TEMA 09

1. *La protección de datos.*
2. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Obligaciones de la ley especialmente aplicables a las sociedades mercantiles estatales.*
3. *El Reglamento (UE) 2016/679, de 27 de abril, 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. Principios y derechos. Obligaciones.*

SINDICATO LIBRE

VERSION 2020

1. La protección de datos.

1.1. Introducción

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), establece en su punto 1 que "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

El Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, fue publicado en el BOE número 17, de 19 de enero de 2008. El Título VIII de este reglamento desarrolla las medidas de segundad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

El Reglamento General de Protección de Datos 2016/679, que se empezó a aplicar a partir del 25 de mayo de 2018, recoge como uno de sus principales objetivos acabar con la fragmentación existente en las distintas normativas de los países comunitarios. Además, persigue la adaptación de las normas de protección de datos a la rápida evolución tecnológica y los fenómenos derivados del desarrollo de la sociedad de la información y la globalización.

En el caso de España, tal y como recoge la información del Ministerio, la adaptación de nuestra legislación al Reglamento General de Protección de Datos hace necesaria la elaboración de una nueva Ley Orgánica en sustitución de la actual, cuyas normas y desarrollo deberán ser revisadas y adaptadas para evitar contradicciones. Igualmente, la AEPD deberá desarrollar cuestiones concretas que el reglamento comunitario remite a las autoridades nacionales de control y tendrá que revisar sus tratamientos de datos personales para adaptarlos a esas exigencias.

Novedades destacadas

En el caso de España, donde la protección de datos es un derecho fundamental protegido por el artículo 18.4 de la Constitución, se recogen novedades tanto en el régimen de consentimiento como en los tratamientos y en la introducción de nuevas figuras y procedimientos.

Adelanta a los 13 años la edad de consentimiento para el tratamiento de datos en consonancia con la normativa de otros países de nuestro entorno. Además, se tomará en cuenta el tratamiento de los datos correspondientes a personas fallecidas sobre la base de la solicitud de sus herederos, se excluye la figura del consentimiento tácito que se sustituye por una acción afirmativa y expresa por parte del afectado y se recoge manifiestamente el deber de confidencialidad. En caso de una inexactitud en los datos personales obtenidos de forma directa, se excluye la imputabilidad del responsable de su tratamiento si este ha adoptado todas las medidas razonables para su rectificación o supresión.

Entre las novedades, también se destaca la potenciación de la figura del delegado de protección de datos, persona física o jurídica cuya designación ha de ser comunicada a la autoridad competente, que mantendrá relación con la **AEPD** (Agencia Española de Protección de Datos). Por su parte, la AEPD se configura como autoridad administrativa independiente cuyas relaciones con el Gobierno se realizan a través del Ministerio de Justicia. Se establece la necesaria cooperación y coordinación con las correspondientes autoridades autonómicas de protección de datos.

Tal como se ha señalado, el 31 de julio de 2018 entró en vigor el *Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.* **Su finalidad es adaptar la actual normativa al Reglamento europeo, aunque manteniendo determinados preceptos regulados en la anterior Ley 15/1999 de 13 de diciembre, tal como señala la Disposición final única.** *Vigencia:*

"El presente real decreto-ley entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado» y lo estará hasta la vigencia de la nueva legislación orgánica de protección de datos que tenga por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones."

1.2. La Seguridad de la información en Correos

El Grupo Correos, consciente de la necesidad de proteger la Información, entendida como un activo clave para el desarrollo de su negocio, impulsa la Seguridad Corporativa estableciendo un Área con profesionales especializados en Seguridad de la Información, con la misión de:

- Definir el marco normativo y la estrategia de Seguridad de la Información.
- Analizar periódicamente el valor de Información.
- Evaluar y Gestionar el Riesgo.
- Auditar el cumplimiento frente al marco normativo.
- Representar a la Organización y a sus intereses, respecto a la Seguridad de la información.

El ejercicio de estas funciones se desarrolla mediante la formalización de un conjunto de Servicios, agrupados por ámbitos operativos, que se ofrecen a la Organización interna.

Así, en cuanto a la Auditoría de seguridad de información, este servicio define, ejecuta y registra el programa de Auditorías de Seguridad, informando objetivamente a la Dirección del nivel de cumplimiento de los controles auditándose impulsando la gestión de las acciones recomendadas, en base al riesgo identificado, y enmarcado en el proceso de mejora continua de la Seguridad del Grupo Correos. Coordinar y gestionar las acciones auditoras de segundas y terceras partes, sobre las unidades de Tecnología del Grupo, optimizando la dedicación de los recursos auditados y garantizando la proporcionalidad de la información requerida.

Este servicio permite al Grupo Correos obtener los siguientes beneficios:

- **Evaluar** el nivel de implantación de la política de Seguridad de la Información del Grupo Correos en la Organización y en todos los proveedores de servicios que acceden a la información del Grupo en el desarrollo de sus funciones.
- **Comprobar** el cumplimiento de los requerimientos sobre "Seguridad de la información" que establecen la normativa vigente y nuestros clientes en la contratación de servicios y en el tratamiento de la información.
- **Asegurar** una gestión eficiente de las acciones recomendadas para mitigar o eliminar los riesgos identificados en las auditorías realizadas.
- **Centralizar** la gestión de las auditorías del Grupo Correos en materia de Seguridad de la Información exigidas al Grupo Correos, para dar una única visión del nivel de seguridad tasado.

