla todo lo referente a la documentación de los tratamientos del nuevo Reglamento (art. 28). Estas nuevas obligaciones referentes a la documentación no serán aplicables a las PYMES en el caso de que los tratamientos de datos personales sean accesorios a sus actividades principales (art. 28.4.b).

En algunos casos habrá que modificar las condiciones del contrato de prestación de servicio del Encargado del tratamiento (art. 26), ya que la PYME deberá velar porque el encargado de tratamiento cumpla las medidas de seguridad.

Habrà que revisar la documentación referente a las funciones y obligaciones del personal para evaluar si el actual Responsable de Seguridad, necesario a partir de niveles de seguridad medio (art. 109 RLOPD), seguirá siendo obligatorio con el nuevo Reglamento, puesto que el futuro Delegado de Protección de Datos únicamente será necesario designarlo en las PYMES cuando las actividades principales de tratamiento requieran un seguimiento periódico y sistemático de los interesados (art. 35), no entrando a valorar el nivel de los datos.

Habrà que revisar los procedimientos de notificación y gestión de incidentes de seguridad (para aquellas PYMES que sean proveedores de servicios de comunicaciones electrónicas, esto ya se encuentra regulado en el Reglamento UE 611/2013):

- Notificar la violación de datos a la Autoridad de Control (art. 31).
- Notificar la violación de datos al interesado (art. 32).

Habrà que revisar los procedimientos para cumplir los derechos de los afectados e incluir aquellos procedimientos para:

- Cumplir las condiciones de información al interesado (art. 14). La Comisión adoptará medidas apropiadas para las microempresas y las pequeñas y medianas empresas.
- Cumplir las condiciones para el consentimiento al tratamiento (art. 7). Se debe prestar especial atención al tema del uso de las cookies, regulado por el art. 22.2 de la Ley 34/2002.
- Cumplir el derecho al olvido y supresión (art. 17).
- Cumplir el derecho a la portabilidad de los datos (art. 18).

Habrà que añadir procedimientos para la evaluación de impacto de los tratamientos que entrañen riesgos específicos para los derechos y libertades de los interesados (art. 33), cambiando la forma de aplicar actualmente las medidas de seguridad contempladas en el RLOPD.

Habrà que añadir procedimientos para notificación y consulta previa a la Autoridad de Control (art. 34) y desaparecerà la obligación actual de inscripción de creación, modificación o supresión de los tratamientos (Capítulo II del RLOPD).

Con respecto a la obligación actual de realizar auditorías bienales (art. 96 RLOPD), el nuevo Reglamento no exige esos plazos, indicando únicamente que el responsable del tratamiento implementará mecanismos para verificar la eficacia de las medidas aplicadas (art. 22.3). Las PYMES deberían implementar procedimientos, protocolos y herramientas que les permitan regular las actividades del personal, prevenir los actos no conformes con dicha regulación, mitigando los riesgos y en su caso obtener pistas de auditoría y logs.

La propuesta de Reglamento. Análisis DAFO. Estrategias

Análisis DAFO	
ORIGEN INTERNO	ORIGEN EXTERNO
<p style="text-align: center;">POSITIVO</p> <p style="text-align: center;">FORTALEZAS</p> <p>(Factores internos que favorecen o impulsan la aplicación del Reglamento)</p> <ul style="list-style-type: none"> • Aumenta la responsabilidad en la implantación de mecanismos que garanticen el cumplimiento de los nuevos principios como el de "Accountability" y las obligaciones en materia de Protección de Datos. • Podrán manejar su propio enfoque basado en la existencia de riesgos en Protección de Datos. • Fomento de la autorresponsabilidad. • Aumento de la imagen profesional, visión más positiva de sus servicios. • Incremento de la confianza de los ciudadanos en la PYME. • Facilita el diseño de estrategias de empresa alineadas con la normativa • Amplia la marca empresarial de confianza en privacidad y capacidad de atraer usuarios. • Capacidad de adaptación a la nueva normativa de las PYMES que ya cumplan. 	<p style="text-align: center;">NEGATIVO</p> <p style="text-align: center;">DEBILIDADES</p> <p>(Factores internos que limitan o reducen la capacidad de la PYME en la aplicación del Reglamento)</p> <ul style="list-style-type: none"> • Tendrán obligación de conservar la documentación de todas las operaciones de tratamientos de datos efectuadas bajo su responsabilidad • Deberán elaborar y aplicar políticas internas de protección de datos que den cumplimientos al principio del "Privacy by desing" y el de "Privacy by default". • Necesitarán programas de formación de empleados. • Estarán obligadas a pre-evaluar el impacto en materia de protección de datos de cada una de las actividades y productos desarrollados. • Deberán notificar los incidentes graves de seguridad. • Mayor riesgo de sanciones. • Limitación de recursos humanos, económicos y técnicos.
<p style="text-align: center;">OPORTUNIDADES</p> <p>(Factores externos que pueden suponer una ventaja para la PYME en la aplicación del Reglamento)</p> <ul style="list-style-type: none"> • Eliminación de la obligación de notificar y registrar los ficheros de datos personales ante la autoridad de control. • Permiten la entrada en mercados transfronterizos con mayores garantías de seguridad. • Nuevos clientes internacionales con mayores garantías derivadas de la armonización de derechos. • Simplificación de las cargas administrativas de protección de datos para las PYMES. • Legislación más clara. • Mayor posibilidad de presencia internacional y más facilidad para las posibilidades de expansión de los negocios en la UE. • Mayor transparencia para los ciudadanos. • Protege uno de los activos más valiosos de la PYME, los datos personales de clientes, recursos humanos, etc. • La Comisión se ocupará de facilitar la adopción de medidas específicas para las PYMES y el establecimiento de formularios y procedimientos normalizados para las comunicaciones a los interesados, incluido el formato electrónico. 	<p style="text-align: center;">AMENAZAS</p> <p>(Factores externos que pueden impedir o dificultar la aplicación del Reglamento en la PYME)</p> <ul style="list-style-type: none"> • Obligación de cooperar y rendir cuentas no sólo ante la autoridad de control nacional sino también ante la Comisión. • Para prestación de servicios de la sociedad de la información deberán obtener el consentimiento previo de los padres o tutores de los menores de 13 años para que el tratamiento sea lícito. • Asumirán la carga de la prueba de la prestación del consentimiento por el interesado. • Deberán adoptar los mecanismos adecuados para garantizar el derecho al olvido y a la portabilidad de los datos, en su caso. • Deberán notificar las brechas de seguridad. • Existirá brecha digital entre aquellas PYMES que tienen mayor capacidad para el cumplimiento y las que no.

Análisis DAFO

ESTRATEGIAS

Así, se proponen inicialmente como estrategias las siguientes:

- Promover acciones específicas dirigidas a las PYMES en materia de cumplimiento de las obligaciones de protección de datos.
- Analizar y detectar cuales son las necesidades más comunes para facilitar el cumplimiento de modo estandarizado.
- Evaluar y promocionar a través de los medios de comunicación acciones de sensibilización.
- Realizar campañas y programas de formación a los empleados de las PYMES.
- Desarrollar modelos y prácticas normalizadas que proporcionen un enfoque de sus riesgos en protección de datos que se perfile sostenible y rentable en el tiempo.

La propuesta de Reglamento.

El futuro. ¿Aprobación?. ¿No aprobación?. Evolución.

No debemos tampoco olvidar los datos que nos presentan diversos estudios y encuestas realizados por Consultoras y Empresas referentes mundiales del sector, y que ponen de manifiesto como las PYMES o bien siguen sin tener el nivel de preocupación recomendable frente a la seguridad de la información (incidencias, ataques, ciberseguridad), o bien se consideran incapaces de afrontarlas dada la velocidad de evolución y desarrollo de tales incidencias y de la tecnología necesaria para enfrentarse a ellas junto con la diversidad y complejidad de reglamentaciones (LOPD, RLOPD, LSSI-CE, LISI, LGT, LPI...), que deben ser contempladas, interpretadas e implementadas en sus organizaciones.

Todo esto no hace más que incrementar el nivel de incertidumbre de las PYMES (obviamente refiriéndonos a aquellas PYMES “cumplidoras” de acuerdo a las estadísticas) frente a la aprobación, no aprobación o aprobación con mayores o menores modificaciones de la Propuesta de Reglamento UE de Protección de Datos, que contemplan, inmersas en la crisis económica actual, la carga adicional que puede implicar su aprobación, tanto económica como de procesos de trabajo y procedimientos de documentación e información.

Conforme al articulado de la Propuesta de Reglamento UE de Protección de Datos, aparecen nuevos (o se modifican de forma sustancial los existentes) elementos, conceptos y situaciones que le plantearan a las PYMES, la obligación, en su proceso de adaptación, de nuevas medidas, cambios importantes en sus procedimientos y protocolos de tratamiento de la información, revisión y modificación de su Documento de Seguridad, modificaciones en la tipología y tipificación de los datos, modificación y adecuación de las medidas y niveles de seguridad en el tratamiento de los datos.

Añadido a esto, como hemos señalado anteriormente, las PYMES se enfrentan a la evolución de la Tecnología, con nuevas formas y escenarios de captura, acceso, tratamiento y almacenamiento de la información, Cloud Computing, acceso remoto, teletrabajo, tablets, smartphones, (BYOD), bases de datos distribuidas, intranets y extranets, big data, comercio

electrónico, redes sociales, etc., contemplándolo desde dos perspectivas principales: por un lado, la adopción y adaptación de dichas tecnologías y herramientas para un mejor desarrollo de las actividades empresariales con una reducción o racionalización de los costes unido a un uso optimizado de los recursos, incluyendo la externalización de varios o todos los procesos de gestión de la empresa, y por otro, el uso de equipamientos y tiempos de trabajo por parte de los empleados para actividades particulares.

Para ambas perspectivas, los órganos directivos de las PYMES deberán analizar y tomar decisiones sobre cuáles, en qué plazos, con qué medios, para qué procesos y qué información y datos se tratarán con dichas tecnologías y herramientas, contemplando el uso de las mismas con parámetros económicos (costes, optimización), de recursos humanos (tiempo de dedicación, productividad) y desde el punto de vista de nuestro Estudio, conforme a los requisitos en materia de seguridad de los datos que establece la Propuesta de Reglamento UE de Protección de Datos en su artículo 30, debiendo implementar medidas técnicas, organizativas y legales para garantizar los niveles de seguridad adecuados a los datos que se traten.

Y es aquí cuando se le plantean nuevas problemáticas a las PYMES. En muchos casos las PYMES desconocen o no son capaces de analizar los riesgos a los que se enfrentan, o no tienen correctamente definidos los procesos internos para poder evaluar adecuadamente el impacto sobre la privacidad en el tratamiento de los datos y del uso de tales tecnologías, o por su tamaño no poseen la capacidad necesaria para poder negociar en un plano de igualdad los requisitos legales, los contratos y las salvaguardas necesarias con los encargados del tratamiento en los casos de Cloud Computing o externalización de procesos.

CONCLUSIONES

La Propuesta de Reglamento UE de Protección de Datos no se debe contemplar como una normativa más, ni como un obstáculo o reto (que lo es, no solo uno sino que representa múltiples retos), sino como una oportunidad, estratégica, para que se de a la Protección de Datos, a la Seguridad de la información y por lo tanto a la Privacidad, la importancia capital que debe tener en el “core” de nuestros negocios, ya que en palabras del director de la Agencia Española de Protección de Datos, D. José Luis Rodríguez Álvarez, *“sin protección de datos no hay confianza y sin confianza no habrá un desarrollo sólido de la economía digital”*.

Por lo tanto, la Propuesta de Reglamento puede significar requisitos que es posible convertir en oportunidades:

Oportunidad, de afrontar el análisis de los sistemas de información en los procesos de negocio; qué información, “los datos”, tenemos en ellos, cómo los obtenemos, cómo los tratamos, cuál es el flujo de los mismos a través de los distintos departamentos y procesos de la organización, cómo debemos analizarlos, tratarlos, salvaguardarlos y llegado el caso, destruirlos.

Oportunidad, de formar a los integrantes de las organizaciones del valor que representa la información, “los datos”, para el desarrollo de los negocios.

Oportunidad, de optimizar recursos, de aprovechar las ventajas tecnológicas teniendo un conocimiento preciso de la información, “los datos”, que la organización posee, dónde, cuándo, con qué medios o de qué manera es manejada.

Oportunidad, para que, tras la aprobación, con las modificaciones que resulten, o la no aprobación de la Propuesta de Reglamento UE de Protección de Datos, junto las situaciones de ataque a la privacidad de los últimos meses, se tome la adecuada conciencia de la importancia de la privacidad, los riesgos alrededor de ella y que se sepa transmitir desde la empresa mediante las medidas legales, técnicas y organizativas el valor añadido que supone la preservación de la privacidad, “los datos”.

Oportunidad porque será la clave para conocer y entender los procesos de negocio y sus interacciones, pudiendo obtener la información correcta en el momento oportuno. Para ello, se necesitará conocimiento y dedicación de la dirección y del personal y compromiso con los procesos, procedimientos y tecnologías que nos ayuden a implementar las mejores prácticas para gestionar “los datos”, y por lo tanto “los datos personales” de clientes, empleados, socios, personal de contacto, proveedores, etc., que se encuentren en los sistemas de información.

En definitiva, las obligaciones de las PYMES, como Responsables del tratamiento, se verán modificadas sustancialmente ya que, entre otras cuestiones, deberán añadir políticas internas para dar cumplimiento a los principios de “Privacidad desde el diseño” y “Privacidad por defecto”, revisar profundamente sus Documentos de seguridad y aplicar medidas de seguridad en base a una evaluación de riesgos inicial seguida, en algunos casos, de una evaluación de impacto relativa a la Protección de datos de las operaciones de tratamiento previstas. Todo

Reflexiones sobre el futuro de la Privacidad en Europa

esto supondrá un aumento de la burocracia y un esfuerzo para las PYMES que tendrá que ser dirigido y tratado de forma específica por la Comisión.

Una vez superado el gran reto de adaptación al nuevo Reglamento, se habrá conseguido una gestión de la seguridad (de los datos personales) basada en riesgos, tal y como siguen los códigos de buenas prácticas para sistemas de gestión de seguridad de la información (SGSI) tales como la ISO/IEC 27002.

The background of the slide features the European Union flag, which consists of a blue field with twelve five-pointed gold stars arranged in a circle. The flag is shown with a slight wave and is partially obscured by a bright, glowing light source in the lower-left quadrant. From this source, several white light rays extend diagonally upwards and to the right, creating a sense of movement and focus. The overall color palette is dominated by the deep blue of the flag and the bright white of the light rays.

Cap. 2
Privacy Impact Assessment
y
Privacy by Design

ABSTRACT

En este bloque del estudio, se profundizará en dos conceptos esenciales y totalmente novedosos; los informes de impacto en privacidad y la privacidad por diseño.

Un PIA (Privacy Impact Assessment) debe ser parte integral del diseño de cualquier iniciativa que pueda plantear riesgos relevantes en la privacidad. Es una forma de gestión de riesgos, que sirve para identificar y mitigar riesgos en privacidad en la fase inicial de un proceso de desarrollo de un programa o sistema y debe incardinarse en el proceso de gestión de riesgos de la compañía.

La Privacidad por Diseño o Privacy by design (en adelante PbD, por sus siglas en inglés) promueve una cultura proactiva en la protección de los datos personales. Privacidad como leitmotiv en la construcción de software y en la ejecución de procesos de negocio y soporte de cualquier organización. Este concepto fue ideado y promocionado por Ann Cavoukian, Comisaria de Información y Privacidad de Ontario, Canadá.

DESARROLLO

PRIVACY BY DESIGN. OBJETIVOS Y PRINCIPIOS

Los objetivos de PbD son: (1) para los ciudadanos, asegurar la privacidad y obtener el control personal de su información y, (2) para las organizaciones, una ventaja competitiva sostenible.

Para alcanzar dichos objetivos, se proponen los siguientes **7 Principios Fundamentales** basados en las publicaciones de la Comisión de Información y Privacidad de Ontario:

1. **Proactividad versus Reactividad; Enfoque Preventivo versus Correctivo.** PbD requiere de una actuación positiva y con carácter *ex ante* por parte de las organizaciones, orientada a hacer prevalecer la privacidad del usuario y su libertad de elección.
2. **Privacidad como configuración por defecto:** Los datos personales estarán protegidos automáticamente en cualquier sistema de información o en cualquier proceso de negocio.
3. **Privacidad Integrada en el Diseño:** PbD debe estar integrada en el diseño y arquitectura de los sistemas de TI y en los procesos de negocio. La privacidad se convierte en un elemento esencial de la funcionalidad.
4. **Funcionalidad Total – “Suma Positiva”:** Privacidad como activo para el negocio. En contraposición de una visión en la cual una de las partes debe perder para que la otra gane (suma cero) – por ejemplo, asumiendo que hay que ceder privacidad para ganar seguridad. Minimizando la posible dicotomía entre privacidad y seguridad.
5. **Seguridad Punto-a-Punto. Protección Completa del Ciclo de Vida de los Datos:** garantizando una administración segura del ciclo de vida de la información desde el inicio hasta el final.
6. **Visibilidad y Transparencia. Mantenerlo Abierto:** Objetivos, políticas y procedimientos de privacidad claramente establecidos y accesibles para los usuarios, así como verificables por estos o por terceras partes.
7. **Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario:** Por encima de todo, PbD requiere mantener el interés de los usuarios en una posición prioritaria, ofreciéndoles por defecto medidas robustas de privacidad, notificaciones apropiadas y facilitando opciones amigables para el usuario.

INICIATIVAS DE LA INDUSTRIA:

1. PET: Privacy Enhancing Technologies

Nuestra legislación actual ya contemplaba la necesidad de que cualquier tecnología o proceso de negocio destinado a tratar datos personales contemplara los necesarios requisitos de seguridad, dentro del Título VIII del RLOPD.

Las Privacy Enhancing Technologies (PETs) o tecnologías orientadas a mejorar la privacidad, comprenden los sistemas de información, las comunicaciones y los servicios que per-

miten al usuario proteger la privacidad de su información, controlando el acceso a sus datos y evitando el procesamiento innecesario, facilitando el cumplimiento de los requerimientos de privacidad sin perder funcionalidad. Las PETs proporcionan ayuda al usuario para poder controlar y ejercer sus derechos de privacidad, buscando proporcionar: anonimato o pseudonimia, inobservabilidad e imposibilidad de vinculación

2. ¿Qué está haciendo la industria del software?

Muchos fabricantes de software como Microsoft o IBM, entre otros, concienciados con la necesidad de proteger la privacidad de los usuarios, han desarrollado tecnologías para proteger y para gestionar la privacidad, los Privacy - Identity Management System son ejemplos de tecnologías en auge cuya finalidad es preservar la privacidad del usuario, proporcionándole la capacidad de controlar sus datos personales y negociar los términos de uso.

Por lo general, los fabricantes están haciendo que sus herramientas incorporen funcionalidades como las siguientes:

- Recopilación de los mínimos datos necesarios.
- Evitar el uso o el procesamiento innecesario de datos personales sin pérdida de funcionalidad del sistema de información.
- Ejercer el control de acceso a los datos para el propósito establecido y para los usuarios y procesos autorizados.
- Proporcionar el acceso parcial o totalmente anónimo.
- Cifrar información.
- Consentimiento informado del acceso a los datos personales.
- Negociar la aplicabilidad de la política de privacidad de acceso a los datos con el usuario y su implementación.
- Registro, trazabilidad y cumplimiento.

Otro ejemplo lo tenemos en OASIS (Organization for the Advancement of Structured Information Standards), Comité Técnico dedicado a impulsar el desarrollo, convergencia y adopción de estándares abiertos para la sociedad global de la información. Algunos de los estándares impulsados por OASIS están orientados a proteger la privacidad del usuario sirviendo de referencia para la implementación de políticas de seguridad y privacidad, animando a las organizaciones a incluir la privacidad en el diseño y en la arquitectura.

Algunas de sus publicaciones están dedicadas totalmente a la privacidad de datos:

- OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC
- OASIS Privacy Management Reference Model (PMRM) TC

RELACIÓN PbD y PIAs

La Privacidad por Diseño parte del supuesto de que para su puesta en marcha se han realizado PIAs sobre la información, finalidades del tratamiento de datos, los sistemas de información y demás medios que intervendrán en el tratamiento.

En este sentido, la implementación de PbD en todos los ámbitos de una organización podría conllevar la realización de varios PIAs, en función de la complejidad de las finalidades de tratamiento, los datos personales que son tratados en relación con cada finalidad y la propia actividad de negocio.

Los conceptos de Privacy by Design, Privacy by Default y Privacy Impact Assessment implican la necesidad de implantar unos criterios de gestión de riesgos y de considerar los aspectos de privacidad desde su concepción.

Se trata de cambiar la forma en cómo las organizaciones se enfrentan al respeto a la privacidad, convirtiéndolo en algo proactivo y no reactivo, focalizándose en la prevención de forma efectiva y eficaz.

METODOLOGÍA

En cualquier organización todos tienen una responsabilidad directa o indirecta en relación con la privacidad. Sin embargo, debe reconocerse que la identificación de quiénes tienen a su cargo dicha responsabilidad puede ser una tarea compleja. En este sentido y para ayudar en esta tarea, la Comisión de Información y Privacidad de Ontario propone el siguiente modelo:



Fuente: Foundational Principles. Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Ann Cavoukian, Ph.D. Information and Privacy Commissioner, Ontario, Canada. December 2012 (La traducción es nuestra).