En esa misma línea se señalan las líneas a seguir en cuanto a **Política de Seguridad de la Información**, de tal forma que las empresas del Grupo Correos reconocen que la información es un activo fundamental de la Organización y declaran que su protección es un objetivo prioritario para el cumplimiento adecuado de los servicios que presta con los niveles de confianza y seguridad exigidos. La Política de Seguridad de la información concierne a toda la Organización y declara el compromiso de la Dirección del Grupo de implantar, documentar y difundir las directrices y requerimientos de seguridad a través del marco normativo desarrollado que culmine en la gestión segura de la Información que trata cada uno de nuestros procesos. A tal fin, la Dirección constituye los siguientes objetivos estratégicos sobre Seguridad de la Información:

- **Mantener unos niveles de seguridad**, en términos de Confidencialidad, Integridad y Disponibilidad, ajustados y coherentes con las necesidades del Negocio y la confianza de nuestros clientes.

- **Constituir el Comité de Seguridad Corporativo** que es el órgano que tiene encomendada la gestión de todo aquello que tenga como objetivo prevenir, salvaguardar y fortalecer la seguridad de los activos de información.

- **Implantar las medidas técnicas y organizativas** que proporcionan el nivel de seguridad adecuado para preservar la información, los sistemas que la soportan y los procesos que la tratan, así como verificar el cumplimiento del marco legal vigente que le sea de aplicación.

- **Difundir** este documento y el marco normativo de Seguridad de la Información que lo desarrolla y **Promover la Formación y Concienciación** en esta materia, a todo el personal de la Organización.

- Crear un **Sistema de Gestión de la Seguridad de la Información** basado en estándares internacionales para identificar, cuantificar, priorizar y tratar los riesgos, así como para evaluar y revisar el desarrollo de la Política de Seguridad de la Información como marco de definición de las directrices básicas de seguridad.

- Establecer un **Sistema de Gestión de la Continuidad de Negocio** que, ante desastres que interrumpan de manera prolongada la actividad de negocio, permita a Correos continuar operando sus procesos críticos, garantizando la entrega de sus productos y servicios, de acuerdo con sus objetivos de empresa y las obligaciones legales existentes.

Todo el personal, interno y colaboradores, está obligado a conocer y cumplir dentro de su ámbito de responsabilidad las medidas de seguridad establecidas en este documento. El acceso a la información y a los sistemas de información estará condicionado a la adhesión a esta Política y a la normativa que la desarrolla, siendo estas de obligado cumplimiento.

1.2.1. Cumplimiento regulatorio. Buenas prácticas

Este servicio identifica y analiza el marco legal existente en materia de Seguridad de la Información (Protección de Datos, Sociedad de la información, Comercio electrónico...) que afecte al Grupo Correos, integrando su contenido en el cuerpo normativo interno y verificando el cumplimiento de las medidas técnicas y organizativas que resulten para garantizar el adecuado cumplimiento de las obligaciones.

A) Objeto

El objeto es establecer de una manera sencilla las pautas de seguridad que son necesarias para hacer un buen uso de los sistemas de información, con el objetivo de que puedan ser conocidas y aplicadas por todos los usuarios de CORREOS y colaboradores y reducir la probabilidad de fallos y daños causados por problemas de seguridad.

Para la elaboración de estas buenas prácticas se han tenido como referencia los criterios establecidos por el Estándar Internacional ISO/IEC UNE-ISO/IEC 27002 adoptando las precauciones necesarias para garantizar el nivel de seguridad exigido por el marco legal vigente en materia de protección de datos de carácter personal (Reglamento General de Protección de Datos -Reglamento UE 2016/679- / Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos / Ley 15/99 de 13 de diciembre/, RD 1720/2007 de 21 de diciembre).

B) Normativa de referencia

Es la siguiente, la ya indicada:

- Reglamento General de Protección de Datos - **Reglamento UE 2016/679**.
- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
- Ley 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal.
- RD 1720/2007 de 21 de diciembre, Reglamento de Medidas de Seguridad sobre ficheros de tratamiento de datos de carácter personal.
- Política de Seguridad de Correos.

Además de la legislación, existen varias normas emitidas por el Organismo Internacional de Estandarización (conocido en sus siglas inglesas, ISO) que cuentan con reconocimiento internacional y que es importante conocer.

- **UNE-ISO/IEC 27001:** Sistema de gestión de seguridad de la información (esta norma sigue el modelo PDCA).
- **UNE-ISO/IEC 27002:** Código de buenas prácticas para la gestión de la seguridad de la información. Este modelo agrupa un total de 133 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información. Está organizado en 11 dominios y 33 objetivos de control.

C) Recomendaciones generales de Seguridad

1. Directrices generales:

- Accede únicamente a la información necesaria para el desarrollo de tus funciones.
- Usa las aplicaciones corporativas. No crees tus propios ficheros y no trabajes en local con información procedente de un sistema de información.
- Utiliza las Unidades de Red para guardar tu trabajo diario.
- El uso de los equipos informáticos y la información de CORREOS es para uso profesional únicamente.
- Evita que las personas que no deban tener acceso a una información determinada puedan conocerla.

2. Protección de la información y de los sistemas de información:

- Ordenadores personales y portátiles:

- Ten activado siempre el salvapantallas con contraseña.
- Siempre que dejes tu puesto de trabajo, aunque sea por un periodo corto de tiempo, bloquea el ordenador.
- Siempre que dejes tu puesto por un periodo largo de tiempo, apaga el ordenador.
- No instales software no autorizado en el ordenador.
- Los portátiles no deben estar desatendidos, si viajas con un portátil, tenlo siempre cerca.
- La eliminación de la información de un ordenador, disco duro, CD/DVD se ha de realizar siempre de forma segura.