Del mismo modo, para ayudar a los interesados en su aplicación, ha desarrollado una "Guía de Implementación" en la que explica las "acciones" requeridas para implementar los 7 principios de PbD, que pueden resumirse de la siguiente forma:

Principio 1. Proactivo, no Reactivo; Preventivo no Correctivo

Objetivo	Acciones	Responsables
Anticipar y evitar incidentes	<ol style="list-style-type: none"> 1. Programa de privacidad sólido y proactivo fomentado por la Alta Dirección. 2. Integración de la privacidad en el resto de procesos y operaciones de la organización. 3. Métodos sistemáticos para evaluar riesgos de privacidad y seguridad. 4. Fomentar prácticas de privacidad probadamente compartidas por diversas comunidades de usuarios e interesados, en una cultura de mejora continua. 	<p style="text-align: center;">Alta Dirección</p> <p>(Consejo de Administración, CEO, CPO, CIO, COO, CSO, propietarios).</p>

Principio 2. La Privacidad como configuración por defecto

Objetivo	Acciones	Responsables
Garantizar la privacidad de los usuarios de manera automática	<ol style="list-style-type: none"> 1. Finalidades específicas y concretas. 2. Minimizar la recogida de datos únicamente a lo estrictamente necesario. 3. Limitar el uso de los datos personales a la finalidad para la cual fueron recabados. 4. Políticas y procedimientos que eviten fugas de datos. 	<p>Ingenieros de software. Responsables funcionales Responsables de procesos y/o negocio</p>

Principio 3. Privacidad Integrada en el Diseño

Objetivo	Acciones	Responsables
Garantizar que la privacidad se convierte en un componente esencial de la funcionalidad.	<ol style="list-style-type: none"> 1. Realizar PIAs en la etapa de diseño de cualquier iniciativa. 2. Procesos y sistemas de gestión de la identidad 3. Privacidad en el ciclo de vida del software y de los procesos de negocio. 4. Integrar la privacidad en los objetivos normativos, (leyes sectoriales, legislación general, etc.) desde un enfoque guiado por "la flexibilidad, el sentido común y el pragmatismo". 	<p>Responsables funcionales Responsables de procesos y/o negocios Ingenieros de software Reguladores</p>

Principio 4. Funcionalidad Total – “Suma Positiva”, no “Suma Cero”

Objetivo	Acciones	Responsables
Minimizar la posible dicotomía entre privacidad y seguridad	<ol style="list-style-type: none"> 1. Reconocer que diversos y legítimos intereses de negocios deben coexistir. 2. Conocer, participar y asociarse para comprender mejor los múltiples, y a veces divergentes, intereses involucrados. Practicar las 3 Cs: comunicación, consulta y colaboración. 3. Perseguir soluciones y opciones innovadoras para conseguir funcionalidades múltiples. 	<p>Alta Dirección Responsables funcionales Responsables de procesos y/o negocios Ingenieros de software</p>

Principio 5. Seguridad Punto-a-Punto. Protección Completa del Ciclo de Vida de los Datos

Objetivo	Acciones	Responsables
Protección del dato en todo su ciclo de vida	<ol style="list-style-type: none"> 1. Implantar soluciones de cifrado de datos. 2. Asegurar la destrucción y eliminación segura de los datos personales al final de su ciclo de vida. 	<p>Ingenieros de software Responsables funcionales Responsables de procesos y/o negocios</p>

Principio 6. Visibilidad y Transparencia. Mantenerlo Abierto

Objetivo	Acciones	Responsables
Cumplimiento de las políticas de privacidad	<ol style="list-style-type: none"> 1. Identificación de responsables de contacto en materia de privacidad. 2. Políticas y procedimientos accesibles y en lenguaje sencillo comprensible para cualquier usuario. 3. Publicación de extractos de PIAs así como el resultado de auditorías o certificaciones de seguridad. 4. Hacer disponible una lista de las bases de datos personales que conserva en su organización. 	Alta Dirección Ingenieros de software Arquitecto de sistemas

Principio 7. Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario

Objetivo	Acciones	Responsables
Protección y funcionalidad centrada en el usuario	<ol style="list-style-type: none"> 1. Opciones de privacidad configuradas por defecto. 2. Proporcionar información adecuada al usuario. 3. Adoptar opciones amigables con el usuario: <ol style="list-style-type: none"> a) Mantener las preferencias de los usuarios b) Proporcionar a los usuarios acceso a sus propios datos. c) Permita el acceso a las prácticas de gestión de la información de su organización. 	Alta Dirección Ingenieros de software Responsables funcionales Responsables de procesos y/o negocios

ELABORACIÓN DE INFORMES DE IMPACTO DE PRIVACIDAD

CONCEPTO PIA

La Propuesta de Reglamento europeo de Protección de Datos publicada por la Comisión el 25 de enero de 2012, regula en su art. 33 la evaluación de impacto relativa a la protección de datos estableciendo la obligación de que los Responsables y Encargados del Tratamiento lleven a cabo una evaluación de impacto de la protección de datos (conocida internacionalmente como PIA o Privacy Impact Assessment) cuando existan riesgos específicos para los derechos y libertades de los interesados con motivo de su naturaleza, alcance o fines. Y se detallan las operaciones de tratamiento que entrañan riesgos específicos.

Por tanto, procede a continuación analizar qué es un PIA y para qué sirve.

Se puede definir a un PIA como un proceso o metodología para determinar los riesgos o impactos que una propuesta o proyecto tiene en la privacidad de los individuos así como para determinar los medios o soluciones para mitigar o evitar dichos riesgos o impactos negativos.

Un PIA consiste en una identificación y evaluación, con mayor o menor profundidad, de los potenciales riesgos y efectos que en los aspectos y requerimientos de privacidad podrían tener nuevos servicios, operaciones, procesos, proyectos, programas, iniciativas, políticas, sistemas, productos o tecnologías, dado que implican tratamientos de datos personales y produce como resultado una respuesta sobre si se aceptan, mitigan o evitan dichos riesgos identificando las soluciones o medios correspondientes.

Un PIA puede ayudar a una organización a ganarse la confianza del usuario en que la privacidad ha sido tenida en cuenta desde el diseño del proyecto, tecnología o servicio. Demuestra que esa organización considera la privacidad una prioridad.

Es un proceso que debería comenzar lo más pronto posible cuando todavía hay oportunidad para influenciar en el diseño y detalles finales del proyecto en cuestión. Los costes de hacer cambios aumentan cuanto más tarde se realicen en un proyecto.

EXPERIENCIA INTERNACIONAL

Actualmente hay diferentes países, Estados y regiones (caso de disponer de Autoridad de control propia en materia de Protección de Datos) donde se vienen utilizando los PIAs. Existen estudios comparativos entre ellos con un alto nivel de granularidad en el detalle de sus especificaciones y contenido. Por citar dos de ellos:

- “A Privacy Impact Assessment Framework for data protection and privacy rights” En él se analizan los diferentes PIAs según las directrices que marca su correspondiente autoridad de control.
- “An Evaluation of Privacy Impact Assessment Guidance Documents”. Es interesante porque los clasifica en tres grupos en función de su calidad, con la prevención de que dicha clasificación está sujeta a interpretación y puede variar en el transcurso del tiempo:
 - **Grupo 1. Calidad insuficiente:** Forman parte de él USA y todos sus estados, Canadá y todas sus provincias (a excepción de Ontario y Alberta) y todos los Estados australianos (excluyendo Victoria).
 - **Grupo 2. Calidad moderada:** Engloba a Nueva Zelanda, Australia y Hong Kong.
 - **Grupo 3. Alta calidad:** Lo constituyen, en orden cronológico de su publicación Ontario y Alberta de Canadá, Inglaterra y Victoria de Australia.

TIPOS DE PIAs

Existen diferentes tipos de PIAs en función del alcance perseguido: por colectivo de usuarios, tipología de información, sistema de información o un proceso de negocio.

La experiencia inglesa a través de las directrices del ICO (Information Commissioner’s Office), que es su Autoridad de control en materia de protección de datos, habla de dos tipos concretos de PIA: El Full-scale PIA (PIA a escala completa) y el Small-scale PIA (PIA a pequeña escala), menos formal que el anterior y a menudo empleado cuando únicamente se focalizan aspectos específicos del proyecto.

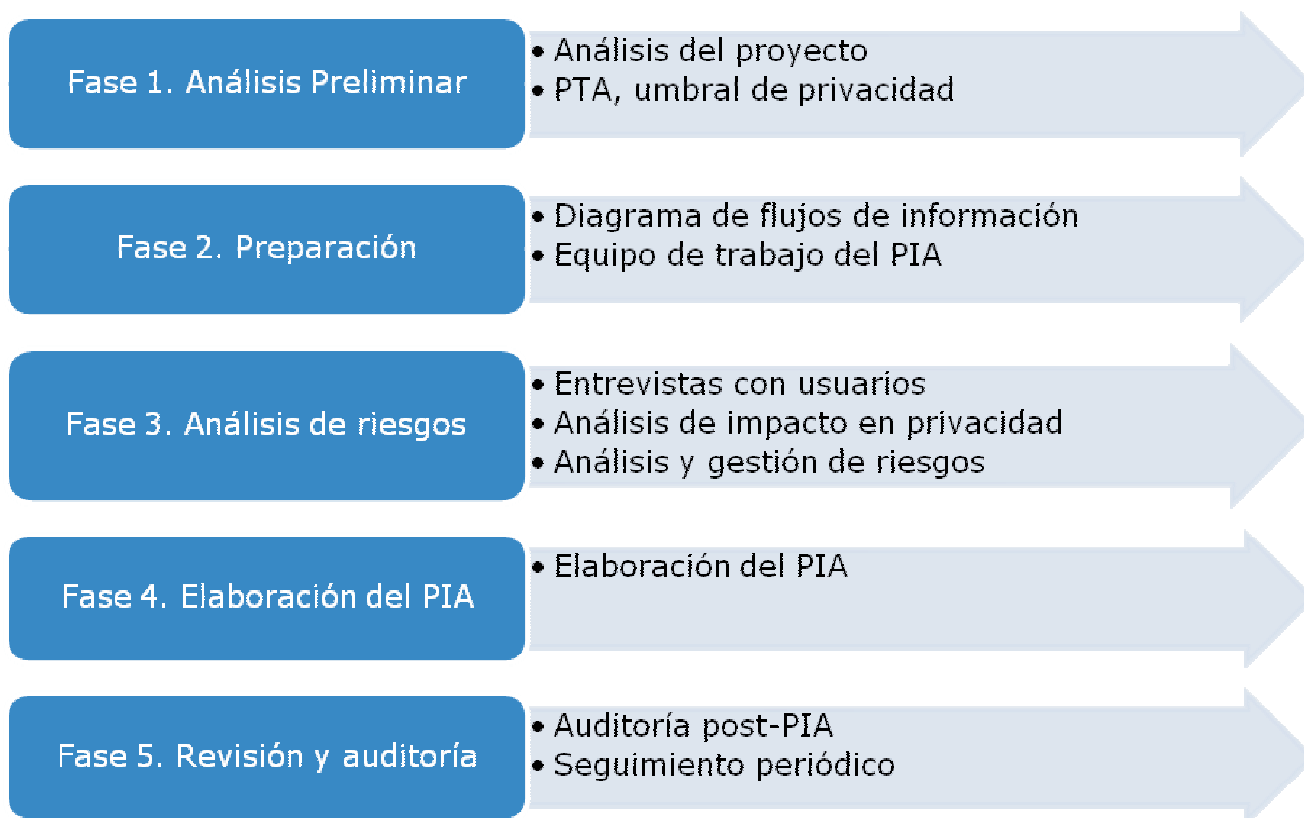
Un PIA lo podrá efectuar el DPO (Data Protection Officer), un profesional externo o un equipo de profesionales. La pregunta que surge es ¿cómo saber a priori, si no disponemos de DPO, si es necesario efectuar un PIA (completo o reducido) o bien podemos prescindir de él debido a la naturaleza de los datos tratados?

Para ello se podrá realizar un PTA (Privacy Threshold Analysis – análisis de umbral de privacidad), que consiste en un análisis previo que nos permitirá determinar si es necesario realizar un PIA completo o reducido. El PTA será el primer análisis a realizar a lo largo del PIA.

METODOLOGÍA

No existe una metodología estándar, internacionalmente reconocida, para elaborar un PIA. Sin embargo, de la experiencia de diferentes países donde viene utilizándose desde hace algún tiempo, se puede extraer una forma de hacer común que ha dado buenos resultados.

Las diferentes actividades que constituyen el proceso de elaborar un PIA, pueden dividirse en cinco fases como recomienda el ICO para el full-scale PIA. Se resumen en la siguiente ilustración.



A continuación se describe esta metodología.

Fase 1. Análisis preliminar

La finalidad de ésta fase es verificar si efectivamente es necesario el PIA, en cuyo caso se establece una base para poder elaborarlo con eficacia y eficiencia. Está constituida por dos actividades:

- **Análisis del proyecto:** Recopilación y análisis de toda la información relacionada con el proyecto.
- **PTA (Privacy Threshold Analysis).** Su umbral nos orientará sobre el nivel de detalle necesario en las diferentes actividades del PIA.

Fase 2. Preparación

Está constituida por dos actividades:

- **Diagramas de flujos de información:** Se crean los diagramas y describen los flujos de información de naturaleza personal del proyecto.

- **Equipo de trabajo del PIA:** En función de la magnitud del proyecto, se constituirá un PCG (PIA Consulting Group – Grupo consultor del PIA), normalmente multidisciplinar que se encargará de apoyar en el desarrollo del PIA.

Fase 3. Análisis de riesgos

Entrevistas con las partes interesadas, un análisis de riesgos y la búsqueda de soluciones que permitan mitigar los riesgos identificados. Está constituida por tres actividades:

- **Entrevistas con usuarios:** Se recopila toda la información de detalle en el proyecto desde diferentes puntos de vista en el ámbito de la privacidad.
- **Análisis de impacto en la privacidad:** Se identifican las vulnerabilidades del proyecto y se analiza su impacto en la privacidad. Para ello podemos basarnos en los **IPP (Information Privacy Principles)**, que encontramos en algunas legislaciones de protección de datos que vienen utilizando PIAS (Inglaterra - Data Protection Act 1998, Schedule 1, p. 80 y siguientes, Victoria, Nueva Zelanda).
- **Análisis y Gestión de riesgos:** Partiendo del anterior análisis de impacto, se evalúa la probabilidad de que las amenazas sobre la privacidad se materialicen y se propone una estrategia de gestión (mitigación, eliminación o aceptación justificada del riesgo).

Fase 4. Elaboración del PIA

Se trata de un informe que detalle todas las etapas anteriores y finaliza con un apartado de conclusiones y recomendaciones.

Fase 5. Revisión y auditoría

El propósito de esta fase es asegurar que las nuevas características de diseño que surgen del PIA se implementen y sean efectivas. Está constituida por dos actividades:

- **Auditoría post-PIA:** Se trata de revisar el proyecto para asegurar que se incorporen en el diseño las recomendaciones del PIA.
- **Seguimiento periódico:** Se tendrá en cuenta el Ciclo de Vida del proyecto, ajustando el PIA a las futuras variaciones del mismo

CONTENIDO DE UN PIA

PROPUESTA DE CONTENIDO DE UN PIA			
Apartado	Sec	Subapartado	Consultar fase en metodología
Identificación de la organización	1.1	Datos identificativos	
	1.2	Actividad	
	1.3	Visión, misión, valores	
	1.4	Entorno de control de la privacidad	
Identificación del proyecto	2.1	Visión de conjunto	De la FASE 1 (Análisis preliminar)
	2.2	Objetivos	
	2.3	Alcance	
	2.4	Vínculos con otros proyectos	
Descripción del proyecto y flujos de información	3.1	Detalles del proyecto	De la FASE 2 (Diagramación de flujos de información)
	3.2	Diagrama de flujos de información	
	3.3	Recogida de información personal	
	3.4	Tratamiento información personal	
	3.5	Cesiones de información personal	
	3.6	Calidad de los datos	
	3.7	Seguridad de los datos	
	3.8	Acceso y Rectificación	
Análisis de privacidad	4.1	En la recogida	De la FASE 3 (Análisis de impacto en la privacidad)
	4.2	En los tratamientos	
	4.3	En las cesiones	
	4.4	En la retención y destrucción	
	4.5	En la calidad de los datos	
	4.6	En la seguridad de los datos	
	4.7	En el acceso y rectificación	
Evaluación de riesgos de privacidad	5.1	En el recabado	De la FASE 3 (Análisis y Gestión de Riesgos)
	5.2	En los tratamientos	
	5.3	En las cesiones	
	5.4	En la retención y destrucción	
	5.5	En la calidad de los datos	
	5.6	En la seguridad de los datos	
	5.7	En el acceso y rectificación	
Hallazgos y recomendaciones	6.1	Resumen de hallazgos	
	6.2	Recomendaciones	
CONCLUSIONES	7.1	Conclusiones finales	
	7.2	Plan de actuación y auditoría	

CONCLUSIONES

Un PIA debe ser parte integral del diseño de cualquier iniciativa que pueda plantear riesgos relevantes en la privacidad. Una vez que los riesgos se han identificado, se pueden entonces implementar las salvaguardas y controles necesarios para eliminar o minimizar los riesgos. El objetivo de un PIA es evitar que aparezcan los problemas y, por tanto, evitar gastos y *trastornos* posteriores, dado que los costes de hacer cambios aumentan cuanto más tarde se realicen en un proyecto.

La Propuesta de Reglamento Europeo de Protección de Datos aumentará considerablemente la utilización de los PIAs en Europa, lo que traerá importantes beneficios para todos: organizaciones, ciudadanos, reguladores, etc. Debemos celebrar que se incluyan disposiciones normativas que incentiven a los responsables a implicarse, desde el principio, en una adecuada protección de los datos, y las evaluaciones de impacto sobre protección de datos contribuirán notablemente a ello.

BIBLIOGRAFÍA / REFERENCIAS

Dirección General de Justicia de la Comisión Europea - A Privacy Impact Assessment Framework for data protection and privacy rights (2011), <http://www.piafproject.eu/Deliverables.html>

International Data Privacy Law 1, 2 (p 111-120) - An Evaluation of Privacy Impact Assessment Guidance Documents (2011), <http://www.rogerclarke.com/DV/PIAG-Eval.html>

Information Commissioner's Office - Privacy Impact Assessment Handbook version 2.0 (2009)
http://www.ico.org.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

Office of the Victorian Privacy Commissioner - Privacy Impact Assessments (2009), .

Office of the Victorian Privacy Commissioner - Information Privacy Principles "

Privacy Commissioner - Information Privacy Principles, <http://www.privacy.org.nz/news-and-publications/guidance-notes/information-privacy-principles/>

ISACA Journal Online - Haris Hamidovic - An Introduction to the Privacy Impact Assessment Based on ISO 22307 (2010)

National Institute of Standards and Technology - SP800-53 Rev.4. Security and Privacy Controls for Federal Information Systems and Organizations (2013), "

Information & Privacy Commissioner -Ontario, Canada - Privacy by Design. Los 7 Principios Fundamentales (2001),
<http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf>

Ann Cavoukian / Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices (2012),
<http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf>

Information Commissioner's Office - Privacy by Design Report (2008)
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~media/document_s/pdb_report_html/PRIVACY_BY_DESIGN_REPORT_V2.ashx

Information Commissioner's Office - Privacy by Design Implementation Plan (2008),
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~media/document_s/pdb_report_html/PBD_ICO_IMPLEMENTATION_PLAN.ashx

Privacy Impact Assessments. Office of The Privacy Commissioner of Canada,
http://www.priv.gc.ca/resource/pia-efvp/index_e.asp

Privacy Impact Assessment Guide. - Office of the Australian Information Commissioner.
<http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide>

Privacy Impact Assessment Handbook. Privacy Commissioner. Nueva Zelanda. <http://www.privacy.org.nz/news-and-publications/guidance-notes/privacy-impact-assessment-handbook/>

Estados Unidos. Privacy Office - Privacy Impact Assessments (PIA). U.S. Department of Homeland Security. <http://www.dhs.gov/privacy-office-privacy-impact-assessments-pia>

Victoria (Australia). Office of the Victorian Privacy Commissioner – Privacy Impact Assessments – a guide <https://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-guide>

Privacy Impact Assessment Policy. . Treasury Board of Canada Secretariat http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist-eng.asp

Privacy Impact Assessments: the UK experience:

Privacy and Data Protection Impact Assessment. Framework for RFID Applications. (2011)

Assuring Data Privacy Compliance. Steve Kenny. <http://www.isaca.org/Journal/Past-Issues/2004/Volume-4/Pages/Assuring-Data-Privacy-Compliance.aspx>

Privacy Impact Assessments: International Study of their Application and Effects. October, 2007, Linden Consulting, Inc. Prepared for Information Commissioner's Office United Kingdom

The International Standards on the Protection of Personal Data and Privacy ("The Madrid Resolution") (2009) http://www.privacyconference2009.org/media/Publicaciones/com-mon/estandares_resolucion_madrid_en.pdf

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

OASIS Privacy Management Reference Model (PMRM) TC

<http://pet-portal.eu/>

<https://www.facebook.com/privacypage>


http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

<http://pet-portal.eu/>

ISO 31000:2009. Evaluación de Riesgos.

ISO 27005:2008. Information security risk management.

ISO 22307:2008. Financial Services – Privacy Impact Assessment.

The background of the slide features the European Union flag, which consists of a blue field with twelve five-pointed gold stars arranged in a circle. The flag is slightly blurred and appears to be waving. Overlaid on the bottom half of the flag are several bright, white, diagonal light rays that create a sense of motion and focus. The overall color palette is dominated by the blue of the flag and the white of the light rays.

Cap. 3
Data Privacy Officer:
perfil, formación,
posición,
competencias y
operativa.

LA FIGURA DEL DPO

ABSTRACT

Trataremos en este apartado de dar respuesta a quién es la persona adecuada para el desempeño de las funciones que la Propuesta de Reglamento Europeo de Protección de Datos contiene en relación a la figura del Data Protection Officer o Delegado de Protección de Datos (en adelante DPO).

Así, se tratará el tema del perfil del DPO, o más bien del candidato idóneo a serlo, con relación a aspectos tales como formación, experiencia, certificaciones, etc., tanto para el caso de que sea interno como para cuando sea externo. Se hablará igualmente de sus competencias y capacidades, haciendo una propuestas específica fundamentada tanto en el texto de la Propuesta de Reglamento como en otras fuentes.

Posteriormente, será el tema de la Posición del DPO en el organigrama de las organizaciones públicas y privadas el que ocupe parte de este apartado, siempre bajo el requisito previo de que cualquier ubicación de esta figura dentro de la jerarquía interna debe garantizar su autonomía.

Por último, se analizarán las posibles funciones y obligaciones del DPO, en base a la Propuesta y también en comparación con la figura del Responsable de Seguridad que establece la Normativa española. Además, se incluirá un cuadro comparativo de diferentes países europeos, en cuanto a su enfoque respecto a figuras similares a la que podría ser la del DPO.

PERFIL DEL DPO

El artículo 35 (en el borrador de la Comisión publicado en enero de 2012) establece la obligatoriedad de designar un DPO en determinados supuestos, figura que tiene su origen en la Directiva 95/46/CE. No obstante, durante la Presidencia Irlandesa de la Unión Europea (primer semestre de 2013), se ha presentado la versión de Borrador del Consejo de la Unión Europea, que parece rebajar la obligatoriedad de tal designación a opcional, si bien en dicho documento se especifica que la legislación de la Unión Europea podrá hacer obligatoria la mencionada designación.

En cuanto al perfil que debería reunir un candidato idóneo para ser nombrado DPO, que podrá ser trabajador por cuenta ajena, desempeñar sus servicios bajo un contrato de prestación de servicios o ser una persona jurídica, el artículo 35.8 de la Propuesta, en su punto 2, determina que:

“El responsable o el encargado del tratamiento designarán el delegado de protección de datos atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar las tareas contempladas en el artículo 37. El nivel de conocimientos especializados requerido se determinará, en particular, en función del tratamiento de datos llevado a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado del tratamiento.”

El texto, no hace más mención al perfil que deba reunir la persona que desarrolle esa función, hasta el punto que el propio Grupo de Trabajo del Artículo 29 (GT 29), en su Dictamen 08/2012 (WP199), recomienda que la Comisión, mediante un acto delegado, *“especifique los criterios aplicables a las cualidades profesionales, en líneas generales, del delegado de protección de datos”*.

Por lo que se refiere a las principales tareas que el DPO deberá realizar, según el artículo 37, tal figura debe contar con *“conocimientos especializados de la legislación y las prácticas en materia de protección de datos”*. Esto nos lleva a los requerimientos de formación que puedan ser exigibles. Parece imprescindible que esta persona cuente con una sólida formación en materia de normativa sobre privacidad, pero no sólo en este campo, sino también en el de la gestión de la seguridad de la información, amén de un profundo conocimiento del sector en el que la organización opere y, por supuesto, de la citada organización.

Puesto que una de sus principales tareas será formar y concienciar al personal en la materia que nos ocupa con el objetivo de conseguir un eficaz y completo despliegue de medidas técnicas y/u organizativas, el DPO debe contar con notables habilidades de comunicación. Esta cualidad –la facilidad para comunicar– también le será muy útil al relacionarse tanto con los usuarios que así lo deseen, como con la propia dirección a la que tendrá que transmitir la situación del cumplimiento en la materia. Y no menos importantes serán sus funciones de documentalista, por lo que no estará de más que conozca cómo funciona un sistema de gestión.

Qué duda cabe que esta formación -unida a la experiencia- será deseable que se pueda contrastar, para lo cual, podrá acudir a las certificaciones profesionales. En nuestro país comienzan a proliferar estas certificaciones en privacidad, siendo las más extendidas en el momento actual, la CDPP promovida por el ISMS Fórum Spain y la ACP promovida por la Asociación Profesional Española de Privacidad. En la XI Jornada Internacional de Primavera de 2012 organi-

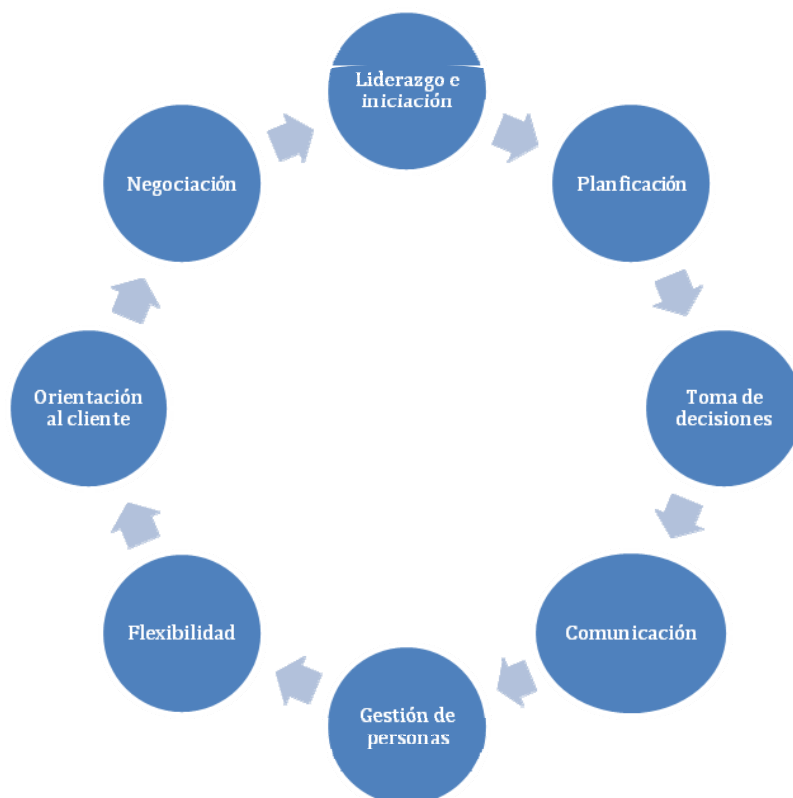
zada por el ISMS Fórum Spain en Madrid, el Supervisor Europeo de Protección de Datos, Peter Hustinx, ya afirmó que no le cabía duda de la utilidad que las certificaciones aportarían a los profesionales y a las empresas que los reclamaran, pero dejó claro que las certificaciones deberán ser homologadas por alguna Autoridad de Control.

Asimismo, y dado que entre las funciones que se asignan a esta figura está la de *“supervisar la implementación y aplicación del presente Reglamento, en particular por lo que hace a los requisitos relativos a la protección de datos desde el diseño, la protección de datos por defecto y la seguridad de los datos”*, parece recomendable, que en ausencia de certificaciones específicas y homologadas en materia de protección de datos, se valoren las certificaciones reconocidas con carácter internacional en materia de seguridad de la información (CISA/CISM de ISACA, Lead Auditor ISO27001 del BSI, etc.).

En lo referente a sus habilidades, deberíamos tener en cuenta que por el grado de independencia que se le exige, ocupará una posición de staff que reportará a algún alto directivo de la organización.

Por lo tanto, parece lógico que reporte directamente a la Dirección General o la Gerencia de la Organización, y es posible que desarrolle un rol directivo. En la asunción de este rol, la resolución de problemas, la toma de decisiones y la comunicación son actividades críticas. En cada etapa que desarrolle, ya sea planificando, organizando o controlando, necesitará estas habilidades. Puesto que trabajará por medio de otras personas y, en continua relación será necesario que sea una persona con buenas habilidades sociales.

En consecuencia, es recomendable que la figura del DPO cuente con las siguientes competencias y capacidades específicas:



Por último, la experiencia requerida para el desempeño del puesto debería ser valorada en base a las funciones a desarrollar, así como en lo que respecta a la participación en proyectos de consultoría y/o auditoría en materia de protección de datos, elaboración de análisis de impactos (Business Impact Assessments o BIAs), así como proyectos de análisis de riesgos.

En este sentido, la experiencia debería cuantificarse en función de la complejidad de los tratamientos de datos que realice el Responsable del fichero, del sector en el que opere y del grado de sensibilidad que puedan incorporar los datos tratados.

POSICIÓN DEL DPO

Una vez descrito en el apartado anterior el perfil del DPO, procede analizar la posición que puede o debe ocupar en el organigrama de las organizaciones, así como la independencia con la que debe contar en el desarrollo de sus funciones.

El apartado 1 del artículo 35 de la Propuesta de Reglamento lanzada por la Comisión regula en qué casos el responsable y el encargado del tratamiento deben designar un DPO:

- Cuando el tratamiento sea llevado a cabo por una autoridad u organismo públicos, si bien el apartado 3 del artículo 35, introduce cierta flexibilidad, ya que el DPO podrá ser designado para varias de sus entidades, teniendo en cuenta la estructura organizativa de la autoridad u organismos públicos.
- Cuando el tratamiento sea llevado a cabo por una empresa que emplee a doscientas cincuenta personas o más. El apartado 2 del citado artículo 35 aclara que en el caso de un grupo de empresas se podrá nombrar un DPO único.
- Cuando las actividades principales del Responsable o del Encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados.
- En casos distintos de los anteriores, el Responsable o el Encargado del tratamiento o las asociaciones y otros organismos que representen categorías de responsables o encargados podrán designar un DPO (apartado 4). Aquí se da vía libre a otras organizaciones para nombrar un DPO.

Al DPO se le exige independencia en sus funciones. Así, según el artículo 36.2 *“El Responsable o el Encargado del tratamiento velarán porque el Encargado de protección de datos desempeñe sus funciones y tareas con independencia y no reciba ninguna instrucción en lo que respecta al ejercicio de sus funciones. El delegado de protección de datos informará directamente a la dirección del Responsable o del Encargado del tratamiento”*.

De este precepto se desprende que el DPO no debería estar dentro de otra área de la empresa para poder cumplir con más rigor el requisito de independencia, y sobre todo, no ubicarse en el mismo departamento que el Responsable o el Encargado del tratamiento (Unidad de Negocio).

En consecuencia, podría encontrarse en el organigrama dependiendo de la Dirección General, pero no dentro de otras áreas o departamentos. Si existe en las empresas departamento de Cumplimiento Normativo, Seguridad de la Información (o similar), y se decide incluir ahí al De-

legado de Protección de Datos, deberá velarse en todo momento por su independencia.

Ligado a este estatus de independencia, el apartado 6 del artículo 35 añade que las funciones profesionales del DPO deben ser compatibles con sus tareas y funciones en calidad de Delegado de Protección de Datos y que no planteen conflictos de intereses, de lo que parece deducirse que sus funciones deberían ser únicamente de DPO.

Además el Responsable o el Encargado del tratamiento, a tenor de lo dispuesto en el artículo 36.3 respaldará al DPO en el desempeño de sus tareas y facilitará el personal, los locales, los equipamientos y cualesquiera otros recursos necesarios para el desempeño de sus funciones y tareas contempladas en el artículo 37, y que se tratarán en el siguiente apartado de nuestro estudio. Según este epígrafe podríamos interpretar que el DPO puede contar con personal a su cargo y/o estar formado por un grupo de personas para el desempeño de sus tareas.

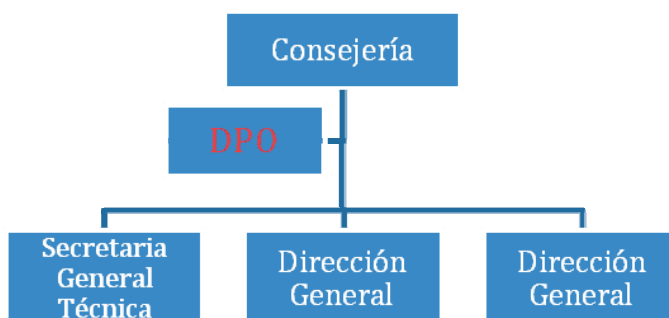
Asimismo, y en el caso de que se haya subcontratado al DPO, la organización no tendría en su organigrama este puesto, pero sí debería establecer qué persona o área de la organización se ocupará de facilitar información al Delegado, etc. Este hecho puede plantear algunos problemas de independencia especialmente en las PYMES.

A continuación, y de forma ilustrativa se muestra dónde podría quedar incluida la figura del DPO en las organizaciones que cuenten con él y no lo subcontraten.

- Entidades de más de 250 empleados:



- Entidades donde el tratamiento sea llevado a cabo por una autoridad u organismo públicos¹:



¹La estructura de las Administraciones públicas varía de unas a otras, aunque en la mayoría de los casos, tanto los Ministerios como las Consejerías, y en muchas ocasiones, también las Concejalías de los Ayuntamientos, comparten como elemento común la existencia de Direcciones Generales, a partir de las cuales se ejerce la competencia administrativa. Tomamos como ejemplo una ficticia Consejería, que se organiza en Direcciones General y que cuenta también con una Secretaría General Técnica.

Por otra parte, y sin perjuicio de su encaje en el organigrama de la organización, el DPO debe ser accesible a los titulares de los datos personales, ya que según el apartado 10 del artículo 35, *“los interesados tendrán derecho a entrar en contacto con el Delegado de Protección de Datos para tratar todas las cuestiones relativas al tratamiento de los datos que les conciernan y a solicitar el ejercicio de sus derechos”*. Por esta razón, y de conformidad con el apartado 9 del artículo 35 *“los datos de contacto del DPO, serán comunicados por el Responsable o por el Encargado del tratamiento a la Autoridad de Control y al público”* (artículo 35.9).

FUNCIONES Y OBLIGACIONES

Las funciones del DPO se encuentran reguladas en el artículo 37 de la Propuesta de Reglamento, si bien de su redacción, se extrae que no sólo se regula su competencia sino que supone un mandato tanto para el Responsable como al Encargado al incluirse que *“ambos encomendarán, como mínimo, las siguientes tareas”*.

Asimismo, debemos considerar que estas funciones son una regulación de mínimos –el texto indica que *“como mínimo”* tendrá las citadas competencias-. Incluso la delegación realizada en favor de la Comisión en el apartado 2 del artículo 37, podría llevar a un desarrollo más pormenorizado del ámbito de actuación del Delegado de Protección de Datos.

Antes de analizar cuáles son estas funciones, debemos acudir a dos documentos a través de los cuales se ha desarrollado el perfil de esta figura. El primero de ellos, es el Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de los datos, cuyo artículo 24 apartado 1, recoge las funciones del Delegado de Protección de Datos:

“1. Cada institución y cada organismo comunitario nombrará al menos a una persona para que actúe como responsable de la protección de datos encargado de:

- a) garantizar que los responsables del tratamiento y los interesados sean informados de sus derechos y obligaciones de conformidad con el presente Reglamento;*
- b) responder a las solicitudes del Supervisor Europeo de Protección de Datos y, en el marco de sus competencias, cooperar con el Supervisor Europeo de Protección de Datos a petición de éste o por iniciativa propia;*
- c) garantizar de forma independiente la aplicación interna de las disposiciones del presente Reglamento;*
- d) llevar el registro de aquellas operaciones de tratamiento realizadas por el responsable del tratamiento, el cual contendrá la información a que se refiere el apartado 2 del artículo 25;*
- e) notificar al Supervisor Europeo de Protección de Datos las operaciones de tratamiento que pudieran presentar riesgos específicos con arreglo al artículo 27. Dicha persona deberá velar por que el tratamiento no tenga efectos adversos sobre los derechos y las libertades de los interesados.”*

En este sentido, el Reglamento 45/2001 regula la figura del DPO en el ámbito de las instituciones y organismos comunitarios.

El segundo de los documentos, proviene del Supervisor Europeo de Protección de Datos, en el que fija su postura sobre el Reglamento anteriormente citado, y que también analiza las funciones, calificándolas de la siguiente manera:



En cuanto a lo que recoge la Propuesta de Reglamento, el apartado 1 del artículo 37 establece lo siguiente:

- “1. El responsable o el encargado del tratamiento encomendarán al delegado de protección de datos, como mínimo, las siguientes tareas:*
- a) informar y asesorar al Responsable o al Encargado del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y documentar esta actividad y las respuestas recibidas;*
 - b) supervisar la implementación y aplicación de las políticas del Responsable o del Encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;*
 - c) supervisar la implementación y aplicación del presente Reglamento, en particular por lo que hace a los requisitos relativos a la protección de datos desde el diseño, la protección de datos por defecto y la seguridad de los datos, así como a la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos en virtud del presente Reglamento;*
 - d) velar por la conservación de la documentación contemplada en el artículo 28;*
 - e) supervisar la documentación, notificación y comunicación de las violaciones de datos personales de conformidad con lo dispuesto en los artículos 31 y 32;*
 - f) supervisar la realización de la evaluación de impacto relativa a la protección de datos por parte del responsable o del encargado del tratamiento y la presentación de solicitudes de autorización o consulta previas, si fueran necesarias de conformidad con lo dispuesto en los artículos 33 y 34;*
 - g) supervisar la respuesta a las solicitudes de la Autoridad de Control y, en el marco de las competencias del delegado de protección de datos, cooperar con la Autoridad de Control a solicitud de esta o a iniciativa propia;*
 - h) actuar como punto de contacto para la Autoridad de Control sobre las cuestiones relacionadas con el tratamiento y consultar con la Autoridad de Control, si procede, a iniciativa propia.”*

Parte de estas funciones están, obviamente, influenciadas por el resto del texto normativo comunitario. Por ejemplo, el DPO tendrá que impulsar y controlar el cumplimiento del principio de "Accountability", supervisar la realización de las Evaluaciones de Impacto de Privacidad ("Privacy Impact Assessments"), o notificar las brechas de seguridad.

El resto de funciones, estarían formadas por el asesoramiento jurídico, la formación y ser punto de contacto con la Autoridad de Control. Recordemos a este respecto, que su nombramiento parece que se pretende que haya de ser comunicado a la respectiva Autoridad.

La figura del DPO no está recogida en la legislación española la cual sólo contempla la existencia del llamado Responsable de Seguridad, pero únicamente cuando en los tratamientos de datos personales haya que implementar las medidas de seguridad de nivel medio y alto. Si comparamos ambas figuras, el DPO abarca muchísimas más funciones que el Responsable de Seguridad, ya que éste, como su nombre indica, sólo se refiere al ámbito de la seguridad. En cambio, el DPO será el encargado de velar porque la organización cumpla con la Protección de Datos, no sólo en lo relativo a la seguridad, sino sobre todos los principios y obligaciones detallados anteriormente.

En cambio, si existen otras legislaciones europeas que han regulado esta figura (Ver Anexo I).

CONCLUSIONES

La definición del Delegado de Protección de Datos en la Propuesta de Reglamento General de Protección de Datos, al menos en la versión de la Comisión, va más allá de las funciones que actualmente tiene el Responsable de Seguridad en la Normativa española, de manera que se le otorga competencias de suma importancia para la Protección de Datos, no sin crear disyuntivas en cuanto a su implantación en las empresas.

En cuanto a la designación, su mandato está acotado en el tiempo, se establece la obligatoriedad de comunicación de los datos personales del DPO a los organismos competentes con fines de entrar en contacto con el mismo, así como la opción para los grupos de empresas de nombrar un DPO único. Este último punto abre la puerta para que desde las multinacionales españolas se gestione de forma centralizada la protección de datos de todas sus filiales europeas.

La Propuesta de Reglamento también detalla algunas directrices sobre el perfil deseado de un DPO, siendo los elementos prioritarios la valoración de la experiencia, la titulación en una materia específica relacionada con la función, y las certificaciones profesionales. No obstante estos dos últimos elementos no están mencionados de forma expresa en el texto normativo comunitario.

Uno de los aspectos más críticos, principalmente en las empresas, será como asegurar la independencia y el desarrollo de sus funciones sin plantear conflictos de intereses, teniendo en cuenta, además, que el DPO deberá integrar el cumplimiento de la normativa de protección de datos personales con la consecución de los objetivos de negocio de su compañía.

En resumen, si bien el DPO contribuirá a generar una mayor responsabilidad entre las empre-

sas y administraciones en el cumplimiento de la normativa de protección de datos, existen aspectos, como los que hemos citado, que deberán ser aclarados, ya sea mediante la previsión que se recoge en su regulación para ser desarrollada por actos delegados de la Comisión, o en la redacción final de la misma, ya que algunos apartados pueden ser eliminados como el referente a su obligatoriedad.

ANEXO I - COMPARATIVA LEGISLACIONES EUROPEAS- FIGURA DEL DPO

País	Figura	Observaciones
España	Responsable de Seguridad	
Alemania	Data protection official. Similar al data protection officer. Section 4f) y g) Es obligatorio nombrar un DPO en el primer mes de actividad de la empresa, depende del sector de actividad, en principio es necesario que 20 personas en las empresa traten DCP. Es necesario tener conocimientos sobre la materia, es posible que sea una persona externa a la compañía.	Existen también leyes federales (y agencias). Tienen legislación sectorial como el Social Security Code (Sozialgesetzbuch). Excepcionalmente la ley protege datos de personas jurídicas.
Bélgica	No.	
Eslovaquia	Personal data protection official. Siempre que el responsable tenga más de cinco empleados. Es obligación del Responsable que este reciba formación, la Oficina puede llegar a solicitar que se acredite la formación.	Legislación muy estricta. En el caso de que se traten datos de categorías especiales, se exige que se realice un "Proyecto de Seguridad" incluyendo el mismo un análisis de riesgos.
Francia	No.	
Grecia		El responsable del fichero debe nombrar una persona que tenga la cualificación profesional suficiente que garantice el cumplimiento de las medidas de seguridad.
Italia	No.	Regulación sectorial en la ley (bancario, laboral, judicial, sanitario, comunicaciones electrónicas, marketing directo...). Disponen de códigos deontológicos de los diferentes sectores.
Polonia	SI, Administrator of information security.	
Portugal	No.	
Reino Unido	No.	
Rumania	No.	
Letonia	Necesidad de nombrar a un Personal Data Protection Officer. Existe un registro público de Responsables de protección de datos.	Necesidad de nombrar a un Personal Data Protection Officer que deberá ser licenciado en derecho o ingeniero formado específicamente en Protección de Datos. El nombramiento debe ser registrado ante la autoridad de protección de datos estableciendo entre otros el período durante el que ocupará su cargo. El PDPO deberá elaborar un informe anual de la situación de la empresa.
República Checa	No.	No hay nada reseñable.

BIBLIOGRAFÍA / REFERENCIAS

Grupo de Trabajo del Artículo 29. Dictamen 8/2012 (WP199) por el que se proporciona más información sobre los debates relativos a la reforma de protección de datos.


http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_es.pdf#h2-2

Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de los datos.

http://ec.europa.eu/justice/policies/privacy/docs/application/286_es.pdf

Supervisor Europeo de Protección de Datos. Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001.

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf

The background of the slide features the European Union flag, which consists of a blue field with twelve gold stars arranged in a circle. The flag is partially visible at the top and right edges. Overlaid on the flag are several bright, white, diagonal light rays that originate from the bottom left and fan out towards the top right. These rays are accompanied by several out-of-focus white circles of varying sizes, creating a bokeh effect. The overall color palette is dominated by the blue of the flag and the white of the light effects.

Cap. 4
Reglamento
Europeo de
Protección de Datos,
BCRs y Grupos
multinacionales.

ABSTRACT

La Propuesta de Reglamento UE de Protección de Datos, entre otros aspectos novedosos, implementa un sistema de regulación, mediante herramientas vinculantes de carácter interno para “organizaciones internacionales” con el fin de flexibilizar el movimiento de datos dentro del Grupo Empresarial multinacional y dotar de transparencia el tratamiento de datos frente al titular, respetando el derecho a la intimidad y al propio control de los datos personales.

Ya desde 2002, el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE (en adelante, GT 29), en relación al artículo 26.2 de la Directiva 95/46/CE y observando las dificultades en dichas organizaciones, estableció la posibilidad de que éstas pudieran elaborar, con arreglo a la legislación aplicable, normativas internas vinculantes, de obligado cumplimiento, oponibles a terceros en caso de incumplimiento y aprobadas por las Autoridades de Control mediante el Mecanismo de Coherencia, propuesto y regulado por la propia Propuesta de Reglamento UE de Protección de Datos. Dichas normas se conocen como “*Normas Corporativas Vinculantes*” o más comúnmente por su denominación en inglés “*Binding Corporate Rules*”, con el objetivo de facilitar las transferencias internacionales de datos entre empresas pertenecientes a un mismo grupo multinacional que cuente con empresas ubicadas tanto en países que proporcionen un nivel de protección adecuado, como en países que no proporcionen dicho nivel.

Su importancia e implementación ha sido tal que ya en la actualidad, se han definido, con la misma estructura, contenido y procedimiento de aprobación aquellas “*Binding Corporate Rules*” orientadas a los Encargados del Tratamiento, teniendo en cuenta el tratamiento de datos personales derivado de la prestación de servicios, denominadas “*Binding Corporate Rules for Processor*”.

El objetivo de este capítulo es poder dar una visión práctica de la problemática y posibles alternativas del tratamiento de datos y posterior movimiento a nivel internacional de datos en el seno de Grupos Multinacionales, atendiendo al grado de Responsabilidad según las relaciones internas y con terceros (responsabilidad vertical) y la evaluación del riesgo del tratamiento (responsabilidad horizontal); así como analizar la naturaleza, contenido, estructura, y características de la aprobación e implementación de las “*Binding Corporate Rules*”.

DESARROLLO

1.- SUJETO OBLIGADO: GRUPOS EMPRESARIALES MULTINACIONALES

El tratamiento de datos, de ámbito internacional, debe estar sujeto al régimen de garantías, principalmente jurídicas, que permitan acreditar el cumplimiento de las normativas, europeas y estatales de aplicación, entendiendo por tales, el cumplimiento y sometiendo a alguna de ellas:

1. La adecuación del movimiento internacional de datos, donde encontramos incluido el actual mecanismo "Safe Harbor" o "Puerto Seguro".
2. A falta de adecuación se requieren garantías apropiadas y que se encuentren recogidas en Instrumentos Jurídicamente Vinculantes, como por ejemplo:
 - a) Las Cláusulas Contractuales Tipo: bien adoptadas por la Comisión Europea, por una Autoridad de ontrol competente o bien conjuntamente mediante el *Mecanismo de Coherencia*, previsto en el artículo 57 de la Propuesta de Reglamento UE de Protección de Datos.
 - b) Las Binding Corporate Rules (BCRs) aplicables tanto a Responsables de Fichero como a Encargados del Tratamiento (*Binding Corporate Rules for Processor*).
 - c) Los contratos "ad hoc" autorizados previamente por una Autoridad de Control.
3. En caso de no disponer de los anteriores, se exigen garantías de naturaleza Administrativa, como son las Autorizaciones Previas por la Autoridad de Control competente, para cualquier movimiento internacional de datos.
4. La sujeción de las transferencias internacionales de datos a las Excepciones previstas por la Propuesta de Reglamento UE de Protección de Datos, a las que habrían de sumarse las demás incluidas en las normativas nacionales de cada Estado Miembro, que en el caso de España serían las recogidas en los Arts. 33 y 34 de la LOPD y Arts. 65 a 70 del RDLOPD, puesto que no se contempla su derogación.

En consecuencia, estaríamos ante una delimitación de responsabilidades encuadrables como:

- **Responsabilidad Horizontal:** dependiendo del riesgo identificado atendiendo a la forma, procesos, y respeto a los derechos y libertades de los interesados, y
- **Responsabilidad vertical:** identificada como aquella que ya se delimitaba en la Directiva 95/46/CE, en la relación entre Responsables de Fichero y Encargados del Tratamiento, regulada mediante las cláusulas contractuales correspondientes al tipo de tratamiento y servicio prestado.

1.1.- RESPONSABILIDAD HORIZONTAL: EVALUACIÓN DEL RIESGO.

El tratamiento de datos personales se realizará conforme a unos estándares definidos en las llamadas "Binding Corporate Rules", que analizaremos más adelante, vinculantes y exigibles a todas las entidades del grupo, con independencia de su ubicación geográ-

fica, dentro o fuera del Espacio Económico Europeo. Por tanto habrá uniformidad en el tratamiento de datos, sin importar dónde se traten.