- Información en papel:

- Custodia la documentación en todo momento e impide que personas no autorizadas puedan acceder a la información que contiene.

- No dejes información accesible a terceras personas en tu mesa de trabajo, en la impresora o el fax.
- Guarda y almacena la documentación de forma ordenada en armarios y cajones cerrados con llave.
- La destrucción de documentación con información sensible se debe realizar de forma segura de modo que se impida la reconstrucción posterior y el acceso a la información.
- Destruye manualmente los documentos, utiliza las destructoras de papel o usa aquellos medios que Correos pone a tu disposición pero, en cualquier caso, hazlo de forma segura

3. Uso del identificador de usuario y de la contraseña:

- El identificador del usuario (UC) y su contraseña son personales e intransferibles. Te identifican frente al sistema y te hacen responsable de las acciones que se realizan con ellos.
- No comuniques la contraseña a nadie y no la escribas en ningún sitio, es la manera más sencilla de encontrarla y alguien te podría suplantar.
- Si sospechas que alguien conoce tu contraseña de acceso, modifícala.
- Cambia la contraseña periódicamente, como mínimo 1 vez al año.
  - Una contraseña segura se compone como mínimo de 8 caracteres alfanuméricos incluye tanto letras mayúsculas como minúsculas, dígitos y signos de puntuación.
  - Se desaconseja la utilización de nombres comunes fáciles de adivinar o palabras que se puedan encontrar en el diccionario.

4. Uso apropiado del Correo electrónico y de internet:

- Envío de correos electrónicos:

- No envíes información sensible o confidencial por correo electrónico.
- Comprueba antes de enviar un correo electrónico el destinatario y la información que envías.
- No respondas correos de SPAM ni reenvíes mensajes cadena.
- Recuerda que si alguien tiene tu clave de acceso podría mandar correos en tu nombre.

- **Recepción de correos electrónicos:**

- Da tu dirección de correo electrónico solo a personas que conozcas.

- Abre únicamente correos de remitentes conocidos.
- Antes de ejecutar un adjunto, analízalo con el antivirus; si proviene de un desconocido no lo ejecutes, elimínalo automáticamente.
- No uses los ***links*** que aparecen en un correo para acceder a un sitio web.
- Si recibes un correo en el que te solicitan tus datos bancarios, no los envíes y avisa a tu banco inmediatamente.

- **Navegación por internet:**
  - Ten activado el antivirus mientras navegas por Internet.
  - No proporciones información personal en sitios no confiables de Internet.
  - Evita visitar zonas peligrosas, el mero hecho de visitarlas puede provocar un ataque a tu sistema.
  - No realices descargas de sitios no confiables.

5. Software malicioso y antivirus.

Un virus o software malicioso es un programa de ordenador que produce acciones nocivas en el sistema informático en el que actúa. Existen distintos tipos de virus o códigos dañinos como:

- **Virus informáticos**, código que es capaz de generar copias de sí mismo en programas distintos al que ocupa.

- **Gusanos**, código que absorbe recursos del Sistema, de forma creciente, hasta que lo bloquea por saturación.

- **Caballos de Troya**, programa de uso autorizado que contiene código dañino. Cuando este programa comienza a ejecutarse, el código dañino toma el control.

- **Bombas Lógicas**, código que se ejecuta al producirse un hecho predeterminado, por ejemplo, una determinada fecha, un número de encendidos del sistema, determinada secuencia de teclas, etc.

Para evitar el software malicioso, la única recomendación valida es mantener un programa antivirus **instalado, activado y actualizado**.

No abras o ejecutes ficheros recibidos de fuentes desconocidas, ficheros descargados de Internet o recibidos por otros medios (CD, disquetes, etc.) sin haber revisado previamente la posible presencia de virus o cualquier otro ***software*** malicioso.

Notifica al CAU cualquier anomalía que detectes en tu PC.

D) Decálogo de seguridad

1. Emplea los recursos que Correos pone a tu disposición solo para uso profesional.
2. Cierra la sesión y bloquea el equipo cuando te ausentes del puesto de trabajo.
3. Accede exclusivamente a los sistemas de información a los que estés autorizado.
4. Protege las contraseñas, manteniéndolas en secreto y eligiendo una que no esté en el diccionario.
5. Comprueba que tienes activado el antivirus, no abras mensajes de remitentes desconocidos y no ejecutes adjuntos no solicitados.
6. No instales o utilices software que no haya sido proporcionado por Correos.
7. Conoce la Normativa de Seguridad que se encuentra en la intranet.
8. Identifícate de forma visible dentro de cualquier edificio de Correos.
9. Guarda la información de forma adecuada para que no se divulgue a personas no autorizadas.
10. Reporta cualquier incidente de seguridad al Centro de Atención de Usuario (CAU).

1.2.2. Ciclo de vida del Dato

Como activo de la organización, el ciclo que sigue la gestión del dato, desde su momento de recogida hasta cuándo debe ser desechado, debe guiarse por el máximo respeto hacia la salvaguarda de los derechos de los interesados, así como al cumplimiento íntegro del RGPD.

A) Entrada

Base de legitimación. El dato se recaba en base a alguna de las opciones de legitimación que reconoce el RGP:

- Por el consentimiento afirmativo del interesado.
- Por cumplimiento de una obligación legal.
- En base a un interés legítimo.