Además de por las Normas internas vinculantes, supletoriamente regirá la Propuesta de Reglamento UE de Protección de Datos y en lo que no lo contradiga, las normas nacionales de los Estados miembros donde se sitúen las compañías del grupo.

1.2.- RESPONSABILIDAD VERTICAL: RELACIONES ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO.

Ya la Directiva 95/46/CE, establecía la necesidad de plasmar, mediante cláusulas contractuales concretas, la delimitación de las obligaciones y medidas de seguridad necesarias para el tratamiento que terceros, para la prestación de un servicio al Responsable del Fichero, debían cumplir.

Este aspecto ha sido desarrollado, junto con las obligaciones del Responsable del Fichero, y se hacen extensivas al Encargado del Tratamiento, tanto más que también deberán cumplir con lo contenido en las Normas internas vinculantes. Es concretamente el artículo 33, al establecer la necesidad de una "Evaluación del Impacto" previa, cuando afirma que "(...) *evaluación del impacto de las operaciones de tratamiento previstas (...)*"; y siempre y cuando estemos ante una transferencia internacional sujeta a una normativa interna vinculante (BCR) deberá procederse a la obtención de la correspondiente autorización (artículo 34).

Así mismo, se prevé un régimen de "*Corresponsabilidad*" establecido en el artículo 22 de la Propuesta de Reglamento UE de Protección de Datos en relación al artículo 14 del mismo texto, respecto al Deber de Información al interesado, siendo un elemento más a la hora de delimitar la Responsabilidad "vertical" que también estará en las políticas y mecanismos internos de graduación de dicha responsabilidad en función de la forma societaria del Grupo Empresarial Multinacional.

Esta Responsabilidad vertical, como así la ha identificado el Consejo de Europa, va a suponer la identificación clara de las obligaciones concretas y la ponderación del grado de cumplimiento y exigibilidad que la nueva Norma europea prevé.

2.- BINDING CORPORATE RULES

Por primera vez, la Propuesta de Reglamento UE de Protección de Datos regula transferencias internacionales de datos fuera del Espacio Económico Europeo, dentro de una "*organización internacional*", y las "*transferencias ulteriores*", dándoles identidad propia y requerimientos propios, cuando hasta el momento solamente había contemplado la transferencia internacional a "*Terceros países*". Por lo tanto, no solamente será importante el destino de los datos sino el tipo de sujeto que las realiza y en el entorno en el que se tratan, ponderando los riesgos derivados.

A través del art. 43, la Propuesta de Reglamento UE de Protección de Datos reconoce explícitamente que, por primera vez, sería posible transferir datos personales fuera de la Unión Eu-

ropea sobre la base de un " *equilibrio de intereses*" probado, estableciendo unos requisitos mínimos.

Así surgieron las BCRs, con el objetivo de facilitar las transferencias internacionales de datos entre entidades (filiales o sucursales) pertenecientes a un mismo grupo multinacional. Se trata de una alternativa a las cláusulas contractuales tipo (artículo 70.4 RDLOP) para los grupos multinacionales, que conforma un marco de cumplimiento de la privacidad corporativa, constituido por un contrato vinculante, procesos y políticas comerciales, formación y directrices..., aprobado por las Autoridades de protección de datos de la UE y oponibles ante éstas, para garantizar la legalidad de las operaciones de transferencia de datos en su organización, independientemente de si el país es considerado como uno de los países que proporciona un nivel de protección adecuado conforme a la normativa o no.

2.1.- CONCEPTO Y NATURALEZA VINCULANTE.

Las BCRs son un conjunto de reglas o cláusulas corporativas vinculantes cuyo objeto es establecer y parametrizar las prácticas de una entidad, en el tratamiento de datos, con el fin de facilitar las transferencias internacionales de datos en el seno de dicha corporación.

Las BCRs no deben confundirse con los códigos de conducta o códigos tipo, ya que se caracterizan, entre otros aspectos por ser:

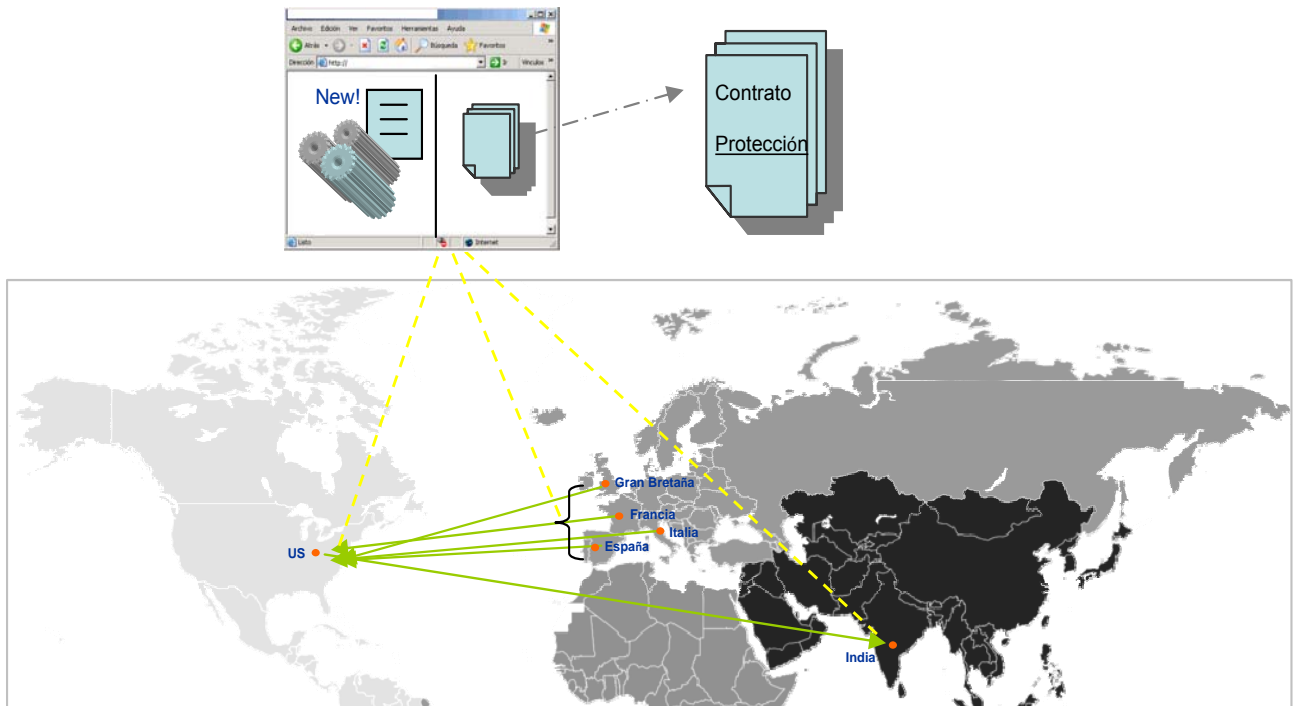
- Vinculantes o exigibles legalmente.
- Aplicables a un grupo de empresas o entidades sometidas al control de la entidad matriz.
- Se constituyen como normas, cuyo cumplimiento puede ser exigido de forma externa por parte de terceras entidades oficiales e independientes.
- Dotan a las organizaciones multinacionales de un marco común bajo el que poder realizar las transferencias de un modo ágil y legítimo.

La naturaleza vinculante de las BCRs implica que los miembros de la corporación (sucursales/filiales), empleados y directivos..., tienen la obligación de cumplirlas. Las BCRs son soluciones a medida, teniendo en cuenta la tipología de Grupo Empresarial, el objeto de su actividad económica y el entorno en el que operan. El nivel de detalle de unas BCRs debe ser extensivo y suficiente para permitir a las Autoridades de Control asegurarse, y en última instancia verificar, que el tratamiento es adecuado.

Las BCRs resultan herramientas atractivas por los beneficios a nivel organizativo que, para el desarrollo normal y la evolución natural de un Grupo Empresarial, el transferir datos a otras entidades del grupo, dentro de unos parámetros de seguridad aprobados por las Autoridades de Control, resulta fundamental, como son la *Flexibilidad*, en las transferencias de datos, y la *Transparencia* de sus actuaciones frente al interesado, y la capacidad de control de su cumplimiento.

Las normas internas están adecuadas a la naturaleza, contexto, alcance y objetivos de las actividades de tratamiento y los riesgos que pueden derivarse del tratamiento para los derechos y libertades de los interesados, determinándose las medidas adecuadas

a adoptar por el Grupo Multinacional, siempre con sometimiento a lo previsto en la Propuesta de Reglamento UE de Protección de Datos.



En el ejemplo del gráfico, caso de incumplimiento, supongamos que fuera la Sucursal Española la que incumple las normas internas, (p.e. un empleado cuelga una actuación en la red), responde la Sucursal Española hasta donde lleguen sus activos, y a partir del agotamiento de los mismos, responderá la matriz estadounidense. Lo mismo es predecible de las demás sucursales europeas y de la India, pese a ser un país tercero, ya que todas se encuentran vinculadas por las normas internas vinculantes. Así mismo, si incumpliera la matriz, a ésta se le podrían exigir responsabilidades directamente, y agotados sus activos se podría recurrir a las sucursales que dependen jurídicamente de la matriz.

2.2.- PROCEDIMIENTO DE APROBACIÓN. DESIGNACIÓN DE LA “LEAD AUTHORITY”

Para la presentación de la solicitud de aprobación de una BCR, deberá cumplimentarse el formulario que el GT 29 pone a disposición de las entidades, y deberá procederse a la designación de una Autoridad de Control perteneciente a un Estado Miembro y donde el Grupo Multinacional disponga de su sede o bien de una entidad del Grupo a la que pueda delegar la responsabilidad del control y supervisión del cumplimiento de las BCRs por parte de todo el grupo. La Corporación Multinacional deberá tener en cuenta que, prevalece como principal criterio de elección, el domicilio social de la entidad solicitante.

La Autoridad de Control, o “*Lead Authority*” gestionará el procedimiento de autorización con el resto de autoridades, incluyendo los propios organismos de la UE, mediante el Mecanismo de Coherencia, que ya prevé el artículo 57 de la Propuesta de Reglamento UE de Protección de Datos.

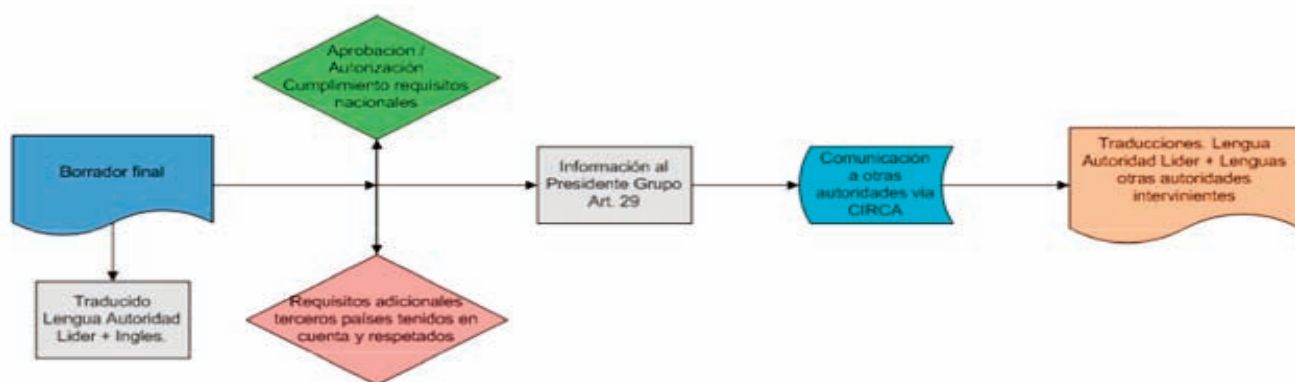
En todo caso, la Autoridad de protección de datos designada debe tener capacidad para decidir si son la entidad más adecuada dadas las circunstancias o por el contrario sería conveniente remitir el caso a otra Autoridad de Control más competente.

La documentación que conforman las BCRs contempla las políticas, códigos, procedimientos y contratos con empleados y terceros, así como una declaración general de principios. Es preciso identificar una persona de contacto de la organización a la que se dirigirán las consultas/dudas.

Las BCRs deben contener una descripción clara de las medidas de protección de datos a aplicar y deben en particular velar por:

- Transparencia y equidad a los interesados.
- Limitación del tratamiento a la finalidad declarada.
- Garantizar la calidad de los datos; la seguridad; derechos individuales de acceso, rectificación y oposición al tratamiento, etc.
- Definir un mecanismo de notificación y registro de cambios, informando a la Autoridad de Control de los cambios significativos.
- Estar sujetas a auditorías periódicas (interna, externa o una combinación de ambas) que podrán remitirse a la autoridad competente a su requerimiento.

El procedimiento de autorización a seguir para lograr la aprobación, una vez seleccionada y validada la Autoridad de protección de datos competente, puede estructurarse de la siguiente forma:



En cualquier caso, el artículo 43.1 de la Propuesta de Reglamento UE de Protección de Datos, recoge los elementos que una Autoridad de Control deberá valorar para aprobar una BCRs:

- a) "(...) sean jurídicamente vinculantes y se apliquen a todos los miembros del grupo de empresas del responsable o del encargado del tratamiento, incluidos sus empleados, que asegurarán su cumplimiento;(...)"

El GT 29 estableció, además de lo anterior, en su WP 74 (apartado 3.3) la necesidad de que además de estas normas las empresas deberán cumplir con los requisitos

normativos asociados a la regulación local. En el redactado de la Propuesta de Reglamento UE de Protección de Datos no se menciona nada relacionado específicamente con este aspecto, lo cual plantea dudas en relación a las ventajas reales que pueda proporcionar el establecimiento de las BCRs.

- b) (...) confieran expresamente a los interesados derechos exigibles;(...)
- c) Y con carácter esencial, (...) cumplan los requisitos establecidos en el apartado 2 del artículo 43 (...).

2.3.- ¿CÓMO PLANTEAR SU ELABORACIÓN?

Desde un punto de vista práctico, para llevar a cabo el desarrollo de BCRs, hay que tener en cuenta las siguientes recomendaciones para lograr un efectivo cumplimiento normativo y desarrollo interno:

- 1) Redacción de normas adecuadas al sector y ámbito geográfico de aplicación.
- 2) Definición clara de procedimientos para su aplicación y desarrollo.
- 3) Buscar el equilibrio entre las normas nacionales y su aplicación práctica a nivel global.
- 4) Definición del flujo de datos, especialmente aquellos con destino transfronterizo.
- 5) Delimitación del ámbito y forma de tratamiento, adaptado a la normativa y a los niveles de protección, con especial atención a los datos especialmente sensibles.
- 6) Mecanismos de control internos adecuados a la tipología de tratamiento y los agentes corporativos que intervienen, esencialmente mediante auditorías internas.
- 7) Establecer claramente los procedimientos internos para el correcto ejercicio de los derechos reconocidos a los titulares de datos personales, que permitan una tramitación de reclamaciones en los plazos legalmente establecidos, y contando con mecanismos de control "ad hoc".

En definitiva, deberá aplicarse la medida de "Evaluación del Impacto" que, en los artículos 33 y 34, recoge la Propuesta de Reglamento UE de Protección de Datos, en base a la ponderación del riesgo, los elementos y actuaciones a considerar ante la elaboración y posterior aprobación de las BCRs.

2.4.- CONTENIDO MÍNIMO Y PARÁMETROS ESENCIALES

ASPECTOS PRINCIPALES	CONTENIDO	
ALCANCE Y ÁMBITO DE APLICACIÓN	<p>Alcance geográfico. Actividad Económica. Estructura empresarial (sucursales/filiales). Descripción de los flujos de datos y finalidades de las transferencias. Tipología de datos tratados. Forma del tratamiento Responsable de Seguridad .</p>	
CUMPLIMIENTO DE GARANTÍAS Y PRINCIPIOS NORMATIVOS	<p>Delimitación de la Finalidad del tratamiento y posterior transferencia de datos. Calidad de los datos. Proporcionalidad de obtención y tratamiento de datos. Cumplimiento y Transparencia del deber de información. (artículo 14 RGPDUE). Establecimiento de procesos internos para la gestión y respuesta al Ejercicio de Derechos (acceso, rectificación, cancelación y oposición). Acreditación de la compatibilidad de las BCRs con la normativa estatal correspondiente.</p>	
TRATAMIENTO DE DATOS ESPECIALMENTE SENSIBLES	<p>Delimitación de la finalidad de su tratamiento. Destinatarios. Forma de tratamiento. Legitimación para su tratamiento (consentimiento, protección del interés vital de interesado....).</p>	
CARÁCTER VINCULANTE Y EXIGIBLE	<p>Cumplimiento: de principios y obligaciones contenidos. Adopción de medidas correctoras. Mecanismos de control y supervisión (auditorias...).</p>	
SEGURIDAD y CONFIDENCIALIDAD	<p>Medidas técnicas y organizativas que garanticen la confidencialidad e integridad de los datos. Garantías del nivel de protección aplicable. Medidas específicas para el tratamiento y movimiento de datos, especialmente en la red. Medidas acorde con los riesgos según el tipo de tratamiento y naturaleza de los datos protegidos.</p>	<p>En el tratamiento de datos especialmente sensibles: política de seguridad. Aspectos organizativos asociados a la seguridad. Formación, divulgación y concienciación en materia de seguridad. Seguridad ligada a los Recursos Humanos. Relaciones con terceros. Seguridad física y del entorno. Inventario y clasificación de activos. Gestión de activos. Seguridad de las comunicaciones y operaciones. Control de acceso. Adquisición, desarrollo y mantenimiento de sistemas. Gestión de incidentes de seguridad. Disponibilidad de sistemas. Continuidad del negocio. Cumplimiento legal y normativo.</p>
RELACIONES CON TERCEROS	<p>Determinación y garantías a implantar en las relaciones con entidades del mismo Grupo consideradas Encargados del Tratamiento. (artículo 14). Identificación de los supuestos de Cesiones de Datos y cumplimiento de los requerimientos normativos y control. Delimitación del régimen de autorizaciones para el movimiento de datos con destino a terceros.</p>	
RÉGIMEN ESPECÍFICO PARA LAS TRANSFERENCIAS INTERNACIONALES	<p>Restricciones en las transferencias iniciales y/o ulteriores a terceros externos. Detalle de medidas de restricción en transferencias ulteriores fuera del grupo y las normas de obligado cumplimiento para su legitimación.</p>	
FORMACIÓN	<p>Establecimiento de programas de formación internos, atendiendo al tipo de tratamiento de datos y su finalidad.</p>	

RESPONSABILIDAD	Delimitación de la responsabilidad corporativa del Grupo empresarial a nivel interno y externo. Operativa por reclamaciones e infracciones ante la autoridad de control correspondiente.
COLABORACIÓN Y COOPERACIÓN	Asistencia mutua y cooperación con las autoridades de control.
REVISIÓN Y ACTUALIZACIÓN	Determinación del Régimen y procedimientos internos, así como responsables asignados para la revisión y actualización de las BCRs.

CONTENIDO MÍNIMO DE UNA NORMA CORPORATIVA VINCULANTE (BCRs) SEGÚN LA PROPUESTA DE REGLAMENTO UE DE PROTECCIÓN DE DATOS

PROPUESTA DE REGLAMENTO (artículo 43.2)	GT 29
<i>Estructura, miembros e identificación de responsable;</i>	WP 108-
<i>Transferencias (tipología, categoría de datos, tipo tratamientos y sus fines, tipo de interesados y nombre del tercer/os países en cuestión;</i>	WP 108 (4 -7) WP 133
<i>Carácter jurídicamente vinculante, a nivel interno y externo;</i>	WP 108-5
<i>Principios generales en materia de protección de datos:</i>	WP 108-8.2
<i>Derechos de los interesados y medios para ejercerlos</i>	WP 108-8.2.5 WP 153
<i>Aceptación de responsabilidades y posibilidad de exoneración.</i>	WP 108 WP 74
<i>Forma de cumplimiento del Deber de Información a los interesados sobre las normas corporativas vinculantes.</i>	WP 108-5.11, 5.13 y 5.14
<i>Tareas del delegado de protección de datos designado (artículo 35 RGPDUE)</i>	WP 74
<i>Mecanismos internos para garantizar que se verifica el cumplimiento de las normas corporativas vinculantes;</i>	WP 108 (6.1) WP 153
<i>Mecanismos para comunicar y registrar las modificaciones introducidas en las políticas y notificarlas a la autoridad de control;</i>	WP 108 (9.1) WP 74 (4.2)
<i>Mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento, poniendo a disposición los resultados de las verificaciones de las medidas.</i>	WP 108 (5.21)

2.5.- RÉGIMEN DE RESPONSABILIDAD.

Es requisito indispensable la designación de un responsable, dentro del territorio de la Unión Europea, del cumplimiento de las medidas y las garantías a los derechos de los interesados, así como hacerse cargo de las sanciones que puedan derivarse de infracciones del país destino Encargado del tratamiento, pudiendo ser la misma matriz del Grupo Empresarial, o si ésta tiene su sede fuera del territorio del Espacio Económico Europeo, aquella designada por la misma matriz.

El artículo 43.2 f) de la Propuesta de Reglamento UE de Protección de Datos, desarrollando lo previsto en el WP 108 del GT 29, ya prevé este aspecto, dentro del régimen de responsabilidad del Grupo Multinacional en la aprobación y contenido mínimo de las BCRs, y concretamente cuando la sede social del grupo de sociedades no está en la UE / EEE, el grupo de empresas deberá designar un miembro europeo con responsabilidades delegadas a cargo de asegurar que, cualquier miembro extranjero del grupo de multinacional ajusta sus actividades de procesamiento, la interfaz con la principal autoridad, de forma según las BCRs establecidas, puesto que será la Entidad con responsabilidad delegada la que tendrá que hacer frente de las compensaciones adecuadas y del pago, en caso de daños producidos, por la violación de las reglas corporativas vinculantes por parte de cualquier miembro del grupo de sociedades.

Teniendo en cuenta que, en caso de conflicto, el interesado demandante puede elegir la jurisdicción aplicable, pudiendo ser ésta la del país origen de la transferencia de los datos, o bien la jurisdicción de la sede u entidad europea en el que se delegan las responsabilidades, es necesario establecer un marco de protección que abarque el cumplimiento de las posibles regulaciones que apliquen a la procedencia de los datos. Así mismo, y a pesar de ello, la aplicación de las medidas de seguridad necesarias establecidas por la entidad responsable, no eximen de la necesidad del cumplimiento de la legislación local del país destino.

La sede o aquella entidad miembro que debe establecer el marco de control sobre las medidas de seguridad implantadas, además de aceptar la responsabilidad y comprometerse a adoptar las medidas necesarias para remediar los actos de los otros miembros del grupo de empresas fuera de la Unión Europea deberá comprometerse, en su caso, a pagar una indemnización por los daños producidos por la violación de las reglas corporativas vinculantes por parte de cualquier miembro vinculado por el régimen.

El grupo multinacional deberá adjuntar las evidencias a su solicitud de autorización de que la sede de la UE o la entidad designada tiene activos suficientes en la UE para cubrir el pago de la indemnización por incumplimiento de las BCRs en circunstancias normales o que ha tomado medidas para asegurar que no sería capaz de satisfacer tales demandas en esa medida (por ejemplo: la cobertura del seguro de responsabilidad civil). Al margen de todo lo anterior, debe tenerse en cuenta que, para algunos grupos con determinadas estructuras corporativas, no siempre es posible imponer a una entidad específica toda la responsabilidad por el incumplimiento de las BCRs. En estos casos, el GT 29 reconoce que el grupo multinacional puede demostrar por qué no es posible que ellos designen una entidad única en la UE y pueden proponer otros mecanismos de responsabilidad que se ajusten a la organización.

Por ejemplo, la creación de un mecanismo de responsabilidad solidaria entre los importadores de datos y los exportadores de datos como se ve en las Cláusulas Contractuales Tipo de la Unión Europea 2001/497/CE de 15 de junio de 2001, o para definir un régimen de responsabilidad alternativo basado en las obligaciones de diligencia debida según lo prescrito en el estándar de la UE cláusulas contractuales 2004/915/CE de 27

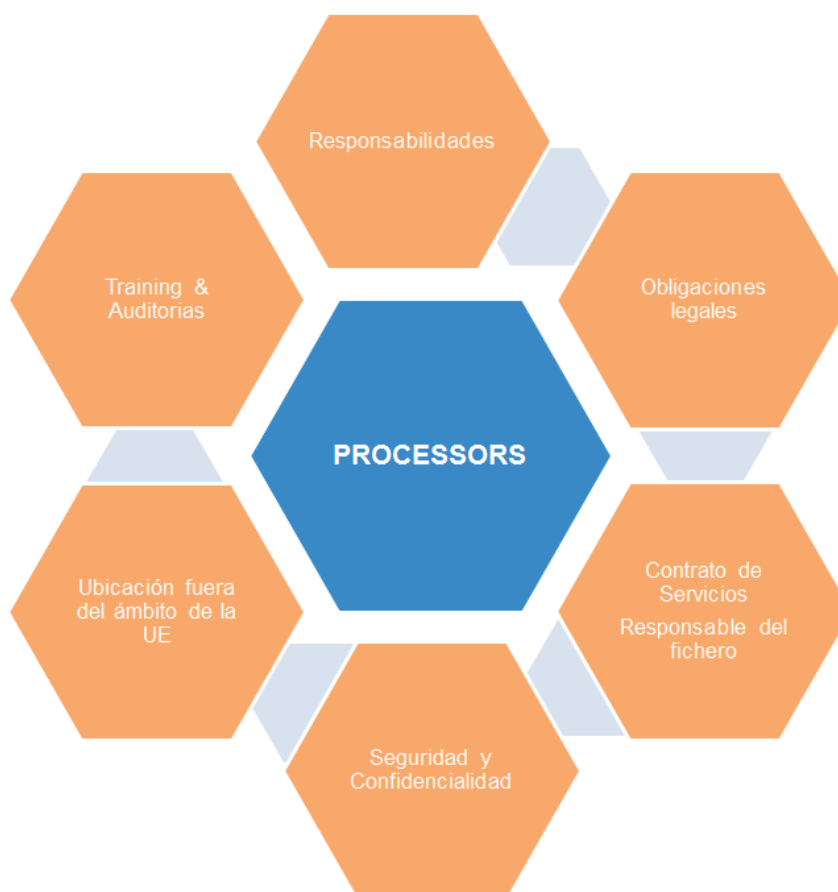
de diciembre de 2004, y en última instancia, en relación a las transferencias a Encargados del Tratamiento, es la aplicación del mecanismo de la responsabilidad de las cláusulas contractuales estándar 2002/16/CE de 27 de diciembre de 2001.

Las autoridades de protección de datos pueden aceptar esas soluciones alternativas de responsabilidad estudiando cada caso individualmente. En cualquier caso, resulta necesario que cualquier mecanismo alternativo garantice el respeto y cumplimiento de los derechos de los interesados y no supongan un menoscabo de dichos derechos.

2.6.- HACIA LAS BCRs FOR PROCESSORS.

La principal ventaja de las "*Bilding Corporate Rules for Proccessors*" es que aportan a los Responsables del Fichero confianza y transparencia en el cumplimiento de los requerimientos normativos aplicables al tratamiento de datos personales por un Encargado de Tratamiento, estando éstos sometidos al cumplimiento de BCRs concretas, y proporcionando la transparencia necesaria que garantice el cumplimiento de los deberes y obligaciones previstos por la legislación de aplicación (medidas de seguridad, incluso si el encargado transfiere datos a terceros subcontratados, ubicados dentro o fuera de la Unión Económica Europea), estandarización de los contenidos mínimos de los acuerdos contractuales de prestaciones de servicios que impliquen tratamientos de datos, adecuación al entorno de tratamiento...

En cualquier caso, los elementos a tener presente son los que se ilustran en la figura siguiente:



2.7.- LAS BCR'S Y LAS NORMAS "SAFE HARBOUR"

La consideración de "Puerto seguro" ha recibido críticas, principalmente, por lo sencillo que resulta obtener el certificado y las escasas garantías que éstas ofrecen tanto al afectado (titular de los datos), como a los Responsables de Fichero en sus relaciones con Encargados del Tratamientos sujetos a este tipo de normas.

Se observan como debilidades:

A. La obtención del certificado pasa por abonar las tasas correspondientes y hacer una declaración en la cual se compromete a cumplir con 7 principios de privacidad:

- 1. Notice:** Deber de información (o notificación).
- 2. Choice:** El principio del principio del consentimiento del afectado.
- 3. Transfers to Third Parties:** Países miembros de la Unión Europea.
- 4. Access: (Ejercicio de Derechos)**
- 5. Security:** El principio de seguridad de los datos.
- 6. Data Integrity:** El principio de calidad de los datos.
- 7. Enforcement:** Mecanismos independientes de resolución de conflictos y verificación del cumplimiento, con potestad para sancionar.

B. La verificación del cumplimiento se realiza por la entidad del país (en el caso de España por la AEPD), sin un control externo.

En definitiva, las BCRs, actualmente, se han erigido como la herramienta adecuada para la legitimación, legalización y cumplimiento de las premisas de la Protección de Datos personales, en el seno de Grupos multinacionales, con sedes en diferentes países, incluso fuera el Espacio Económico Europeo, ámbito geográfico de aplicación de la Directiva y su futuro Reglamento de Protección de Datos Personales.

CONCLUSIONES

Los principios básicos que debe regir todo movimiento de datos personales, mediante Transferencias Internacionales son: licitud, calidad, proporcionalidad, consentimiento, información, finalidad y responsabilidad, debiendo cumplirse desde la recogida del dato hasta la recepción de la última transferencia. Estos principios resultan ser la base del tratamiento de datos en Grupos Multinacionales, y los objetivos delimitar en las BCRs para que éstas puedan cumplir con su principal finalidad, que no es otra que la de agilizar el tratamientos de datos entre entidades de un mismo Grupo Empresarial, sin vulnerar los derechos y libertades del individuo en el tratamiento de sus datos personales.

La "*ponderación del riesgo*" y la "*evaluación del impacto*" del tratamiento de datos en los derechos y libertades por Grupos Multinacionales, suponen la aplicación del principio de proporcionalidad en la delimitación de obligaciones para responsables y encargados del tratamiento, determinando su Responsabilidad (horizontal) y el alcance y cumplimiento de la protección de datos personales.

Por otro lado, para los grandes proveedores multinacionales de outsourcing global y servicios de *cloud computing*..., las *BCRs for Processors* representan una oportunidad para ampliar su base de clientes de la UE mediante la simplificación del proceso para los clientes potenciales (especialmente las PYME) y cumplir con sus obligaciones de tratamiento de los datos. Los destinatarios de estos servicios deben ser conscientes, sin embargo, que son responsables de los datos y que las BCRs no se pueden utilizar para transferir y/o delegar en modo alguno sus obligaciones legales al proveedor encargado del tratamiento, sino más bien determinar las reglas en el tratamiento de datos.

BIBLIOGRAFÍA/REFERENCIAS

Working Document WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on June 3, 2003

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

Working Document WP 108: Establishing a model checklist application for approval of Binding Corporate Rules, adopted on April 14, 2005 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

Working Document WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm

Working Document WP 195: 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (June 6, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf (last visited November 30, 2012)."


Working Document WP 155 on Frequently Asked Questions (FAQs) related to Binding Corporate Rules Adopted on 24 June 2008 As last Revised and adopted on 8 April 2009"

Working Document WP 153 setting up a table with the elements and principles to be found in Binding Corporate Rules Adopted on 24 June 2008

Resolución de Madrid de 5/11/2009 (COM (2011) 635 final) sobre los Estándares Internacionales sobre Protección de Datos Personales de la UE.

Memento experto Francis Lefebvre – Protección de Datos – actualizado a 15 de julio de 2012

Todo Protección de Datos – CISS Grupo Wolters Kluwer - 2012



Cap. 5
La nueva
configuración de los
derechos
de los
interesados.

ABSTRACT

Según la Exposición de Motivos de la Propuesta de Reglamento UE de Protección de Datos de la Comisión Europea *“(...) La rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales. Se ha incrementado enormemente la magnitud del intercambio y la recogida de datos. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social. (...)”*

Luego, una mejor protección del derecho fundamental a la Protección de Datos personales resulta clave para generar la debida confianza en los ciudadanos en lo que concierne a su actividad en línea y, en paralelo, también para el desarrollo pleno de las diversas estrategias que integra la Agenda Digital Europea. En este sentido, la Propuesta de Reglamento UE de Protección de Datos hace especial hincapié en la protección de la privacidad de los menores en Internet.

Por lo que, tal y como declara la propia Comisión Europea en la citada Propuesta, *“(...) Ha llegado (...) el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas (...)”*

Pues bien, para la consecución del citado objetivo, resulta imprescindible acometer el pertinente análisis previo y, en su caso, reforzamiento de la actual regulación de los derechos de los interesados en el ámbito de la Protección de Datos personales en el seno de la Unión Europea, teniendo en cuenta que el derecho a la Protección de Datos de carácter personal tampoco es un derecho absoluto, sino que se ha de considerar en relación con su función en la sociedad, es decir, coexistir con otros tantos derechos fundamentales igualmente reconocidos (libertad de expresión; libertad de comunicación; el derecho a la tutela judicial efectiva; derechos de los menores; el derecho de acceso a los documentos; la libertad de empresa, etc.).

A continuación, se realiza una somera revisión de las principales modificaciones dispuestas a tal fin por parte de la proyectada reforma europea, tomando en consideración también las propuestas de modificación respecto al Reglamento contenidas en el documento de 31 de mayo dirigido por la Presidencia irlandesa al Consejo.

DESARROLLO

A fin de examinar la nueva configuración de los derechos de los interesados que se prevé en el Reglamento, se han identificado tres bloques temáticos de interés y que se han catalogado, respectivamente, como transversal, específico y relativo a procesos de defensa o reclamación tal y como se indica a continuación.

1. BLOQUE TEMÁTICO TRANSVERSAL.

1.1: CONSIDERACIONES GENERALES.

Tal y como se infiere de los arts.11 a 13 de la propuesta de Reglamento, en éste se re-fuerzan los principios de transparencia y de información adaptada, accesible, inteligible, clara y sencilla por lo que respecta al tratamiento de datos personales y al ejercicio de los derechos de los interesados.

Por otra parte, en lo que concierne a los procedimientos y mecanismos para el ejercicio de los derechos de los interesados se destaca lo que sigue:

- a) Se mantiene el deber del Responsable de prever, con carácter general, procedimientos y mecanismos de carácter gratuito que permitan y faciliten el ejercicio de los derechos de los interesados.
- b) Se incluye la obligación del Responsable del tratamiento de informar sin demora al interesado y, a más tardar, en el plazo de un mes a partir de la recepción de la solicitud, de si se ha tomado alguna medida con arreglo a lo dispuesto en el artículo 13 y en los artículos 15 a 19 y debiendo facilitar la información solicitada.
- c) El plazo al que alude el apartado b) podrá prorrogarse un mes, si varios interesados ejercen sus derechos y si su cooperación es necesaria, en una medida razonable, para impedir un esfuerzo innecesario y desproporcionado por parte del responsable del tratamiento. Si el Responsable del tratamiento se niega a dar curso a la solicitud del interesado, le informará de las razones de la denegación y de la posibilidad de presentar una reclamación ante la Autoridad de Control, así como de recurrir a los tribunales.
- d) La Comisión podrá establecer formularios y procedimientos normalizados para la comunicación contemplada en el apartado b), incluido el formato electrónico, con especial atención al caso de microempresas y PYMES.
- e) Por último, se destaca que la última versión del Consejo introduce un nuevo apartado que establece que cuando el Responsable del tratamiento tiene razonables dudas sobre la identidad de la persona que hace la solicitud prevista en los artículos 15 a 19, éste puede solicitar el suministro de información adicional necesaria para confirmar la identidad del interesado.

1.2: DERECHOS EN RELACIÓN CON LOS DESTINATARIOS (ARTÍCULO 13).

Los mismos están en relación directa con la obligación del Responsable del tratamiento de comunicar cualquier rectificación o supresión llevada a cabo con arreglo a los artícu-

los 16 y 17 a cada uno de los destinatarios a los que se hayan comunicado los datos, salvo que ello sea imposible o exija un esfuerzo desproporcionado.

1.3: DERECHO A LA INFORMACIÓN (ARTÍCULO 14).

Es el derecho del interesado a ser informado, con carácter general, en el momento de la recogida de sus datos personales, al menos, de ciertos extremos, por ejemplo, la identidad y los datos de contacto del Responsable del tratamiento y, en su caso, de su representante y del Delegado de Protección de Datos, los fines del tratamiento a que se destinan los datos personales, el plazo de conservación de los datos personales o la existencia de derechos personales, entre otros de interés.

1.4: DERECHO DE ACCESO (ARTÍCULO 15).

Es el derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no sus datos personales, así como a obtener información al respecto (fines del tratamiento, categorías de datos personales de que se trate; destinatarios, etc.). También tendrá derecho a que le comunique los datos personales objeto de tratamiento. Si el interesado realiza la solicitud en formato electrónico, la información se facilitará en ese mismo formato, pudiendo la Comisión especificar formularios y procedimientos normalizados a tal fin.

1.5: DERECHO DE RECTIFICACIÓN (ARTÍCULO 16).

Se mantiene el derecho del interesado a derecho a obtener del responsable del tratamiento la rectificación de los datos personales que le conciernen cuando tales datos resulten inexactos, así como su derecho a que se completen los datos personales cuando estos resulten incompletos, en particular, mediante una declaración rectificativa adicional. El documento del Consejo añade un nuevo párrafo a este artículo limitando este derecho de rectificación cuando los datos que se traten sean con fines de investigación histórica, estadística y científica.

1.6: DERECHO AL OLVIDO Y A LA SUPRESIÓN (ARTÍCULO 17).

Entre las novedades más significativas introducidas por a Propuesta de Reglamento UE de Protección de Datos destaca el denominado "derecho al olvido", tratando el legislador con su regulación un cambio radical en la manera de gestionar la privacidad y generando un interesante debate sobre su alcance, legitimidad y los límites del ejercicio de este derecho.

Los ciudadanos son cada vez más conscientes de su derecho a la protección de los datos personales y ello les lleva a cuestionarse sobre el tratamiento que terceros realizan o pretenden realizar respecto a su información personal y, con ello, si resulta conveniente o necesario ejercitar la cancelación o supresión de sus datos frente a los mismos. Al respecto, resultan llamativos los datos que arroja la última Memoria publicada por la Agencia Española de Protección de datos de 2011, donde se pone de manifiesto que de las tres solicitudes iniciales de Tutela recibidas en la Agencia en 2007 se

ha pasado a 160 reclamaciones en 2011, lo que duplica además el número de las recibidas respecto al año anterior.

Según prevé el artículo 17 de la Propuesta de Reglamento UE de Protección de Datos el interesado tendrá derecho a que el Responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo menor de edad cuando concurren las condiciones dispuestas en este precepto. Luego el “derecho al olvido” se puede definir como el derecho que tiene el titular de un dato personal a borrar, bloquear o suprimir información personal en los términos y condiciones indicadas en el citado artículo.

Tal y como indica Sebastián Zarate, algunos autores conciben el “derecho al olvido” en un doble sentido: “como derecho a olvidar y como derecho a ser olvidado”. Pudiendo analizarse de dos formas. El primero, como un derecho de caducidad de información personal, por ejemplo, por haber cesado la finalidad de tratamiento que justifica el mismo o, incluso, por haberse opuesto el interesado al tratamiento en coherencia con el artículo 19 de la Propuesta de Reglamento UE de Protección de Datos, y el segundo, como un derecho a olvidar información que pueda aparecer negativa para la persona, es decir, lo que algún autor ha denominado como de “nuevo comienzo”, o dicho de forma más coloquial, un “borrón y cuenta nueva”.

En todo caso, con el fin de reforzar el denominado “derecho al olvido” el legislador obliga a los Responsables del tratamiento que hayan hecho públicos datos personales a informar a los terceros que estén tratando estos datos de que un interesado le solicita que supriman sus datos (supresión de cualquier enlace a esos datos personales, o a cualquier copia o réplica de los mismos), debiendo tomar todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable. Asimismo, se destaca la obligación del Responsable del tratamiento de implementar mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos.

Por lo anteriormente expuesto ¿podemos hablar de un “derecho al olvido” como tal?, o ¿estamos más bien ante un derecho subjetivo de cancelación?. Al respecto, tal y como reconoce el Abogado General D. Nilo Jääskinen en sus conclusiones presentadas el 25 de Junio del 2013 la Directiva 95/46/CE en sus artículos 12, letra b) y 14 letra a), no establece un derecho general al olvido en el sentido de que el titular del dato está facultado al borrado de sus datos personales que considera lesivos o contrarios a sus intereses.

Ahora bien, el “derecho al olvido” no puede concebirse como un derecho, en modo alguno, absoluto. De hecho, el apartado 3 del artículo 17 prevé la necesaria conservación de los datos en determinados supuestos como el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el artículo 80; por motivos de interés público; en el ámbito de la salud pública de conformidad con lo dispuesto en el artículo

81; con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el artículo 83; para el cumplimiento de una obligación legal de conservar los datos personales; o en los casos contemplados en el apartado 4 del mismo precepto.

Así destaca el conflicto del “derecho al olvido” con la libertad de expresión (artículo 80). Al respecto, el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea establece que toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. La propuesta del Reglamento con el fin de garantizar este derecho establece que el tratamiento de datos personales solo con fines periodísticos, o con fines de expresión artística o literaria, debe disfrutar de una excepción a los requisitos de determinadas disposiciones del presente Reglamento, con el fin de conciliar el derecho a la protección de los datos de carácter personal con el derecho a la libertad de expresión, y en especial, el derecho de recibir o comunicar informaciones. Es más, incidiendo en lo anterior el documento del Consejo establece que el derecho a la protección de datos de carácter personal coexiste con otros derechos fundamentales, específicamente con el derecho a la libertad de expresión. Por otra parte, en este documento también se contempla ya la posibilidad de divulgar datos personales en los documentos oficiales de interés público (libertad de acceso a los documentos públicos).

En todo caso, la configuración final del derecho al olvido parece estar sujeta, en gran medida, a la interpretación judicial que finalmente pudiera emitir el Tribunal de Justicia de la Unión Europea como respuesta a las cuestiones prejudiciales que le ha planteado la Sala de lo Contencioso-Administrativo de la Audiencia Nacional en España sobre la interpretación de la Directiva 95/46/CE en relación con la actividad de los motores de búsqueda de Internet, a fin de que el citado Tribunal pudiera pronunciarse sobre la responsabilidad de los motores de búsqueda y de los titulares de sitios web y para que precisara acerca de la posibilidad o no de impedir y, en su caso, bajo qué condiciones, la indexación de información parcial.

En este ámbito, el abogado General D. Nilo Jääskinen en sus conclusiones no vinculantes publicadas el 25 de Junio del 2013 considera que i) el proveedor de servicios de motor de búsqueda en internet no puede cumplir las obligaciones del responsable de tratamiento y por tanto ninguna autoridad nacional de protección de datos puede requerir al proveedor de servicios de motor de búsqueda en internet que retire información, salvo en los supuestos que el proveedor de servicios no respete los códigos de exclusión ii) que la Directiva no establece ningún “derecho al olvido” generalizado. Por tanto, no puede invocarse tal derecho frente a proveedores de servicios de motor de búsqueda sobre la base de la Directiva, aun cuando ésta se interpreta con arreglo a la Carta de los Derechos Fundamentales de la Unión Europea. Ahora bien, se destaca que las conclusiones del Abogado General, aun teniendo gran relevancia, no vinculan al Tribunal de Justicia, por lo que resulta prematuro, tal y como ha indicado expresamente la propia Agencia Española de Protección de Datos, deducir cuál será el criterio final del órgano judicial sobre las cuestiones jurídicas planteadas.

1.6: DERECHO A LA PORTABILIDAD DE LOS DATOS (ARTÍCULO 18):

Se contempla este nuevo derecho, el cual, opera en una doble vertiente, a saber:

- 1) La posibilidad de obtener una copia de los datos personales objeto del tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos y;
- 2) La posibilidad de transferir datos de un sistema de tratamiento automatizado a otro en un formato electrónico comúnmente utilizado. Sólo es de aplicación para los datos automatizados, y no se especifica mucho sobre el formato en que se deben proporcionar la copia para la portabilidad y es que, además, en ambos casos, se faculta a la Comisión, por la vía de los pertinentes actos de ejecución, para especificar el formato electrónico contemplado, así como las normas técnicas, modalidades y procedimientos para la transmisión de datos personales. Todo ello sin perjuicio y con respeto, parece matizar el último documento del Consejo, de los derechos de propiedad intelectual que concurran. Por último, el documento del Consejo incluye un nuevo apartado donde se elimina la posibilidad del ejercicio de la portabilidad cuando los datos sólo se usen para fines de investigación histórica, estadística o científica.

1.7: DERECHO DE OPOSICIÓN Y ELABORACIÓN DE PERFILES (ARTÍCULOS 19 Y 20).

En la Propuesta de Reglamento UE de Protección de Datos se ha hecho una sustanciosa modificación en la redacción reafirmando el ejercicio del derecho de oposición, para que se haga efectiva desde el momento de la presentación de la solicitud, y no se traten directamente para fines comerciales cuando el interesado así lo haya manifestado. Este derecho se ofrecerá explícitamente al interesado de manera inteligible y será claramente distinguible de cualquier otra información. Al igual que en el derecho a la portabilidad de los datos, el documento del Consejo se plantea la inclusión de un nuevo apartado donde se elimina la posibilidad del ejercicio del derecho cuando los datos sólo se usen para fines de investigación histórica, estadística o científica. Por lo que respecta a la elaboración de perfiles, aunque no puede reconocerse como un nuevo derecho de los interesados, si parece regularse de una forma más profusa y detallada.

1.8: LIMITACIONES (ARTÍCULO 21).

Este precepto permite, en definitiva, que a nivel comunitario o a nivel de los diversos Estados Miembros se pueda limitar a través de las pertinentes medidas normativas el alcance de las obligaciones y de los derechos previstos en la Propuesta de Reglamento UE de Protección de Datos, cuando tal limitación constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar otros intereses o derechos igualmente protegibles indicados en aquél (la seguridad pública; la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales; la protección del interesado o de los derechos y libertades de otras personas, etc.). Como se puede apreciar, en la Propuesta de Reglamento UE de Protección de Datos se modifica, en parte, la enumeración de supuestos, intereses y derechos que pueden justificar estas

medidas respecto a lo indicado en el artículo 13 de la Directiva 95/46/CE, en donde se mencionan también de forma expresa otros supuestos como la defensa y la seguridad nacional. Estos supuestos se retoman e incorporan de nuevo, precisamente, en el documento del Consejo. Asimismo, también aumentan las previsiones que debe contener, como mínimo, la medida legislativa que pretenda adoptarse al amparo de este artículo.

2. BLOQUE TEMÁTICO ESPECÍFICO.

2.1: DERECHO A LA COMUNICACIÓN DE UNA VIOLACIÓN DE DATOS PERSONALES AL INTERESADO (ARTÍCULO 32).

Conforme a este artículo, cuando sea probable que la violación de datos personales afecte negativamente a la protección de los datos personales o a la privacidad del interesado, el Responsable del tratamiento (después de haber procedido a la notificación a la Autoridad de Control por dicha violación sin demora injustificada y, de ser posible, a más tardar en 24 horas después de que haya tenido constancia de ella conforme el artículo 31), comunicará al interesado, sin demora injustificada, la violación de datos personales. Ahora bien, la comunicación de una violación de datos personales al interesado no será necesaria si el Responsable del tratamiento demuestra, a satisfacción de la Autoridad de Control, que ha implementado medidas de protección tecnológica apropiadas y que estas medidas se han aplicado a los datos afectados por la violación. Resulta llamativo que en el documento del Consejo el plazo de 24 horas se proponga ampliar hasta 72 horas, ampliación de plazo que, por lo tanto, se traslada al plazo relativo a la notificación del interesado no haciéndola, además, necesaria en más casos, es decir, el Responsable del tratamiento tiene más supuestos a los que acogerse para no notificar la brecha de seguridad al interesado. De esta forma, se flexibilizan y relajan las obligaciones para el Responsable del tratamiento en estos casos.