PrivacybyDesign. Todo tratamiento de datos debe considerarla privacidad desde el diseño o la creación de nuevos proyectos, adoptando las medidas necesarias para asegurar el cumplimiento de la norma y las garantías necesarias en relación con los derechos de los interesados.

B) Gestión

Registro de actividades de tratamiento. Con el RGPD no es necesario declarar los ficheros a la Agencia Española de Protección de datos, pero sí llevar un registro interno donde indicar una serie de información (finalidades, comunicación de los datos, datos del responsable...).

Aproximación a riesgos y medidas de seguridad. Desaparecen las medidas de seguridad estandarizadas por tipo de dato para dar paso a medidas de seguridad acordes al riesgo que el tratamiento de los datos pueda ocasionar al interesado (marginación, exclusión social, contratar servicios...).

DPO. El Delegado de Protección de Datos o DPO es el máximo responsable de la organización en cuestiones de protección de datos, asumiendo tareas de apoyo y asesoramiento en la organización así como de punto de contacto con los interesados y la Agencia Española de Protección de Datos.

Gestión de derechos. El RGPD suma nuevos derechos ejercitables por el interesado. A los denominados ARCO (acceso, rectificación, cancelación y oposición) se añaden los de limitación de tratamiento y el derecho a la portabilidad.

C) Cese del tratamiento

Bloqueo del dato. Una vez el dato no vaya a ser tratado, existirá la posibilidad de bloquear los datos para aquellos casos en los que deba conservarlo.

Cancelación.- O, de eliminarlo del fichero sin posibilidad de recuperarlo.

1.2.3. Medidas de Seguridad. Enfoque basado en riesgos

Todas las organizaciones estamos obligadas a proteger la información que tratamos, garantizando que en el desempeño de nuestras funciones se velará por la protección de la privacidad, evitando toda acción que pueda impactar negativamente en los derechos y libertades de las personas.

A) ¿Qué deben garantizar las medidas de seguridad en el tratamiento de los datos de carácter personal?

Confidencialidad. Deben garantizar que sólo accederán a los datos las personas que tengan la correspondiente autorización.

Integridad. Deben proteger la veracidad y exactitud de los datos.

Disponibilidad. Deben asegurar que los datos permanecerán disponibles.

Resiliencia. Deben comprometer la capacidad de recuperación y establecimiento del estado inicial de los datos en caso de verse afectados por un incidente.

B) ¿Qué medidas deben aplicar las organizaciones?

Antes del RGPD

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento tenían reguladas las medidas que debían aplicar en función del nivel de los datos:

- **Básico**. Identificativos: Nombre, Apellidos, Direcciones de contacto (físicas o electrónicas), Teléfono (fijo o móvil), Otros.

- **Medio**. Infracciones/perfiles: Comisión infracciones penales o administrativas, Ficheros de Solvencia, Ficheros de AA. Tributarias, Seguridad Social y Mutuas, Ficheros de EEFF (Serv. Financieros), Elaboración de perfiles (ej. selección de personal).

- **Alto**. Especialmente protegidos: Ideología, Afiliación sindical, Religión, Creencias, Origen racial, Salud, Vida sexual, Violencia de género, Fines policiales (obtenidos sin consentimiento).

Después del RGPD

Enfoque basado en riesgos:

- **Identificar riesgos**. Las medidas de seguridad deben adoptarse en función del riesgo que supone el tratamiento de los datos para los derechos y libertades de las personas, como pueden ser consecuencias negativas de exclusión social, laboral, etc. Para analizar los riesgos se tendrán en cuenta aspectos como: naturaleza, ámbito, contexto y fines del tratamiento.

- **Aplicar medidas técnicas y organizativas** para garantizar el nivel de seguridad adecuado en función de los riesgos detectados. Toda organización deberá aplicar por tanto las medidas técnicas y organizativas adecuadas para la actividad del tratamiento desarrollada y sus objetivos, algunas de ellas por ejemplo, pueden ser: aplicar la minimización y la seudonimización de los datos, técnicas de cifrado, regular el control de acceso a los datos, etc.

El análisis de riesgos en el RGPD forma parte del principió de **Accountability**: cumplir con la normativa y poder demostrar ese cumplimiento en todo momento.

C) ¿Qué son las Evaluaciones de Impacto sobre la Protección de Datos o "PÍAS"?

Cuando el tratamiento de los datos suponga un alto riesgo para los derechos y libertades de las personas deberá realizarse una Evaluación especial de Impacto en la protección de datos personales.

¿En qué casos?

- En la elaboración de perfiles tras el análisis de los datos, por ejemplo, para el envío de información comercial.

- En el caso de tratamiento de datos a gran escala de categorías especiales (las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical).
- Observación sistemática a gran escala de una zona de acceso público.

D) Conclusiones

- La aplicación de medidas previstas por el RGPD debe adaptarse a las características de las organizaciones y el riesgo que los tratamientos de los datos de carácter personal puedan suponer para los derechos y libertades de las personas.
- Cumplir con los principios de protección de la privacidad y aplicar las medidas que nuestra organización haya implementado garantizará el correcto tratamiento de los datos y la protección de la privacidad.

1.2.4. Información y Consentimiento

En las operaciones de recogida y tratamiento de datos debemos:

- Informar a sus titulares de aspectos relativos al tratamiento de sus datos.
- Obtener su consentimiento para realizar el tratamiento.