2.2: DERECHOS DE LOS INTERESADOS Y EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (PIA) (ARTÍCULO 33).

El PIA es obligatorio en las operaciones de tratamiento que entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines (tratamiento de datos basados en perfiles, datos sensibles, datos salud, control de áreas de acceso público con video vigilancia, especialmente cuando se utilicen a gran escala, datos sobre menores y datos genéticos o datos biométricos). Así, la norma contiene una descripción sobre lo que el asesoramiento debe contener, los riesgos, las medidas que deben adoptarse para superarlos, las salvaguardas que deben existir para asegurar la protección de datos y el cumplimiento de esa regulación. En el PIA el papel de los interesados es muy importante, tal y como establece el artículo 33.4 de la Propuesta de Reglamento UE de Protección de Datos, ya que en el informe se debe especificar qué esfuerzos ha hecho la organización para consultar con los interesados, recabar sus opiniones e ideas sobre los posibles impactos de privacidad, la forma en que dicha privacidad podría verse afectada por el proyecto (positiva y / o negativamente) y cómo los impactos negativos pueden ser mitigados, evitados, o eliminados. Por úl-

timo, la exención que se establece en la Propuesta de Reglamento UE de Protección de Datos respecto al uso de los PIA cuando el Responsable del tratamiento sea una autoridad u organismo públicos y cuando el tratamiento se efectúe en cumplimiento de una obligación legal, no parece aceptable habida cuenta que muchos organismos públicos tratan datos personales especialmente sensibles, y que en dichas entidades puede existir una ruptura en la seguridad y consecuentemente los interesados verse muy afectados. Por consiguiente, sería recomendable que las entidades públicas sean las primeras en abrazar e implementar este tipo de medidas en aras a reforzar la protección de los interesados.

2.3: DERECHOS DE LOS INTERESADOS Y DELEGADO DE PROTECCIÓN DE DATOS (DPO) (ARTÍCULO 35).

De conformidad con la Propuesta de Reglamento UE de Protección de Datos se exige la contratación del mismo cuando: (i) el tratamiento sea llevado a cabo por una autoridad u organismo público; (ii) el tratamiento sea llevado a cabo por una empresa que emplee a doscientas cincuenta personas o más y (iii) las actividades principales del Responsable o del Encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados. A la vista de sus funciones (artículo 37), esta figura tiene un papel importante en el debido tratamiento y atención a los derechos de los interesados en el marco de la organización del Responsable del tratamiento. Lamentablemente, en el Documento del Consejo esta figura se torna de obligatoria en determinados supuestos a totalmente opcional.

2.4: DERECHOS DE LOS INTERESADOS EN EL MARCO DE LA ELABORACIÓN DE CÓDIGOS TIPO (ARTÍCULO 38).

Los códigos de conducta promovidos por la Propuesta de Reglamento UE de Protección de Datos constituyen una excelente oportunidad, por la vía de la autorregulación, de reforzar y amplificar los derechos de los interesados, sobre todo, en lo que concierne a la información y protección de los niños. De acuerdo con el resultado de la sesión del Consejo de marzo 2013, en relación a los mismos se han vuelto a redactar enteramente los artículos sobre los códigos de conducta (artículo 38) y los mecanismos de certificación (artículo 39) y se han introducido nuevos artículos sobre el control de los códigos de conducta (artículo 38 bis) y los organismos y procedimientos de certificación (artículo 39 bis). Igualmente, varios Estados Miembros consideran que hay más margen para incentivar el uso de los códigos aprobados y de los mecanismos de protección de los datos de certificación aprobados mediante el establecimiento de vínculos más estrechos entre estos artículos y el proceso de evaluación de riesgos de los artículos 22, 23, 26 y 30 relativos a las obligaciones del Responsable y del Encargado de la protección de datos, perfeccionando los criterios para distinguir los diferentes tipos de riesgo que puedan dar lugar a diferentes tipos de obligaciones de los Responsables y Encargados. Aparece así en el nuevo texto la utilización de datos seudónimos como medio para

ponderar las obligaciones del Responsable y del Encargado de la protección de datos en determinados casos.

Las asociaciones y otros organismos que representen a categorías de responsables del tratamiento en varios Estados Miembros podrán presentar a la Comisión proyectos de códigos de conducta, así como modificaciones o ampliaciones de códigos de conducta existentes.

3. BLOQUE TEMÁTICO RELATIVO A PROCESOS DE DEFENSA O RECLAMACIÓN.

3.1. DERECHO A PRESENTAR UNA RECLAMACIÓN ANTE UNA AUTORIDAD DE CONTROL (ARTÍCULO 73).

De acuerdo con el artículo 73, las personas físicas o naturales, definidas en la Propuesta de Reglamento UE de Protección de Datos como interesados, están legitimadas para presentar reclamaciones cuando el tratamiento de los datos que les conciernen, no se efectúe de acuerdo con lo que dispone dicha Propuesta. Las reclamaciones vinculadas con la ejecución de tratamientos no acordes con la Propuesta de Reglamento UE de Protección de Datos, tienen un contenido amplio: acceso, rectificación, olvido y supresión, oposición, hechos que supongan la conculcación de las obligaciones del Responsable o del Encargado del tratamiento, entre otras. Conforme a este precepto, están legitimadas para interponer una reclamación, las personas físicas, calificadas como interesados, y las personas jurídicas (organismos, asociaciones, organizaciones) cuya finalidad sea “proteger los derechos e intereses de los interesados” en materia de protección de datos al ostentar un interés legítimo para presentar la reclamación ante la Autoridad de Control. El artículo 73 también contempla la posibilidad de que los interesados y/o las personas jurídicas citadas anteriormente, presenten la reclamación ante “la Autoridad de Control de cualquier Estado Miembro” de la UE cuando el tratamiento de los datos personales no responda a los requerimientos de Propuesta de Reglamento UE de Protección de Datos.

3.2. DERECHO A UN RECURSO JUDICIAL CONTRA UNA AUTORIDAD DE CONTROL (ARTÍCULO 74).

Conforme a este artículo 74 de la Propuesta de Reglamento UE de Protección de Datos, cuando la Autoridad de Control no informe al interesado respecto del “curso o resultado de la reclamación” en el plazo de 3 meses, o no cursara la misma, el interesado puede interponer un recurso judicial, ante los órganos jurisdiccionales del Estado Miembro donde la Autoridad de Control está establecida. El contenido del recurso judicial guarda relación con la tutela de los derechos del interesado: acceso, rectificación, oposición, olvido y supresión, etc. También están legitimados para interponer un recurso judicial contra las decisiones de una Autoridad de Control, los organismos, asociaciones, organizaciones, que cita el anterior artículo 73. El interesado, de acuerdo con el artículo 74, también puede solicitar a la Autoridad de Control del Estado Miembro, donde habitualmente reside, que ejercite en su nombre, una acción ante una Autoridad de Control competente de otro Estado Miembro cuya decisión le concierne.

3.3. DERECHO A UN RECURSO JUDICIAL CONTRA UN RESPONSABLE O ENCARGADO (ARTÍCULO 75).

Tal y como prevé el artículo 75 de la Propuesta de Reglamento UE de Protección de Datos, y sin perjuicio de los recursos administrativos disponibles, las personas físicas tendrán derecho a un recurso judicial cuando consideren que los derechos que les asisten han sido conculcados como consecuencia de un tratamiento de sus datos personales no coherente con la citada Propuesta. Las acciones contra un Responsable o Encargado deberán ejercitarse ante los órganos jurisdiccionales del Estado Miembro en el que el Responsable o Encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los órganos jurisdiccionales del Estado Miembro en que el interesado tenga su residencia habitual, a menos que el Responsable sea una autoridad pública que actúa en ejercicio del poder público. Los Estados Miembros deberán ejecutar las resoluciones definitivas de los órganos jurisdiccionales indicadas.

3.4. NORMAS COMUNES PARA LOS PROCEDIMIENTOS JUDICIALES (ARTÍCULO 76).

El artículo 76 de la misma contempla la opción de que las Autoridades de Control establecidas en los países de la UE puedan acudir a los órganos jurisdiccionales para reforzar la coherencia del régimen europeo de protección de datos personales y que el contenido de la Propuesta de Reglamento UE de Protección de Datos se observe. Esta tarea de "armonización" implica el suministro de información entre los órganos jurisdiccionales localizados en los Estados Miembros, para saber si el órgano jurisdiccional competente del Estado al que se dirige el primero, tiene en curso un procedimiento paralelo, contemplando la opción de que el órgano jurisdiccional que solicita la información, cuando aprecie identidad en la medida, decisión o práctica pueda suspender el procedimiento que inició.

3.5. DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD (ARTÍCULO 77).

Según el artículo 77, cualquier persona natural que sufra un perjuicio derivado de una operación de tratamiento ilegal o vinculado con un acto incompatible con la Propuesta de Reglamento UE de Protección de Datos, tiene derecho a obtener una indemnización que repare el daño causado por el Responsable o Encargado del tratamiento. Este derecho a la indemnización puede sustanciarse en un marco de responsabilidad civil extracontractual como contractual. Para que la indemnización sea factible, el perjuicio sufrido debe tener una estrecha conexión con una operación de tratamiento ilegal o con un acto no compatible con la Propuesta de Reglamento UE de Protección de Datos. El daño producido puede tener carácter de emergente o implicar un lucro cesante. El perjuicio sufrido hay que acreditarlo y evaluarlo. Cuando concurren varios responsables o encargados del tratamiento, el artículo 77 plantea que la responsabilidad es solidaria para quienes intervienen en el tratamiento de datos personales, los mismos deben asumir el importe total de los daños. Esto no excluye que uno de corresponsables acredite que no es posible imputársele los hechos que generaron el daño, pues su actuación fue diligente, concurren causas de fuerza mayor, por ejemplo, quedando exonerado de la obligación de indemnizar el perjuicio causado mediante el abono de la cuantía de indemnización que le correspondiere.

4. TRATAMIENTO ESPECÍFICO DE LOS DATOS DE LOS MENORES (ARTÍCULOS 6, 8, 11, 17, 33, 38 Y 52).

Si por algo se caracteriza la nueva propuesta regulatoria europea en materia de Protección de Datos personales es, precisamente, por la introducción de modificaciones normativas de interés en torno a la licitud y condiciones del tratamiento de los datos personales de los niños respecto a los servicios de la sociedad de la información que se les ofrecen de forma directa. Así, el mero hecho de introducir, por primera vez, una definición legal de “niño” a través del artículo 4 de la Propuesta de Reglamento UE de Protección de Datos, basada en la Convención de Naciones Unidas sobre Derechos del Niño, -y que no incluía la Directiva 95/46/CE-, ya supone un importante avance que pone de relieve la importancia de esta materia. Entre otros, la proyectada reforma normativa ofrece los siguientes elementos de interés:

- Consolida el principio de protección específica a los menores como principio informador del sistema.
- Plantea una especial consideración de los intereses, derechos y libertades de los niños en el juicio o evaluación que deba realizarse respecto a la determinación del interés legítimo del responsable.
- Implica la obligatoriedad en el uso de un lenguaje accesible, claro, llano y fácilmente comprensible para los menores respecto a cualquier información y comunicación que se les dirija.
- Posibilita la especificación por la Comisión de formularios tipo en relación con el tratamiento de datos personales de los niños.
- Reconoce la especial pertinencia de los derechos de rectificación y del «derecho al olvido» en el caso de que los interesados hubieran dado su consentimiento siendo niños.
- Prevé que sólo será lícito tratar datos de menores de 13 años si media la autorización de su correspondiente representante legal. El responsable del tratamiento, por tanto, hará esfuerzos razonables para obtener un consentimiento verificable, teniendo en cuenta la tecnología disponible. Será posible la adopción de medidas específicas para las microempresas y PYMES.
- Propone que la Comisión pueda: 1) Especificar los criterios y condiciones aplicables a los métodos de obtención del consentimiento verificable, así como para establecer formularios normalizados a tal fin; 2) Determinar los criterios y condiciones en relación con el consentimiento de los niños y; 3) Adoptar formularios tipo en relación con el consentimiento de los niños.
- Respecto a la evaluación del impacto relativa a la protección de datos, cuando las operaciones de tratamiento entrañen riesgos específicos para los derechos y libertades de los interesados, entre las que se citan, el tratamiento de datos personales en ficheros a gran escala relativos a niños, prevé que el responsable del tratamiento deba recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto.

- En lo relativo a la elaboración de códigos de conducta, promueve que se tenga especialmente en cuenta la información y la protección de los niños.
- Potencia que las Autoridades de Control realicen actividades de sensibilización sobre los riesgos, normas, garantías y derechos relativos al tratamiento de datos personales, con especial atención a los niños.

CONCLUSIONES

Del análisis realizado cabe concluir que, sin duda, la Propuesta de Reglamento UE de Protección de Datos tendrá un impacto significativo en los derechos de los interesados, en aspectos como:

- Se refuerzan los principios de transparencia y de información adaptada, accesible, inteligible, clara y sencilla.
- Se homogeniza en un mes el plazo de respuesta al ejercicio de derechos.
- Se regula el “derecho al olvido”, expresión que tiene diferentes variantes en función de los datos a que pueda referirse y de los efectos que se pretendan de la misma.
- Se incorpora al interesado como una de las partes a comunicar la concurrencia de una brecha de seguridad, lógicamente cuando le afecte, y en diferentes plazos depende si hablamos de la Propuesta de la Comisión o del Consejo.
- Se establecen diversas vías para la reclamación por la vulneración de los derechos regulados, que pueden llegar hasta la civil para la reclamación de daños.
- Se regulan de manera específica, detallada y con cierto nivel de precisión que resulta necesario (veremos si suficiente o no), los derechos de los menores y los requisitos para el tratamiento de sus datos personales.

BIBLIOGRAFÍA / REFERENCIAS.

Carta de los Derechos Fundamentales de la UE.

Sebastián Zarate Rojas "La problemática entre el derecho al olvido y la libertad de prensa". Marzo-mayo 2013. .

Nilo Jääskinen. Conclusiones del Abogado presentadas el 25 de junio del 2013. Asunto C131/12:

Agencia Española de Protección de Datos. Memoria 2011.

Casino Ruiz, Miguel Ángel. "El periódico de ayer, el derecho al olvido en internet y otras noticias". Civitas Revista española de Derecho Administrativo nº 156/2012.

Lacasta Casado, Ramón, y otros, Auditoría de la Protección de Datos, Editorial Bosch, S A, Barcelona 2009.

Llácer Matacás, María Rosa, Coordinadora, Protección de Datos Personales en la Sociedad de la Información y la Vigilancia, La Ley, Wolters Kluwer España, S A, Madrid 2011.

Palomar Olmeda, Alberto, Codirector, y otros, Comentario al Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Editorial Aranzadi, S A, Pamplona 2008.

Sierra Gil de la Cuesta, Ignacio, Coordinador, Tratado de Responsabilidad Civil, Editorial Bosch, S A, Barcelona 2008.

Wright, David, and Paul de Hert, , Springer, Dordrecht, 2012.

Privacy Impact Assessment Overview, Privacy Impact Assessment Guide, Privacy Impact Assessment International Study by ICO.

The state of the art in privacy impact assessment- David Wright-Brussels 2012.

Finn, Rachel, David Wright y Michael Friedewald, "Siete tipos de la privacidad", en Serge Gutwirth, Yves Poullet et al. (eds.),

Protección de datos europea: la mayoría de edad, Springer, Dordrecht, 2013.

Raab, Charles and David Wright, "", Chapter 17, in David Wright and Paul De Hert (eds.), Privacy Impact Assessment , Springer, Dordrecht, 2012.

Self Regulation and Codes of Practice-Data Protection Comissioner.

Article 29 Working Party papers nº 74, 107, 108 y 204.

Les règles internes d'entreprise (BCR)-Un code de conduite pour les entreprises- CNIL.



Cap. 6

Seguridad:

Análisis de riesgos,
RLOPD y Estándares
de Seguridad de
la Información.

1. ANÁLISIS DE RIESGOS HACIA HERRAMIENTAS PET Y LA EVALUACIÓN PURA DE LA PROTECCIÓN DE LA PRIVACIDAD.

RESUMEN

A diferencia del actual RLOPD, que detalla en su Título VIII la relación de medidas de seguridad que se deben implementar según la naturaleza de los datos, la Propuesta de Reglamento UE de Protección de Datos introduce un enfoque basado en el riesgo, de modo que las medidas técnicas y organizativas de seguridad deben venir determinadas por una previa evaluación de riesgos.

Esto supone un importante cambio, en el que se modifica la obligatoriedad de implementar un catálogo de medidas de seguridad concretas por la responsabilidad de evaluar el riesgo que entraña para la privacidad el tratamiento de datos, así como la implementación de las medidas de seguridad apropiadas para mitigar estos riesgos.

Otra importante novedad es la introducción de la variable de los costes de las medidas de seguridad. La determinación de controles, en respuesta a los riesgos identificados, deberá tener en cuenta las técnicas existentes y los costes de implementación, lo que establece una clara decisión por la gestión de la privacidad basada en riesgos. No obstante, se introduce una indeterminación respecto a cómo valorar si un determinado coste se considera excesivo.

Por otro lado, las modificaciones propuestas en mayo de 2013 por el Consejo introducen el concepto de utilización de seudónimos, promoviendo siempre que sea posible un tratamiento de los datos de forma que no sean atribuidos a una persona física sin el uso de información adicional. En este contexto, cabe destacar el papel que las herramientas PET (Privacy Enhancing Technologies) podrán desempeñar, en cuanto que su utilización, tenida en cuenta desde el diseño de los nuevos tratamientos de datos, pueden disminuir el riesgo para la privacidad y, por tanto, las medidas de seguridad adicionales necesarias.

CONTENIDO

El Responsable del Fichero o Encargado de Tratamiento deberá identificar los riesgos que supone el tratamiento de datos en términos de privacidad de los interesados y cumplimiento de la normativa europea.

La evaluación de riesgo debe ir más allá de la mera observancia del tratamiento de datos propuesto y la identificación y recomendación de controles a implementar. Durante la realización de este ejercicio, se debe evaluar si existen alternativas que sin suponer una pérdida de funcionalidad presenten un menor riesgo de privacidad y, en consecuencia, unos menores requisitos de seguridad. Se deberán contestar a preguntas como estas:

- ¿Es necesario recopilar todos los datos de carácter personal pretendidos? ¿Podría ofrecer el servicio a los usuarios de forma anónima?
- Si no es así, ¿Cuáles son los datos mínimos que necesito sin perder funcionalidad?

- ¿Quién necesita acceder a qué datos? ¿He identificado el personal estrictamente necesario que necesitará acceso a los datos de carácter personal?
- ¿Puedo trabajar con datos seudónimos? ¿puede al menos una parte del personal trabajar con ellos?

Es en este punto donde las herramientas PET, tenidas en cuenta desde el diseño del nuevo tratamiento de datos, pueden ayudarnos a disminuir el riesgo de privacidad, y por tanto las medidas de seguridad adicionales necesarias y los costes de implementación.

El concepto de herramientas PET se extiende a tecnologías para proteger o mejorar la privacidad de una persona. Tradicionalmente, las herramientas PET han estado asociadas a herramientas que proporcionan un grado de anonimato a las personas, que les permiten proteger su verdadera identidad, permitiendo al usuario utilizar servicios de forma anónima manteniendo el control sobre su información, que revela sólo cuando es estrictamente necesario.

La opción de la anonimización de los datos personales, en la que no se registran datos que identifican a un individuo, supone la máxima protección de los datos personales y el inmediato cumplimiento de los requisitos legales. No obstante, por supuesto no siempre es posible aplicar anonimización en tanto que el registro de los datos personales sea un elemento esencial. En estos casos, una técnica PET importante se refiere a la separación de los datos en varios entornos. Un entorno contiene los datos personales de identificación y los demás entornos el resto de información que concierne a cada uno de los individuos que, por separado, no tienen sensibilidad en cuanto a protección de datos personales, ya que por sí solos no son atribuibles a una persona identificable.

Estas posibilidades de seudonimización se mencionan de forma reiterada en el texto propuesto en mayo de 2013 por el Consejo de Europa en diferentes ámbitos del documento. Cabe señalar que estas técnicas permiten a responsables y encargados aplicar las medidas de seguridad adecuadas para proteger los datos personales de forma más racional, centrándose donde es estrictamente necesario.

Una vez determinado el nuevo tratamiento de datos, se deberá tener en cuenta que la evaluación del riesgo de privacidad debe abarcar todo el ciclo de vida de los datos. Esta evaluación de riesgos debe tener en cuenta las amenazas, en base a su probabilidad e impacto, tanto de la protección de los datos personales y la privacidad de los interesados, como del riesgo de cumplimiento para la organización que entraña cada una de estas fases.

Los responsables y encargados deberán atender a la tipología de datos recabados, finalidad, los flujos de información, acceso por parte de terceros, cesiones, tratamiento, conservación o destrucción de los datos, entre otros aspectos. Para ello, será necesario mantener un método sistemático de análisis, que identifique qué vulnerabilidades presenta el nuevo tratamiento de datos respecto a los diferentes controles de privacidad necesarios.

Al respecto, la propuesta de normativa europea no menciona un método de análisis de riesgo concreto, por lo que se podría tomar de referencia cualquiera de los métodos más extendidos en el mercado. Existen diversos estándares y buenas prácticas que podrían tomarse como base (CRAMM, ISO/IEC 27005, MAGERIT, etc.), si bien en la práctica las organizaciones tienden a generar sus propias instancias de estos métodos tomando como base una de estas normas o incluso una combinación de las mismas.

En cualquier caso, la evaluación de riesgos deberá contemplar los distintos ámbitos que puedan llegar a afectar a la privacidad de los distintos grupos de afectados sobre los que se vaya a realizar un tratamiento de datos. En la siguiente tabla, se muestra el catálogo de controles de privacidad propuesto por el NIST (National Institute of Standards and Technology), lo que podría ser un marco de referencia para la realización de la evaluación de riesgo de privacidad.

CONTROLES DE PRIVACIDAD
<i>Legitimidad y Finalidad</i>
Legitimidad para la recolección de los datos
Finalidad del tratamiento de datos
<i>Accountability, auditoría y riesgos</i>
Gobierno de la privacidad
Análisis de Impacto de Privacidad y evaluación de riesgos
Requisitos de privacidad con prestadores de servicios
Monitorización y Auditoría
Formación y Concienciación
Reporte cumplimiento
Seguridad en el Ciclo de Vida de Desarrollo del Software
Control y Registro de Acceso a la información
<i>Calidad e Integridad del dato</i>
Calidad del Dato
Integridad del Dato
<i>Minimización y retención de los datos</i>
Utilización mínima de datos personales
Retención y Destrucción del dato

El hecho de seguir un método sistemático de evaluación de riesgos debe enriquecerse con los nuevos retos para la privacidad que la evolución tecnológica pueda ir presentando, teniendo en cuenta que ésta siempre se presenta previamente a la legislación que le sea de aplicación. Conceptos ya conocidos como el *Cloud Computing*, las *Redes Sociales*, uso de *APPs*, o la más reciente *Big Data*, son algunos de los ejemplos que me-

recen actualmente una especial atención del evaluador. Cabe señalar en este bloque los actuales riesgos que actualmente presenta el conocido como BYOD (*Bring Your Own Device*), en cuanto a la pérdida de control sobre la información que supone el hecho de que ésta se encuentre en un dispositivo personal del trabajador.

Para cada uno de los controles de privacidad que sean de aplicación, se debe observar qué posibles vulnerabilidades introduciría el nuevo tratamiento de datos. Los riesgos de privacidad detectados deberán mitigarse, trasladarse o aceptarse justificadamente, momento en el que se identificarán y propondrán las medidas de seguridad técnicas y organizativas necesarias para garantizar una seguridad adecuada de los datos.

EN CONCLUSIÓN

La Propuesta de Reglamento UE de Protección de Datos requiere que Responsables y Encargados de tratamiento asuman el papel de proteger la privacidad de los afectados más allá de la implementación de una serie de medidas de seguridad concretas. Serán, por tanto, los propios responsables y encargados quienes deberán evaluar el riesgo que supone para la privacidad de los afectados en tratamiento de datos que realizan.

Esta evaluación de riesgo puede conllevar a una mayor conciencia sobre la necesidad de ceñirse a los tratamientos de datos estrictamente necesarios, lo que podría impulsar la utilización de tecnologías que minimicen el riesgo de privacidad mediante técnicas de seudonimización o anonimización de la información, aumentando de este modo las garantías de protección de la información personal de los ciudadanos.

Por otro lado, la indeterminación en la propuesta de normativa respecto a la aplicación de medidas de seguridad, dejando a Responsables y Encargados de tratamiento la labor de evaluar los riesgos y determinar las medidas de seguridad en función de su coste de implementación, podría dar lugar a que determinados sectores adoptaran tolerancias al riesgo no deseables, que se deberán corregir, por ejemplo, mediante autorregulación.

2. REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS.

RESUMEN

La Propuesta de Reglamento UE de Protección de Datos promueve un enfoque global de la protección de los datos de la ciudadanía, y por ende de la protección de su privacidad, en los 27 países de la Unión Europea. Para llevarlo a cabo pretende introducir una serie de medidas que garanticen el derecho a la privacidad de la ciudadanía en el uso y tratamiento de sus datos personales, ya por los servicios proporcionados desde la sociedad de la información, los nuevos sistemas fruto del avance de las nuevas tecnologías o los sistemas tradicionales. Todo ello con independencia de que estos tratamientos sean realizados por entidades públicas o privadas, que se encuentren dentro de la Unión o que presten servicios a su ciudadanía, aunque no se encuentren establecidos en la misma, lo que pretende eliminar demarcaciones territoriales en el actual contexto de globalización.

CONTENIDO

En el año 2004 el Diccionario de la lengua española (DRAE) reconoce el término privacidad como el *“ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”*.

El principal garante de la privacidad en la recogida y el tratamiento de los datos personales es la necesidad de obtener el consentimiento del interesado. A este respecto la Propuesta de Reglamento UE de Protección de Datos, amplía el concepto de consentimiento del interesado, en relación al establecido en el RLOPD, estableciendo que este además de representar la manifestación de voluntad, libre, inequívoca, específica e informada para el tratamiento de sus datos personales, deberá ser explícito, deduciéndose claramente que el afectado acepta de una forma clara y precisa al tratamiento de sus datos. Esto implica que el tratamiento sólo será lícito si se dispone con este consentimiento o responde alguna de las excepciones contempladas por el Reglamento UE, no dejando cabida a otras excepciones que pueden presentarse para ciertos tratamientos, donde resulta complejo solicitar el consentimiento previo a la recogida, como por ejemplo en la instalación de determinadas cookies como las analíticas, abriendo la posibilidad de poder oponerse al tratamiento inmediatamente después de la recogida. Al mismo tiempo, establece que, la responsabilidad de probar que éste consentimiento ha sido otorgado recae sobre el responsable del tratamiento y que éste consentimiento puede ser revocado en cualquier momento.

Otro aspecto de gran relevancia, que también afecta al consentimiento, es la importancia que la Propuesta de Reglamento UE de Protección de Datos otorga a la privacidad de los niños en su relación con los servicios de la sociedad de la información. Para ello se establece que este tratamiento sólo podrá realizarse, en el caso de menores de 13 años, cuando se haya recabado previamente el consentimiento del padre o tutor del niño. Por el contrario, la normativa actual se presenta más restrictiva, donde el RLOPD establece ésta barrera en los de 14 años y no sólo en los servicios en línea sino en todos los ámbitos, aspectos que suponen adicionalmente retos tecnológicos. Por el contrario, se consideran menor de edad, a los menores de 18 años. Así mismo, indica expresamente que el responsable del tratamiento hará los esfuerzos razonables para obtener este consentimiento de forma verificable y teniendo en cuenta la tecnología disponible. A este respecto, cabría esperar que se considera como “esfuerzos razonables”, y si este “esfuerzo” se medirá igual si se trata de una pequeña o gran empresa, sin dar cabida a aplicar estos criterios para recabar el consentimiento como se expuso en el ejemplo de cookies del apartado anterior.

La Propuesta de Reglamento UE de Protección de Datos incorpora nuevos principios en la de protección de datos a los ya existentes (calidad, información, deber de secreto y consentimiento), como son el “principio de transparencia” en la recogida y tratamiento de los datos, en las relaciones del interesado con el encargado del tratamiento mediante el establecimiento de mecanismos sencillos para el ejercicio de sus derechos y en las relaciones con las Autoridades de Control. Este principio debería redundar en un cambio de orientación en la redacción de las actuales políticas de privacidad y condiciones de uso, favoreciendo la comprensión de las mismas.

El “principio de rendición de cuentas” (accountability) en la gestión que se hace de los datos personales, obligando al responsable del tratamiento a adoptar políticas e implementar medidas apropiadas para asegurar y poder demostrar que el tratamiento de los datos personales se lleva conforme a lo indicado en la Propuesta de Reglamento UE de Protección de Datos.

Como elemento novedoso, cabe destacar también la regulación del “derecho al olvido” cuyo ejercicio por parte de los afectados se enfrenta actualmente a un vacío legal, teniendo que ser ejercitado con la normativa actual, mediante la solicitud del ejercicio del derecho de cancelación o el de oposición. En particular, este derecho obliga a los responsables del tratamiento a suprimir los datos y a abstenerse de dar más difusión sin demora. En el caso de medios de comunicación y boletines oficiales este concepto se entiende como el establecimiento de mecanismos que limiten su localización a través de las técnicas de indexación en los motores de búsqueda. Si bien es cierto, esta última medida no deja de ser una buena práctica cuyo limitante simplemente recae en el buen hacer de estos motores de búsqueda, lo que no impide técnicamente su acceso.

Este vacío incita nuevas oportunidades tecnológicas que deban desarrollar la posibilidad de disponer de un control efectivo de los datos por parte del usuario en un contexto globalizado.

También se regulan las circunstancias que habilitan su ejercicio, entre las que se contempla, cuando los datos personales hayan sido proporcionados por el interesado siendo menor de edad, aludiendo a que no se es consciente de los riesgos que implica el tratamiento.

Por otro lado se introduce el “derecho de oponerse a la elaboración de perfiles”, mediante el cual se garantiza que toda persona tiene derecho a oponerse al tratamiento de sus datos cuando estos tenga por objeto evaluar aspectos de su personalidad, o su rendimiento profesional, económico, etc.

Otro cambio importante respecto a la normativa actual, es la determinación de las medidas de seguridad a aplicar, el RLOPD establece la implementación de medidas con el establecimiento de tres niveles de seguridad acumulativos en función del nivel de los datos tratados, claramente tipificados. Por el contrario la Propuesta de Reglamento UE de Protección de Datos obliga a los responsables y encargados del tratamiento a implementar medidas técnicas y organizativas que garanticen la seguridad de los tratamientos en función de los riesgos a los cuales están expuestos, la naturaleza de los datos y el coste de implementarlo, aspecto que podría inclinar una cierta subjetividad. Es aquí donde aparece como novedad el concepto de “Privacy Impact Assessment” que permitirá precisamente analizar este impacto sobre la privacidad de los datos cuando los tratamientos entrañen riesgos específicos para los derechos y libertades de los interesados en función de su naturaleza, alcance o fines con el fin de determinar las correspondientes medidas de seguridad.

Si bien es cierto que estas nuevas obligaciones presentan un alineamiento con normativas y estándares de seguridad internacionales, no se concreta la metodología a seguir.

Otro aspecto importante es el concepto de “Data Breach Notification”, obligación impuesta a los responsables o encargados del tratamiento de notificar a las Autoridades de Control las “fugas de información”, introduciendo este nuevo concepto y definiéndose como toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados, o tratados de otra forma.

Esta notificación deberá de realizarse en un plazo no superior a 24 horas una vez se haya tenido constancia de la misma. Pero esta obligación, va más allá, cuando se tengan sospechas de que puede afectar a la privacidad de los afectados, esta comunicación deberá de hacerse extensible a los mismos. Obligación que presenta ciertas ambigüedades en la tipificación del tipo de incidente a comunicar, y el escaso margen de tiempo para su realización. Esto se traduce en un gran cambio en la concepción de la gestión de los incidentes de seguridad que afectan a los datos personales por parte de las empresas y las instituciones.

El gran cambio en la concepción de la privacidad viene de la mano de la introducción de un nuevo precepto, la protección de los datos personales desde el diseño y por defecto: “Data protection by design and by default.” El concepto es clave pues consiste en introducir la seguridad como un requisito más, involucrando a los diferentes stakeholders de la organización, evaluando el impacto de la privacidad con anterioridad a la puesta en marcha de cualquier acción que implique un tratamiento de datos personales.

A este respecto, en relación a la adquisición y/o desarrollo de productos de software de seguridad acordes a la normativa implica que los proveedores de soluciones de tratamiento de datos deberán incluir esta concepción de requisito en el desarrollo de las mismas. Esta obligación está en gran parte en consonancia con la Disposición Adicional Única del RLOPD, que recoge que estos productos deberán de incluir una descripción técnica del nivel de seguridad alcanzado.

Por otro lado, la Propuesta de Reglamento UE de Protección de Datos hace referencia a la introducción de mecanismos y sellos de certificación en protección de datos, aporta otro aspecto novedoso, iniciativa que de llevarse a cabo, dará garantías de privacidad a los afectados por el tratamiento de sus datos y condicionará la elección de las empresas y organismos a las cuales confiarán sus datos.

Por último, los Estados Miembros estarán obligados a la creación de Autoridades de Control que contribuyan a fomentar el conocimiento de los ciudadanos de los riesgos, garantías, normas y derechos que les asisten a la par de investigar las reclamaciones que se les remitan. Estas funciones, en la actual normativa recaen a nivel estatal sobre la Agencia Española de Protección de Datos y a nivel autonómico sobre la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos. Además la Propuesta de Reglamento UE de Protección de Datos prevé la designación de una “ventanilla única” frente a la cual podrán ejercitar sus derechos los afectados, en aquellos casos, que el responsable o encargado del tratamiento se encuentre establecido en varios Estados Miembros. Esta “ventanilla única” recaerá sobre la Autoridad de Control

en la que se encuentre el principal establecimiento del Responsable o Encargado del tratamiento.

EN CONCLUSIÓN

Por consiguiente la Propuesta de Reglamento UE de Protección de Datos pretende garantizar el derecho a la privacidad mediante la implementación de medidas que redunden en un mayor control respecto al tratamiento de sus datos por parte de los individuos y reforzando las obligaciones impuestas a los responsables y encargados del tratamiento de los ficheros que presten sus servicios dentro de la Unión Europea. No obstante, cada vez resulta de una mayor complejidad la determinación de la ubicación de la información derivada de paradigmas como el Cloud Computing.

La generación de confianza es un aspecto clave para garantizar el desarrollo de la sociedad de la información. A este respecto la Propuesta de Reglamento UE de Protección de Datos establece la necesidad de incorporar la privacidad desde su concepción. Este punto adquiere vital importancia en los productores de software, que deberán de incorporar la seguridad como requisito en función de los riesgos existentes.

No se debe olvidar que la aplicación de la norma no es un proceso aislado, sino su aplicación coexiste con otras normas existentes. No cabe duda de que un mayor control de la información incide sobre una menor exposición de los datos. Es por ello que, por un lado, este proceso de actualización debería de incidir sobre regulaciones actuales, en especial en el ámbito de la administración pública donde es posible que se deban redefinir obsoletos procedimientos como por ejemplo las notificaciones colectivas basadas en boletines oficiales, en aras de garantizar un verdadero y mayor control de la información.

No obstante, por otro lado, en este contexto cabe un análisis sobre si la tecnología actual responde ante un cumplimiento efectivo que garantice realmente la privacidad de la información. Es posible que esta viabilidad este marcada por la necesidad de inversiones ante proyecto de I+D+i donde la seguridad supone un claro reto para el crecimiento estratégico de las organizaciones y en general de la Sociedad de la Información. Retos como desarrollar mecanismos tecnológicos para servicios Cloud que permitan limitar la exposición de datos a través de técnicas de cifrado transparentes donde el cliente tenga el control de su información, más allá de las establecidas en transito, nuevos mecanismos de autenticación más allá de los tradicionales o incluso desarrollo de herramientas.

3. ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN.

La adopción de estándares, buenas prácticas, marcos de referencia y/o normativas reconocidas en el ámbito de la Seguridad de la Información puede considerarse como un factor determinante que favorece e incluso garantiza el adecuado cumplimiento de lo dispuesto en la Propuesta de Reglamento UE de Protección de Datos. Existen diferentes y diversos estándares que, de forma total o parcial, establecen un adecuado conjunto de medidas, protocolos,

etc. a seguir en materia de seguridad de la información. Atendiendo a la cantidad y diversidad de publicaciones existentes hemos creído conveniente centrarnos en aquellas más representativas y que tienen un mayor alineamiento con la Propuesta de Reglamento UE de Protección de Datos. Esta relación de estándares y buenas prácticas son:

A) ESTÁNDARES ISO (International Organization for Standardization)

Normas internacionales de una entidad de reconocido prestigio y con un amplio despliegue a nivel internacional. Con relación a la seguridad de la información destacamos las siguientes referencias:

ISO/IEC 27001:2005 (Information Security Management System - Requirements)

ISO/IEC 27002:2005 (Code of Practice for Information Security Management)

ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation)

ISO/IEC 13335 (IT Security Management)

ISO 31000 (Risk management — Principles and guidelines)

B) BRITISH STANDARDS INSTITUTION (BSI)

De forma similar a ISO, BSI es una entidad reconocida internacionalmente que ha elaborado distintos estándares y buenas prácticas relativas a la seguridad de la información y aspectos relacionados.

C) PCI DDS - PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Estándar desarrollada por las principales compañías comercializadoras de tarjetas de crédito con el objetivo de mejorar la seguridad de los datos involucrados en las transacciones financieras a través de distintos medios de pago.

D) COBIT (ISACA)

CobiT (Control Objectives for Information and related Technology) es un marco de referencia focalizado en el Gobierno de las IT. Está desarrollado por el ITGI (IT Governance Institute) de la Information Systems Audit and Control Association (ISACA).

E) ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)

Marco de referencia desarrollado por la OGC (Office of Government Commerce) que describe un conjunto de prácticas recomendadas (best practices) en la entrega de los servicios TI.

F) INFORMATION SECURITY FORUM (ISF)

ISF publica periódicamente un informe o estándar de buenas prácticas relativas a la seguridad de la información.

Adicionalmente a estas referencias también hay que considerar la significativa cantidad de normas, marcos de referencia, etc. existentes, que dentro de un ámbito geográfico concreto y/o sectorial para una industria determinada (SOX, HIPAA, etc.), complementan el alcance estos estándares principales. Del mismo modo, también existen distintas entidades, organismos, asociaciones, etc. (NIST, ISSA, ASISonline, ENISA, IETF, ETSI, etc.) de toda índole que a distintos niveles desarrollan estándares de seguridad de la información y/o aspectos afines.

4. ASPECTOS DE PRIVACIDAD EN ISO/IEC 27001:2013

INTRODUCCIÓN

La Propuesta de Reglamento UE de Protección de Datos pretende establecer un nuevo enfoque global que responda mejor al rápido desarrollo de las tecnologías.

Este nuevo enfoque global incluye una nueva perspectiva en lo que se refiere al nivel de protección de los datos personales en el aspecto tecnológico. Un nivel de protección adecuado aplicado en el almacenamiento y tratamiento de los datos personales ha de garantizar la disponibilidad, autenticidad, integridad y confidencialidad de estos.

La norma ISO/IEC 27001:2013, que proporciona un modelo de Sistema de Gestión de la Seguridad de la Información, puede ayudar a establecer los requisitos necesarios para garantizar el nivel de protección necesario en el almacenamiento y tratamiento de los datos personales, así como cumplir con los nuevos requerimientos establecidos en la Propuesta de Reglamento UE de Protección de Datos.

DESARROLLO

La norma ISO/IEC 27001:2013 puede servir de guía para poder definir e implementar políticas, procesos, sistemas y controles de seguridad en una organización partiendo de un análisis y tratamiento de riesgos de la información, en la que están incluidos los datos personales, adaptados a las necesidades de la organización.

Todas las organizaciones, independientemente de su tamaño, naturaleza o tipo, pueden aplicar esta norma para gestionar la mayoría de requerimientos de seguridad que establece la propuesta de Reglamento.

Siguiendo las directrices de la norma ISO/IEC 27001:2013, para poder establecer un sistema de gestión de seguridad de la información en una organización es imprescindible la máxima implicación de la Dirección de la organización aportando su compromiso y liderazgo en la implementación del sistema.

Otro aspecto muy importante es tener un alto conocimiento de la organización tanto a nivel interno como externo, en los aspectos más importantes que puedan ser relevantes y afecten a la información.

Una vez sentadas las bases definidas anteriormente se ha de decidir el sistema de análisis y gestión del riesgo que se va a utilizar y establecer los criterios a seguir.

Una vez determinados los riesgos se han de determinar las medidas para mitigarlos y es aquí donde se pueden aplicar los controles definidos en el anexo A de la norma ISO/IEC 27001:2013 y que se detallan en otra norma relacionada: ISO/IEC 27002:2013 Código de Buenas prácticas para la gestión de la seguridad de la información.

La norma ISO/IEC 27001:2013 también define como establecer los objetivos de seguridad, los recursos y competencias, la planificación, el seguimiento y evaluación, la mejora continua y otros aspectos relacionados con la gestión de la seguridad.

Los controles y los objetivos de control de referencia a aplicar para la mitigación de los riesgos de seguridad incluyen los siguientes:

- Políticas de seguridad.
- Organización de la información.
- Seguridad en recursos humanos.
- Gestión de activos de información.
- Control de accesos.
- Criptografía.
- Seguridad física y ambiental.
- Seguridad en las operaciones.
- Transferencia de información.
- Adquisición de sistemas, desarrollo y mantenimiento.
- Relación con proveedores.
- Gestión de los incidentes de seguridad.
- Continuidad de negocio.
- Cumplimiento con requerimientos legales y contractuales.

El desarrollo en detalle de cómo aplicar estos controles y sus objetivos están en la norma ISO 27002;2013.

CONCLUSIONES

Las normas ISO/IEC 27001:2013 y ISO/IEC 27002:2013 pueden ayudar a todas las organizaciones a aplicar los requerimientos que se establecen en la Propuesta de Reglamento UE de Protección de Datos para proteger los datos personales así como el resto de información que es responsabilidad de la organización tanto si la gestiona ella misma como si la gestiona un tercero.

BIBLIOGRAFÍA/REFERENCIAS

Dutch data protection authority - Privacy enhancing technologies – a white paper for decision makers (2004)

http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf?refer=true&theme=purple

NIST- National Institute of Standards and Technology - SP800-53 Rev.4. Security and Privacy Controls for Federal Information Systems and Organizations (2013)

ENISA - Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools (2006)

Agencia Española de Protección de Datos / Guía sobre el uso de las cookies (2013).

Diario de Sesiones del Congreso de los Diputados” / Comparecencia del señor director de la Agencia Española de Protección de Datos (Rodríguez Álvarez), para informar sobre la memoria de la Agencia Española de Protección de Datos correspondiente al año 2011. A petición propia. (Número de expediente 212/000483) (2012).

Article 29 Data Protection Working Party. Working Document 02/2013 providing guidance on obtaining consent for cookies

<https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards>

<https://www.securityforum.org/shop/p-71-167>


<http://www.infosec.gov.hk/english/technical/files/overview.pdf>

<http://www.iso27001security.com/html/others.html>

<http://www.nisc.go.jp/eng/pdf/K304-101e.pdf>

ISO/IEC 27001:2013. Sistemas de Gestión de la Seguridad de la Información.

ISO/IEC 27002:2013. Código de buenas prácticas para la gestión de la seguridad de la información.



Cap. 7
Accountability:
cómo demostrar el
cumplimiento de
manera continuada
y sostenible

ABSTRACT

El apartado empieza definiendo lo que es *Accountability*, cómo, cuándo y dónde surge y dónde está más extendida, todo ello dentro de un planteamiento formal y general. A continuación pasa al terreno de la Privacidad y la Protección de Datos donde se comentan sus inicios, quiénes empezaron, el porqué de la necesidad de la misma y los tipos existentes.

Continúa con un resumen de las pautas que el Grupo de Trabajo del Artículo 29 (GT29) establece en el Dictamen 3/2010 sobre esta materia.

También, y aunque el estudio se realiza sobre el borrador de Reglamento de enero de 2012 emitido por la Comisión Europea, se exponen las tendencias que marca la propuesta del Consejo de la Unión Europea de mayo de 2013.

Es importante reseñar lo que establecen otras *accountabilities* para mejor entender este concepto, concretándose en las siguientes:

- Principios de *accountability* para el desarrollo sostenible: Norma de principios de *accountability* AA1000APS (2008).
- Stakeholder Engagement Handbook.
- ISO 26000:2010 - Guía de responsabilidad social.
- Global Reporting Initiative (GRI).
- *Accountability* educacional: posibilidades y desafíos para América Latina a partir de la experiencia internacional (CIDE y PREAL).

Por último, se establecen los vectores de principios y medidas que servirán para el correspondiente estudio de los artículos del borrador de Reglamento que se encuentran en el ámbito de lo que entendemos como *accountability*.

En concreto los siguientes principios:

1. La obligación de la organización de adoptar políticas internas tomando en consideración criterios externos, es decir, con los objetivos que marca la Ley.
2. Mecanismos que pongan en práctica las políticas de privacidad, incluyendo herramientas, formación, concienciación y educación.
3. Sistemas internos que aseguren que las herramientas funcionan, mediante revisiones y verificaciones o auditorías externas.
4. Transparencia y mecanismos de participación individual.
5. Medios de solución y aplicación de posibles brechas o incidentes de seguridad.

Y las siguientes medidas:

1. Establecer una política de seguridad.
2. Sancionar el proyecto de *accountability* al máximo nivel de la organización.
3. Disponer de personal dedicado a la función de la privacidad y que esté formado y especializado mediante el desarrollo de políticas de formación y sensibilización.

4. Revisar periódicamente las políticas y los riesgos.
5. Implementar mecanismos para gestión de incidentes y reclamaciones de usuarios.
6. Implementar mecanismos de *enforcement* interno.
7. Establecer un mecanismo interno de tratamiento de quejas.
8. Aplicar procedimientos de verificación y supervisión que garanticen que las medidas no sean solo nominales sino que se apliquen y funcionen en la práctica (auditorías internas o externas, etc.).
9. Establecer la posibilidad de *enforcement* externo.

DESARROLLO

ACCOUNTABILITY

El término “*accountability*” puede definirse de diversas maneras, una de ellas se refiere al deber de informar de las políticas y actuaciones de una organización, de justificar sus actos y de someterse a cualquier tipo de control adecuado para verificar la consistencia de la información.

Surge de la necesidad de hacer más transparentes las acciones y decisiones y de dar cuenta de las políticas y las prácticas que realiza la mencionada organización en todas sus facetas. Esto hace que también se le dé la acepción de “rendición de cuentas”. Sin embargo, el concepto *accountability* es más amplio puesto que añade el concepto de responsabilidad al de rendición de cuentas. El segundo concepto corresponde a una obligación legal, mientras que el primero conlleva más una obligación moral y proveniente de una decisión voluntaria de la organización.