A) Información

1. Antes del RGPD

Se informa a los interesados sobre:

- La finalidad del tratamiento de datos.
- El responsable del tratamiento.
- Los derechos de los interesados: ARCO. (Acceso, Rectificación, Cancelación y Oposición).

2. Después del RGPD

Además:

- Base legitimadora del tratamiento (ej.: relación contractual, obligación legal, consentimiento e interés legítimo).
- Plazos de conservación.
- Identidad y canal de comunicación con el DPO.
- Cesiones de datos personales (ej.: seguridad social).

- Nuevos derechos: limitación en el tratamiento y portabilidad.

Toda esta información debemos proporcionarla de manera:

- Sencilla.
- Clara.
- Comprensible.

B) Consentimiento

1. Antes del RGPD

El consentimiento se otorga: De manera Tácita o Expresa (Sólo en algunos casos, como en supuestos de tratamiento de datos especialmente sensibles, el consentimiento debe ser expreso).

2. Después del RGPD

Solo de manera expresa y con estas características:

- **Inequívoco y positivo:** entendido siempre con un **"Sí"**.
- **Explícito:** otorgado de manera sencilla y detallada.
- **Específico:** para cada uno de los tratamientos que se vayan a realizar sobre los datos.

El consentimiento tiene que darse siempre mediante un acto afirmativo:

SI/FIRMA/ACEPTO

Solo con el compromiso visible y sostenido de todos los miembros de la organización conseguiremos alcanzar los objetivos en materia de privacidad.

Crear una auténtica cultura de cumplimiento es responsabilidad de todos.

2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Obligaciones de la ley especialmente aplicables a las sociedades mercantiles estatales.

La Ley Orgánica 3/2018 de 5 de diciembre de protección de datos personales y garantía de los derechos digitales (en adelante LOPDGDD), representa entre otras muchas cosas, y por lo que al sector sanitario se refiere, la oportunidad perdida de haber conseguido para los datos sanitarios la tan deseada como necesaria regulación legal propia y específica.

En efecto, como es sabido la LOPDGDD objeto de comentario sigue la senda de la derogada LOPD y proyecta su ámbito de aplicación sobre el conjunto de los datos personales, si bien con algunas referencias aisladas a sanidad en su disposición adicional decimoséptima y la disposición final novena, que inevitablemente hay que completar con la lectura del Reglamento UE 2016/679 de 27 de abril.

Un buen ejemplo del carácter complementario/subsidiario de la Ley respecto del Reglamento de la UE se advierte, por ejemplo, en la ausencia de una definición legal de "*dato sanitario*" que, en cambio, sí nos lo proporciona la referida disposición comunitaria en su artículo 4, distinguiendo entre: a) datos genéticos, b) datos biométricos, y c) datos relativos a la salud.

No obstante el artículo 12.5 de la LOPDGDD parece contemplar la primacía de los regímenes especiales que, en materia de protección de datos de carácter personal, pueden establecerse por otras leyes, como bien podría ser el caso de las leyes sanitarias enumeradas en el apartado primero de la disposición adicional decimoséptima. En concreto, dicho precepto legal establece "*cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el capítulo tercero del Reglamento 2016/ 679, se estará a lo dispuesto en aquellas*".

Veamos muy brevemente desde una perspectiva sanitaria los aspectos más relevantes del marco normativo actual en materia de protección de datos, destacando todos aquellos en los que puedan existir diferencias con la legislación sectorial, o bien adquieran especial interés para el ámbito sanitario.

Tratamiento de datos de personas fallecidas.

La LOPDGDD, al igual que el Reglamento comunitario, excluye de su ámbito de aplicación el tratamiento de datos personales de personas fallecidas (art. 2.2.b). Sin embargo el legislador nacional, en su artículo 3, ha querido regular el acceso a los datos personales del fallecido por parte de aquellas personas vinculadas a éste por razones familiares o de hecho, así como sus herederos.

Desde el punto de vista de la legislación sanitaria, el art. 18.4 de la Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, distingue en cuanto al régimen jurídico de acceso a la historia clínica del paciente fallecido según si la petición de acceso la protagoniza un familiar, o si ésta la formula un tercero.

En el primer caso hay que entender que las personas vinculadas al paciente por razones familiares (considerando como tales al cónyuge, ascendientes y descendientes y hermanos si nos ajustamos a lo dispuesto en el art. 4 de la LO 1/82) o de hecho, pueden acceder a la historia clínica salvo que

el fallecido se hubiera opuesto y así se acredite, y en todo caso siendo de aplicación las mismas limitaciones que regirían para el propio paciente si estuviese vivo, a saber: a) la intimidad de terceras personas, b) anotaciones subjetivas, y c) el conocido "*privilegio terapéutico*" de los profesionales sanitarios.

Los deberes de confidencialidad y secreto profesional.

La LOPDGDD establece que el tratamiento de los datos personales, incluidos los datos de carácter sanitario, están sometidos al deber de confidencialidad por parte tanto de los responsables y encargados del tratamiento, como de todas las personas que intervengan en cualquier fase de éste (artículo 5.1). Estamos ante un deber que se complementa, a su vez, con los deberes de secreto profesional a los que alude el apartado segundo del referido precepto legal, y que deberán interpretarse de conformidad con su normativa vigente.

En el ámbito sanitario la relevancia del deber de secreto profesional resulta más que evidente; pensemos por un momento en las obligaciones deontológicas que en este sentido deben asumir todos los profesionales sanitarios, o en las graves responsabilidades penales a las que se enfrenta este colectivo por incurrir en la comisión de un delito de descubrimiento y revelación de secreto tipificado en los artículos 197 y siguientes del Código Penal, en los supuestos de accesos indebidos a la historia clínica, o revelación de secreto a terceros.

Precisamente el Reglamento, en su artículo 9.2. h), cuando alude al tratamiento de datos para fines de medicina preventiva o laboral, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario, o gestión de sistemas y servicios de asistencia sanitaria, establece claramente la obligación de que dicho tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional o bajo su responsabilidad, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros.

Delimitación de bases jurídicas para el tratamiento de datos de salud por las Administraciones Públicas.

Por lo que respecta a la delimitación de las bases jurídicas necesarias para legitimar el tratamiento de los datos sanitarios, cabría destacar la regulación recogida en los artículos 8 y 9 de la LOPDGDD. El primero de ellos por cuánto viene a perfilar con mayor claridad el alcance de las bases jurídicas recogidas en el artículo 6.1 del Reglamento con proyección en el ámbito de las Administraciones Públicas, en concreto: a) el tratamiento de datos para el cumplimiento de una misión realizada en interés público, y b) el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En ambos casos la LOPDGDD deja bien claro que podremos estar ante un tratamiento de datos fundado en cualquiera de los supuestos anteriormente citados, siempre que "*derive de una competencia atribuida por una norma con rango de ley*". Precisamente esta misma exigencia también se predica respecto de los tratamientos de datos en los supuestos previstos en las letras g), h) e i) del artículo 9.2 del Reglamento, que de forma resumida se identificarían con los supuestos de tratamientos de datos por razones de salud. En este sentido el artículo 9.2 -pero ahora de la LOPDGDD -, no deja lugar a dudas cuando establece, respecto del tratamiento de este tipo de datos, que deberán estar amparados en una norma con rango de ley.

En definitiva, la reserva de ley para el tratamiento legítimo de datos personales de carácter sanitario resulta indiscutible, lo que a su vez comporta que la vigencia de buena parte de las abundantes previsiones reglamentarias existentes en esta materia quede en entredicho.

Consentimiento de los menores de edad.

Otro aspecto especialmente delicado en el ámbito sanitario, y sobre el que se pronuncia la LOPDGDD objeto de comentario, es el relativo al tratamiento de datos personales de los menores de edad. La Ley en su artículo 7 fija en 14 años la mayoría de edad en relación con la protección de datos de carácter personal, de modo que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de 14 años. A su vez el artículo 12.6 del referido texto legal, establece que "*en cualquier caso los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de 14 años, los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles*".

La pregunta obligada que habría que plantearse sería si, a la luz de la actual regulación en materia de protección de datos de carácter personal, un paciente menor de edad con 14 o más años cumplidos, podría oponerse a que sus padres puedan acceder al contenido de su historia clínica sin su consentimiento, teniendo en cuenta la existencia en la legislación sanitaria de la figura conocida como "menor maduro". Sobre este respecto, el Informe 339/2015 de la Agencia Española de Protección de Datos, sobre acceso a la historia clínica de los menores entre 16 y 18 años, concluía afirmando que si bien el menor de edad mayor de catorce años podrá, en general, ejercitar por sí solo el derecho de acceso a la historia clínica, en cambio no podría oponerse a que sus padres, titulares de la patria potestad, pueden acceder igualmente a los datos del menor de edad para el cumplimiento de las obligaciones previstas en el Código Civil. Una afirmación discutible.

Ejercicio de derechos.

La LOPDGDD establece que todas las actuaciones que se hayan de llevar a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de derechos serán gratuitas, con las salvedades previstas en los apartados 3 y 4 del artículo 13 de la Ley, a saber: a) peticiones repetitivas reiteradas en el plazo de 6 meses sin causa legítima para ello, y b) elección por el interesado de un medio distinto al ofrecido que suponga un coste desproporcionado.

La traslación al ámbito sanitario de esta previsión legal, supondrá la imposibilidad de exigir al paciente contraprestación económica alguna por la obtención de copia de su historia clínica, más allá de las excepciones a las que me he referido anteriormente.

Por lo que respecta a los restantes derechos, el Reglamento establece en relación con el "*derecho de supresión*", que éste no podrá ser ejercido cuando el tratamiento sea necesario, entre otros casos, por razones de interés público en el ámbito de la salud. Queda clara, por tanto, la inexistencia del derecho de cancelación de los datos sanitarios.

Estrechamente relacionado con el derecho de supresión, el artículo 21 del Reglamento regula el "*derecho de oposición*" al tratamiento de datos personales sobre la base del interés público o el ejercicio de potestades públicas, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses los derechos y las libertades del interesado. Ahora bien, en este otro caso no queda tan claro que los mismos límites que impiden el ejercicio del derecho de cancelación, puedan regir respecto del derecho de oposición al tratamiento de datos sanitarios.

Particularmente confuso resulta el "*derecho a la portabilidad*" (art. 20) de los datos en el ámbito sanitario. Hay que tener en cuenta que conforme al Reglamento comunitario este derecho está ligado a la concurrencia de alguno de los siguientes requisitos: a) que el tratamiento esté basado en el consentimiento o en un contrato, y b) que el tratamiento se efectúe por medios automatizados. Téngase en cuenta que el tratamiento de datos sanitarios en el ámbito de la sanidad pública, no pivota sobre la base jurídica del consentimiento del interesado, sino que se apoyaría sobre el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, bases jurídicas que como ya ha quedado expuesto, hunden sus raíces en la Ley.