La *accountability* es una responsabilidad del órgano de gobierno como actuación colegiada, el cual debe informar no sólo sobre aspectos pragmáticos como el de las actuaciones realizadas (gestión), sino también de otros aspectos que forman parte de la política y la ética del gobierno y que afectan a su propio modo de actuar.

Este concepto aparece en los años 60 en Estados Unidos y llega a Europa en los 70, estando más extendida en el mundo anglosajón.

Después del planteamiento general de lo que significa *accountability* y equiparando la Organización o Compañía con el Responsable del Tratamiento de datos de la Normativa sobre Protección de Datos Personales, se llega a lo que este término significa o puede significar en el terreno de la Privacidad y la Protección de datos. En este caso y dentro de la Unión Europea se trata de lograr la aplicación de medidas apropiadas y eficaces que garanticen la observancia de los principios y obligaciones que dispone la Directiva 95/46/CE (en este momento), así como la disposición y demostración de ese cumplimiento cuando se lo solicitaran las Autoridades de Control. Para ello se ha procedido a su inclusión en la futura Normativa europea de Protección de Datos para trasladar sus principios de la teoría a la práctica.

Para ello, en el año 2009 nace el Proyecto Galway (grupo de trabajo internacional cuyos miembros provienen del sector público y privado, con la función de dar una definición de elementos que deben definir un proyecto de *accountability*), con la idea originaria de servir para mejorar los flujos de datos internacionales y mejorar la gestión interna de protección de datos. En este mismo año se dan los Estándares internacionales de Madrid (“Propuesta Conjunta de Estándares Internacionales de Protección de Datos y Privacidad”), que tienen otra definición que se centra en la adopción de medidas para cumplir la norma y para poder demostrar que se cumple.

El proyecto continúa en el año 2010 en París centrándose en cómo el Regulador puede realizar las mediciones y qué parámetros puede una organización obtener para demostrar que cumple. La tercera fase del proyecto aborda cómo verificar que una organización sea “*accountable*”, analizándose los medios de verificación y estableciéndose los elementos de

comprobación que significan que una organización cumple, no solo de lo obligatorio sino de una disponibilidad a demostrar que tiene medidas y que éstas funcionan.

También se estudió la posibilidad de emitir certificaciones, aspecto que no sólo tiene en cuenta el mínimo de medidas legales a respetar sino también su grado de cumplimiento e incluso el grado de excelencia de cumplimiento más allá de los mínimos legales. En este sentido, se hablaba de dos tipos: general (cumplir la ley) y voluntaria (algo más que cumplir la ley) lo que puede dar lugar a sellos de cumplimiento (muy parecido a lo que ahora lo llamamos autorregulación).

Por la importancia que tiene en esta materia el Dictamen 3/2010 del GT29 conviene resumir las pautas de lo que este grupo de trabajo establece en cuanto a sus aspectos fundamentales:

- I. El GT29 establece lo que considera que deben ser las bases para, en la futura modificación de la Normativa europea sobre Protección de Datos, establecer el llamado principio de responsabilidad o "*accountability*".

El reconocimiento expreso del principio de responsabilidad figura en las Directrices sobre Privacidad adoptadas en 1980 por la OCDE. Recientemente fue incluido en los Estándares internacionales de Madrid, desarrolladas por la Conferencia Internacional de Autoridades de Protección de Datos en 2009. También ha quedado incorporado a la propuesta de norma más reciente de ISO 29100 y es uno de los conceptos principales del Marco de privacidad de CEAP y de sus normas de privacidad transfronteriza. Asimismo se alude a la responsabilidad en los principios de información leal de Canadá incluidos en su Ley de Protección de la Información Personal y de Documentos electrónicos. Por último, las Normas Corporativas Vinculantes (Binding Corporate Rules o BCRs) que se utilizan en el contexto de las transferencias de datos internacionales reflejan el principio de responsabilidad.

- II. El GT29 parte de la base de que, para respetar adecuadamente la protección de datos dentro de una organización, es necesario que forme parte de los valores comprometidos y las prácticas de ésta. Ya en su documento sobre "El Futuro de la Privacidad" (WP 168), manifestaba que el vigente marco jurídico se había mostrado insuficiente para garantizar que los requisitos de protección de datos se tradujeran en mecanismos eficaces que aportaran una auténtica protección y, por tanto, que era necesario que se incluyera un principio de responsabilidad en la revisión de la Directiva 95/46. No obstante, hay que tener en cuenta que una disposición sobre responsabilidad en realidad no representa una gran novedad, puesto que no impone requisitos que no estuvieran ya implícitos en la legislación vigente.

El principio de responsabilidad requiere que los responsables de tratamientos de datos apliquen medidas adecuadas y eficaces para poner en práctica los principios y obligaciones de la Directiva y además demostrar este extremo cuando se les solicitara.

Pero la propuesta debe aportar seguridad jurídica, a la vez de estar formulada en términos suficientemente amplios como para que aquella sea modulable.

- III. El término "*accountability*" no es fácil de traducir fuera del mundo anglosajón, de donde proviene, y apunta sobre todo al modo en que se ejercen las competencias y al modo en

que esto puede comprobarse. Sólo cuando la responsabilidad funciona en la práctica puede desarrollarse la confianza suficiente.

Como complemento al principio de responsabilidad se pueden diseñar requisitos particulares, como la obligación de realizar evaluaciones de impacto sobre la privacidad o el nombramiento de responsables de protección de datos.

- IV. La “arquitectura jurídica” de los mecanismos de responsabilidad plantearía dos niveles:
1. Un requisito reglamentario básico para todos los Responsables del Tratamiento, con dos elementos:
 - a. La aplicación de medidas/procedimientos.
 - b. El mantenimiento de pruebas de dicho extremo.
 2. Sistemas discrecionales de responsabilidad que superaran los requisitos jurídicos mínimos de los principios subyacentes de protección de datos y las modalidades de aplicación o de garantía de la eficacia de las mismas.
- V. Una propuesta concreta del principio de responsabilidad, para el GT29, debería fomentar la adopción de medidas concretas y prácticas, convirtiendo los principios generales de protección de datos en estrategias y procedimientos concretos definidos al nivel del Responsable del Tratamiento de datos en cumplimiento de las leyes y reglamentos aplicables. El tipo de medidas no se especificaría en el texto de la disposición general sobre responsabilidad. Posteriormente, las orientaciones que dieran las Autoridades nacionales de Protección de Datos, el GT29 o la Comisión podrían especificar el mínimo de medidas específicas que constituyeran medidas adecuadas.

Para la aplicación eficaz de dichas medidas sería necesario atribuir competencias y formar al personal implicado en las operaciones de tratamiento, designando además responsables de protección de datos. Cuando el tratamiento sea más amplio o complejo o de alto riesgo, la eficacia de las medidas adoptadas deberá verificarse periódicamente, mediante seguimientos o auditorías externas o internas.

A pesar de ello, no debe olvidarse que la observancia del principio de responsabilidad no implica necesariamente que el responsable del tratamiento cumpla los principios materiales de la Directiva, es decir, no ofrece presunción jurídica de cumplimiento ni sustituye a ninguno de dichos principios.

Algunas medidas comunes de responsabilidad, según el GT29, podrían ser:

- Establecimiento de procedimientos internos previos a la creación de nuevas operaciones de tratamientos de datos.
- Establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos.
- Cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de operaciones de tratamiento de datos.

- Nombramiento de un responsable de protección de datos y otras personas responsables.
- Formación a los miembros del personal.
- Establecimiento de procedimientos de gestión del acceso y de las demandas de corrección y eliminación de datos con transparencia para las personas interesadas.
- Establecimiento de un mecanismo interno de tratamiento de quejas.
- Establecimiento de procedimientos internos eficaces de gestión y notificación de fallos de seguridad.
- Realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas.
- Aplicación y supervisión de procedimientos de verificación que garanticen que las medidas no sean solo nominales, sino que se apliquen y funcionen en la práctica (auditorías internas o externas, etc.).

VI. Estas medidas han de ser modulares, puesto que un enfoque de “talla única” tan sólo forzaría a los Responsables del Tratamiento a embutirse en estructuras mal adaptadas y acabaría fracasando. La modulación estaría en función de los riesgos y la naturaleza de los datos, el tamaño de las operaciones, los objetivos declarados del tratamiento, las transferencias de datos previstas y el tipo de datos tratados, de modo principal.

Para evitar que una excesiva flexibilidad pueda abocar a la incertidumbre, se aconseja que la Comisión o el propio GT29 establezcan directrices de armonización para aportar mayor seguridad. También sería útil desarrollar un programa de cumplimiento de datos tipo, con se hizo con las BCRs.

VII. El papel de las Autoridades de Protección de Datos en este contexto no queda relegado, ni hurtado de competencias, sino que las beneficiará, puesto que tendrán la competencia de recabar del Responsable del Tratamiento pruebas de cumplimiento del principio de responsabilidad. Si la información que solicite la autoridad no se proporciona, esta tendrá causa directa de actuación contra los Responsables del Tratamiento, independientemente de la supuesta violación de otros principios. Por tanto, la actividad de las autoridades se centrará más en su función “ex post” que en su función “ex ante”.

Si un responsable del tratamiento no respeta sus compromisos en políticas internas vinculantes podrá ser sancionado, a mayores de la violación concreta de los principios materiales de protección de datos.

Por último, las Autoridades de Protección de Datos también podrán tener un papel clave en el desarrollo de normas de certificación y desempeñar un papel en la certificación de los organismos de certificación.

Aunque este apartado se desarrolla fundamentalmente sobre el borrador de Reglamento de la Comisión europea de enero 2012, conviene mostrar las modificaciones propuestas por el Consejo de la Unión Europea mayo de 2013:

- Este trabajo no ha sido acordado por todas las Delegaciones y está pendiente de ser revisado por las delegaciones de Chequia, Hungría, Holanda, Polonia y Reino Unido.
- En este documento hay Delegaciones que consideran que la forma jurídica escogida no es la adecuada, sino que preferirían una directiva.
- A lo largo de este último mandato, de Presidencia irlandesa, ha habido intensos debates del Capítulo IV (Obligaciones del Responsable y del Encargado), concretamente el artículo 22 (Obligaciones del Responsable del Tratamiento).
- Se le ha dado una nueva redacción con una “cláusula horizontal”, basada en el riesgo. Esto significa que la naturaleza, contexto, alcance y objetivos de las actividades de tratamiento y los riesgos que surgen por los derechos y libertades de los interesados se tendrán en cuenta para determinar las medidas apropiadas que han de adoptar el Responsable de acuerdo con el Reglamento.
- Dentro del enfoque basado en el riesgo, se han ajustado las obligaciones de notificación de las violaciones de datos.
- Se han perfeccionado los criterios para distinguir los diferentes tipos de riesgo que puedan dar lugar a diferentes tipos de obligaciones de los Responsables y Encargados.
- Se está desarrollando la aplicación de forma voluntaria de los códigos de conducta y los mecanismos de certificación por parte de los Responsables y Encargados, como medio para demostrar el cumplimiento del Reglamento. En el curso de los debates sobre el Capítulo IV, se han perfeccionado los criterios para distinguir los diferentes tipos de riesgo que puedan dar lugar a diferentes tipos de obligaciones de los Responsables y Encargados.

OTRAS ACCOUNTABILITY

Con objeto de dar una mayor visibilidad de lo que representa el concepto objeto de este apartado del Estudio en otros sectores, parece adecuado mostrar otras *accountabilities*:

PRINCIPIOS DE ACCOUNTABILITY PARA EL DESARROLLO SOSTENIBLE: NORMA DE PRINCIPIOS DE ACCOUNTABILITY AA1000APS (2008)

Define *Accountability* como “*el reconocimiento, asunción de responsabilidad y actitud transparente sobre los impactos de las políticas, decisiones, acciones, productos y desempeño asociado a una organización*”. La norma pretende ayudar a las organizaciones que desarrollan un enfoque responsable y estratégico de la sostenibilidad a entender, gestionar y mejorar su desempeño.

Incluye tres principios básicos *Accountability*:

1. Inclusividad: Implicación con grupos de interés.
2. Relevancia: Determinación de la relevancia e importancia de un asunto para la organización y sus grupos de interés.
3. Capacidad de Respuesta: Respuesta de una organización a los asuntos de los grupos de interés que afectan su desempeño en materia de sostenibilidad, siendo responsable ante ellos.

STAKEHOLDER ENGAGEMENT HANDBOOK

En este manual se establecen una serie de buenas prácticas sobre el compromiso con los *stakeholders*. Esto es lo que el Marco de la Serie AA1000 denomina el principio dominante de 'inclusividad'. Se señala que la inclusividad se logra a través de la adhesión a tres principios fundamentales:

1. Relevancia ("*Materiality*"): Requiere saber qué temas preocupan y son importantes para su organización y sus *stakeholders*.
2. Exhaustividad ("*Completeness*"): Supone la comprensión y la gestión de los impactos relevantes y las opiniones y necesidades pertinentes de los *stakeholders*, además de sus percepciones y expectativas.
3. Capacidad de respuesta ("*Responsiveness*"): Implica responder a los impactos relevantes y a las inquietudes de los *stakeholders*.

ISO 26000:2010 GUÍA DE RESPONSABILIDAD SOCIAL

Esta es una norma internacional que proporciona orientación a todo tipo de organizaciones sobre conceptos, términos y definiciones en materia de responsabilidad social, entre otros:

- Rendición de cuentas: Una organización debe rendir cuentas por:
 - Los impactos de sus decisiones y actividades en la sociedad, la economía y medio ambiente, especialmente las consecuencias negativas significativas.
 - Las acciones tomadas para prevenir la repetición de impactos negativos involuntarios e imprevistos.
- Transparencia: Una organización debería ser transparente en sus decisiones y actividades que impactan en la sociedad y el medio ambiente:
 - Revelar de forma clara, precisa y completa y en un grado razonable y suficiente la información sobre las políticas, decisiones y actividades de las que es responsable, incluyendo sus impactos conocidos y probables.
 - Esta información debería estar fácilmente disponible y ser directamente accesible y entendible para aquellos que se han visto o podrían verse afectados de manera significativa.
 - Debería ser oportuna y basada en hechos.
 - Debería presentarse de manera clara y objetiva, para permitir que las partes interesadas evalúen con exactitud el impacto que las decisiones y actividades de la organización producen sobre sus respectivos intereses.
- Respeto a los intereses de las partes interesadas: Identificación e involucramiento con las partes interesadas.

GLOBAL REPORTING INITIATIVE (GRI)

La elaboración de una memoria de sostenibilidad comprende la medición, divulgación y rendición de cuentas (*accountability*) frente a grupos de interés internos y externos en relación

con el desempeño de la organización con respecto al objetivo del desarrollo sostenible.

ACCOUNTABILITY EDUCACIONAL: POSIBILIDADES Y DESAFÍOS PARA AMÉRICA LATINA A PARTIR DE LA EXPERIENCIA INTERNACIONAL (CIDE Y PREAL)

Señala que *accountability* es en parte una rendición a los interesados o involucrados por los resultados del proceso educativo, lo que a su vez se espera tenga como consecuencia un aumento de los niveles de responsabilización de cada actor sobre tal proceso.

Se identificaron 4 condiciones necesarias para un sistema de *accountability* educativa:

1. Estándares: Conocer los resultados esperados de las escuelas.
2. Información: Es necesario contar con información sobre dichos resultados.
3. Consecuencias: Es necesario contar con un sistema objetivo de *accountability* que incluya consecuencias si el desempeño cae por debajo de los estándares deseados.
4. Autoridad: Las escuelas (y las comunidades que estas atienden) deben contar con autoridad para efectuar cambios y mejoras.

CONCLUSIONES

Por último y a modo de resumen, el desarrollo de este subapartado quiere proponer una serie de principios y medidas basados en diferentes fuentes, que se entienden aplicables a la *accountability* en Privacidad y Protección de Datos. En concreto, los siguientes **cinco principios esenciales**:

1. Compromiso de la Organización para la “rendición de cuentas” así como la adopción de políticas internas coherentes. Una organización debe demostrar su voluntad y capacidad de ser responsable y rendir cuentas por el tratamiento de datos que realice. La política interna a implementar debe ser acorde a criterios externos como son las exigencias legales o códigos de buenas prácticas. Debe proporcionar al individuo un vehículo de protección eficaz de su privacidad, e implementar mecanismos de supervisión. Todo ello se debe aprobar por la organización en su más alto nivel y, a su vez, aplicarse a todos los niveles de la organización.
2. Mecanismos para poner en práctica la política de privacidad, incluyendo herramientas que faciliten su conocimiento y cumplimiento, y formación/concienciación: Se deben buscar herramientas que faciliten la toma de decisiones para la protección y uso adecuado de los datos, la formación sobre el uso de esas herramientas y procesos para asegurar el cumplimiento por parte de los usuarios dentro de la entidad.
3. Sistemas de supervisión continua a nivel interno y estudios de control y verificación externa: Las empresas que recopilan y utilizan la información personal deben supervisar y validar si las políticas que se han adoptado y aplicado son eficaces para proteger y asegurar los datos.

Se deben establecer programas para garantizar que los mecanismos se utilizan de manera adecuada por los usuarios de los datos personales internos y externos a la propia

entidad.

Se deberán realizar auditorías con carácter periódico a través de una entidad independiente o bien internamente a fin de verificar y demostrar que cumple con los requisitos de rendición de cuentas. En el caso de que la auditoría se realizase de manera interna, los auditores deberán reportar los resultados a una entidad independiente de la organización.

4. Transparencia y mecanismos de participación individual: Para facilitar la participación individual, los procedimientos de la organización deben ser transparentes. En este apartado existen dos elementos clave, como son: la articulación de procedimientos de información dentro la organización, y la publicación de un aviso de privacidad. Las entidades responsables pueden promover la transparencia a través de avisos de privacidad, iconos, vídeos u otros mecanismos.

5. Medios para la reparación del daño causado: La organización debe establecer en su política de privacidad medios para reparar el daño que se pueda causar a las personas en el tratamiento de sus datos personales por el fracaso de las políticas y prácticas internas. Se debe identificar a una persona dentro de la organización que asuma la función de ser el primer punto de contacto para la resolución de controversias y establecer un procedimiento en virtud del cual las quejas sean revisadas y tratadas. También se podría externalizar este servicio para atender y resolver las quejas de los usuarios.

Tales principio se concretarían en las **siguientes medidas**:

1. Establecer una política de seguridad: Establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos (p.e., cumplimiento de los criterios de calidad de datos, notificación, principios de seguridad, acceso, etc.) que deben ponerse a disposición de las personas interesadas.

2. Sancionar el proyecto de *accountability* al máximo nivel de la organización.

3. Disponer de personal dedicado a la función de la Privacidad y que esté formado y especializado mediante el desarrollo de políticas de formación y sensibilización:

a. Nombramiento de un Responsable de Protección de Datos y otras personas responsables de la protección de datos,

b. Oferta adecuada de protección de datos y formación a los miembros del personal; esto debe incluir a los procesadores (o responsables del proceso) de datos personales (como los directores de recursos humanos), pero también a los administradores de tecnologías de la información, directores de unidades comerciales, etc.,

c. Deben asignarse recursos suficientes para la gestión de la privacidad.

4. Revisar periódicamente las políticas y los riesgos.

5. Implementar mecanismos para gestión de incidentes y reclamaciones de usuarios, para la gestión del acceso y de las demandas de corrección y eliminación de datos, con transparencia para las personas interesadas.

6. Implementar mecanismos de *enforcement* interno:
 - a. Establecimiento de procedimientos internos previos a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación, etc.),
 - b. Cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de operaciones de tratamiento de datos,
 - c. Establecimiento de procedimientos internos de gestión y notificación eficaces de fallos de seguridad,
 - d. Realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas.
7. Aplicar procedimientos de verificación y supervisión que garanticen que las medidas no sean solo nominales, sino que se apliquen y funcionen en la práctica (auditorías internas o externas, etc.).
8. Establecer la posibilidad de *enforcement* externo.

ARTÍCULOS DEL REGLAMENTO DE LA UE,
RELACIONADOS CON LOS PRINCIPIOS BÁSICOS DE ACCOUNTABILITY A APLICAR

	PRINCIPIO 1	PRINCIPIO 2	PRINCIPIO 3	PRINCIPIO 4	PRINCIPIO 5
ARTÍCULOS					
5.F	X				
11.1				X	
12		X		X	
17.7	X		X		
22.1	X		X		
22.2 A) C) Y E)	X	X	X		
23.1		X	X		
23.2	X	X			
29.1		X			
29.2		X			
30.1	X				
30.2	X				
31.1		X			X
31.4		X			X
32.1				X	
33.1		X			X
34.6			X		X
35.1		X			
36.1					
37.1		X			
38.1		X		X	
39.1			X	X	
42.2 A) B) C) Y D)	X				

*Los preceptos del Reglamento de la UE señalados en rojo, son aquellos directamente relacionados con *Accountability*.

ARTÍCULOS DEL REGLAMENTO DE LA UE, RELACIONADOS CON LAS MEDIDAS A APLICAR

ARTÍCULO	MEDIDA 1	MEDIDA 2	MEDIDA 3	MEDIDA 4	MEDIDA 5	MEDIDA 6	MEDIDA 7	MEDIDA 8	MEDIDA 9
5.F	X								
11.1	X				X	X			
12	X				X	X			
17.7								X	
22.1	X					X			
22.2 A) C) Y E)			X			X			X
23.1	X					X			
23.2	X					X			
29.1								X	X
29.2								X	X
30.1						X			
30.2						X			
31.1	X					X		X	X
31.4	X					X		X	
32.1	X					X			
33.1	X					X			
34.6						X		X	X
35.1			X						
36.1									
37.1	X	X	X	X	X	X	X	X	X
38.1	X			X	X	X		X	
39.1								X	X
42.2 A) B) C) Y D)	X	X							

*Los preceptos del Reglamento de la UE señalados en rojo, son aquellos directamente relacionados con *Accountability*.

RELACIÓN ENTRE LOS PRINCIPIOS BÁSICOS Y LAS MEDIDAS A APLICAR EN ACCOUNTABILITY

MEDIDAS

	PRIMERA	SEGUNDA	TERCERA	CUARTA	QUINTA	SEXTA	SÉPTIMA	OCTAVA	NOVENA
PRINCIPIOS									
PRIMERO	X			X	X	X	X	X	X
SEGUNDO	X		X	X	X	X	X		
TERCERO	X			X	X	X	X	X	X
CUARTO	X	X	X		X	X	X		
QUINTO	X				X	X			

BIBLIOGRAFÍA / REFERENCIAS

Dictamen 3/2010, sobre principios de responsabilidad, Grupo de trabajo del artículo 29.

Estándares Internacionales de Protección de Datos y Privacidad (2009).

Recursos y Publicaciones de "The Centre for Information Policy Leadership"

AA10000APS Norma de principios de accountability (2008).

Directrices sobre Privacidad de la OCDE (1980).

ISO 29100 (Information technology — Security techniques — Privacy framework).

Marco de privacidad de CEAP (Foro de Cooperación Económica Asia-Pacífico).

Stakeholder Engagement Handbook

ISO 26000:2010 Guía de responsabilidad social

Global reporting initiative (GRI)

The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal - WP 168

Accountability educacional: posibilidades y desafíos para américa latina a partir de la experiencia internacional (CIDE y PREAL)

Cutt, J. y Murray, V. (2000): Accountability and Effectiveness Evaluation in Non-Profit Organizations. Routledge. London.

Gray, R. (et al) (1996): Accounting and accountability, changes and challenges in corporate and environmental reporting. Prentice Hall.

Slim, H. (2002): GAT Authority? The Legitimacy and Accountability of Non-governmental organisations.



Más información www.ismsforum.es

C/ Castelló, 24, 5º Derecha, Escalera 1 28001 Madrid T.: 34 91 186 13 50