Relaciones entre el responsable del tratamiento y el encargado del tratamiento.

A diferencia de la derogada Ley Orgánica del año 1999, la LOPDGDD no aborda en profundidad las relaciones entre el responsable y el encargado del tratamiento, por lo que habrá que acudir nuevamente al Reglamento comunitario para conocer los términos en los que se han de articular las comunicaciones de datos entre ambas figuras. Este constituye, sin duda, un aspecto

especialmente importante debido a que en el ámbito sanitario suele ser relativamente frecuente el recurso a la figura de la "*externalización*" para la prestación de servicios sanitarios, ya sea a través de la formalización de contratos en el marco de la Ley de Contratos del Sector Público, o bien a través de figuras afines como los convenios singulares de vinculación. En todo caso la disposición adicional segunda de la LOPDGDD, establece que "*En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad*".

Responsabilidad proactiva y la creación de la figura del delegado de protección de datos (DPD).

La LOPDGDD incorpora dos nuevas obligaciones que deben asumir tanto los responsables como los encargados del tratamiento también en el ámbito sanitario:

- La adopción de medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento de los datos personales se efectúa conforme al Reglamento comunitario y la Ley Orgánica.

Estamos ante una obligación de gran importancia en el entorno sanitario por cuánto uno de los supuestos que mayores riesgos presenta para el tratamiento de la información, son todas aquellas situaciones de pérdida de confidencialidad de datos sujetos al secreto profesional, supuestos en los que se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad ,y en particular de menores de edad y personas con discapacidad, y cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales. (art. 28.2 de la LOPDGDD).

- La designación de un DPD en los supuestos previstos en el artículo 37.1.

La LOPDGDD establece que los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes, deben designar un delegado de protección de datos. Se trata, por tanto, de una obligación clara y contundente de modo que resultaría jurídicamente cuestionable la implantación de un único delegado de protección de datos para todos los sectores de actividad administrativa de una Comunidad Autónoma, incluido el sector sanitario, como vienen haciendo algunas Administraciones Públicas.

En todo caso parece innegable que: a) la singularidad de los datos de salud, b) la complejidad organizativa del servicio de salud, y c) el volumen de información que tratan las Instituciones Sanitarias, son argumentos más que suficientes para apostar por la existencia de un DPD propio para sanidad.

Tratamientos de los datos de salud.

Finalizar este brevísimo repaso de la Ley con la regulación que del tratamiento de este tipo de datos se hace en la extensa disposición adicional decimoséptima en relación, a su vez, con la disposición final novena del citado texto legal.

El apartado 2 de la referida disposición adicional analiza de forma monográfica el tratamiento de estos datos con fines de investigación en salud, estableciendo como regla general, que el tratamiento de datos con estas finalidades exige que el interesado haya otorgado su consentimiento. En todo caso, para llevar a cabo un tratamiento con fines de investigación en salud pública, el legislador obliga a realizar una evaluación de impacto que determine los riesgos derivados del tratamiento, someter la investigación científica a normas de calidad, y adoptar medidas dirigidas a garantizar que los investigadores no accedan a datos de identificación.

A partir de este escenario, la citada disposición adicional distingue entre:

a) Tratamiento de datos sanitarios por autoridades sanitarias con competencias en vigilancia de la salud pública.

b) Reutilización de datos personales con fines de investigación.

c) Seudonimización de datos personales con fines de investigación en salud.

Respecto a la disposición final novena ésta modifica el apartado 3 del artículo 16 de la Ley 41/2002 de 14 de noviembre. Conforme a esta nueva redacción, el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación, o de docencia, obliga a preservar los datos de identificación personal del paciente separados de los datos de carácter clínico asistencial, de manera que, como regla general, queda asegurado el anonimato salvo que el propio paciente haya dado su consentimiento para no separarlos.

Sin embargo, tras establecer la importancia de la disociación, el párrafo segundo de este mismo apartado añade que se exceptúan los supuestos de investigación previstos en el apartado 2 de la disposición adicional decimoséptima de la Ley Orgánica. Esta excepción resulta difícilmente comprensible por cuánto el apartado 2 de la referida disposición adicional incluye un supuesto específico para la seudonimización de datos personales que vayan a ser tratados con fines de investigación en salud. Así pues la Ley parece incurrir en cierta contradicción.

Conclusión.

Se ha malogrado una buena ocasión para haber regulado de forma independiente la protección de los datos sanitarios tal y como ya propusiera, entre otros muchos, la Sociedad Española de Salud Pública y Administración Sanitaria (SESPAS). La citada sociedad científica en su informe elaborado a tal efecto, afirmaba "*es ineludible la necesidad de disponer de una ley específica sobre protección de datos personales relativos a la salud; ley que, por ende, se enmarcaría en la normativa del sector sanitario. Hoy es opinión generalizada que lo más operativo es elaborar una ley estatal para la protección de los datos personales de salud, que complemente el RGPD y sustituya a las disposiciones contenidas en la todavía vigente Ley Orgánica de Protección de Datos, en la Ley Básica de Autonomía del Paciente, y en el resto de legislación sanitaria estatal*".

Tan solo nos queda confiar en que los gestores y las autoridades de protección de datos sean conscientes de la singularidad que reviste el dato sanitario, y sepan obrar en consecuencia.

3. El Reglamento (UE) 2016/679, de 27 de abril, 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. Principios y derechos. Obligaciones.

El Reglamento Europeo de Protección de Datos unifica y moderniza la normativa europea sobre protección de datos, permitiendo a los ciudadanos un mejor control de sus datos personales y a las empresas aprovechar al máximo las oportunidades de un mercado único digital, reduciendo la burocracia y beneficiándose de una mayor confianza de los consumidores.

La Directiva Europea de Protección de Datos, por su parte, está destinada a los ámbitos policiales y de la Justicia. Pretende asegurar que los datos de las víctimas, testigos y sospechosos de la comisión de delitos, se encuentren debidamente protegidos en el ámbito de una investigación criminal o de aplicación de la ley. A la vez, esta normativa armonizada facilitará la cooperación transfronteriza de la policía y los fiscales para combatir más eficazmente el crimen y el terrorismo en toda Europa.

Por su importancia, reseñamos a continuación lo principal del Reglamento general de protección de datos.

1. CONTENIDO

Según su **art. 1**, este Reglamento establece:

1. Las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y
2. Las normas relativas a la libre circulación de tales datos.

Según su **art. 2** "El presente Reglamento se aplica **al tratamiento total o parcialmente automatizado de datos personales**, así como **al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero**."

Y no se aplicará, en particular:

a. Al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión

b. A la actividad de las autoridades con fines de prevención o investigación de delitos o de protección de la seguridad pública,

c. A las actividades de los Estados miembros comprendidas en el ámbito de aplicación del capítulo

d. Ni al tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Territorial

Es importante resaltar que, conforme a su **artículo 3** "El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, **independientemente** de que el tratamiento tenga lugar en la Unión o no."

Y, muy especialmente, según el número 2 del mismo artículo, el Reglamento se aplica también al tratamiento de datos personales de residentes en la Unión "**por parte de un responsable o encargado no establecido en la Unión,** cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión."

Es decir, se aplica también al también al tratamiento de datos fuera de la Unión, lo que amplía notablemente su ámbito de aplicación.

Ese alcance tan amplio explica que el Reglamento sea un texto muy extenso y detallado.

Principios rectores

En el ámbito actual de la economía digital, los datos personales han adquirido una enorme relevancia económica, en particular en el área del Big Data. Ello tiene además directas consecuencias en el derecho a la privacidad de los ciudadanos.

En consecuencia, la nueva norma se basa en los siguientes principios:

1. Un continente, una norma

   La nueva normativa establece un único conjunto de normas aplicable en el conjunto de la Unión Europea.

2. Ventanilla única

   Los empresarios solo tendrán que relacionarse con un único supervisor en Europa, lo que se estima representará un ahorro de 2.300 millones de euros al año.

3. Europa se rige por la normativa europea

   Las empresas radicadas fuera de la Unión deberán aplicar las mismas reglas cuando ofrezcan sus servicios en la Unión Europea.

4. Consideración de los riesgos específicos

   Las nuevas normas evitarán pesadas obligaciones genéricas sobre el tratamiento de datos, adaptándolas apropiadamente a sus respectivos factores de riesgo.

5. Privacidad desde el diseño

   Las nueva regulación garantizará que la salvaguarda de la protección de datos se incorpora a los productos y servicios desde sus primeros estadios de desarrollo *(Data protection by design).* Se fomentarán las técnicas *"Privacy-friendly",* como la seudoanonimización, para salvaguardar los beneficios de la innovación en Big Data a la vez que se protege la privacidad.

   Este principio de privacidad desde el diseño (**art. 25.1**), significa que en el diseño de aplicaciones que traten datos personales, se tiene que garantizar la privacidad de los mismos desde el principio. Esto implica, por ejemplo, que en materia de redes sociales, los perfiles de privacidad de los usuarios estarán por defecto cerrados a otros usuarios, debiendo ser el usuario quien los abra a otros.

6. La importancia del consentimiento

   El **consentimiento para el tratamiento de los datos** deberá "libre, específico, informada e inequívoco" y el responsable del tratamiento de los datos deberá poder probar que el titular "consintió el tratamiento de sus datos".

Por tanto, en virtud del principio de responsabilidad, el responsable del tratamiento aplicará las medidas adecuadas para **poder demostrar** que ese consentimiento se prestó en la forma adecuada.

Nuevos derechos de los ciudadanos

Según el profesor **Piñar,** con esta nueva norma se acabaron los conocidos en España como derecho ARCO (Acceso, Rectificación, Cancelación y Oposición). El nuevo Reglamento se refiere ahora a los derechos de Transparencia (**art. 12**), Información (**arts. 13** a **14**), Acceso (**art. 15**), Rectificación (**Art. 16**), Supresión o derecho al olvido (**art. 17**), Limitación del tratamiento (**art. 18**), Portabilidad de datos (**art. 20**) y Oposición (**art. 21**).

Estructura

Se trata de una norma muy extensa, que consta de 173 considerandos previos y 99 artículos, agrupados en once capítulos, con la siguiente estructura:

Capítulo I. Disposiciones generales (arts. 1. *Objeto*, a 4. *Definiciones*)

Capítulo II. Principios (arts. 5. *Principios relativos al tratamiento*, a 11. *Tratamiento que no requiere identificación*)

Capítulo III. Derechos del interesado, divido en 5 secciones; **1.ª Transparencia y modalidades** (art. 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado*); **2.ª Información y acceso a los datos personales** (arts. 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado,* a 15. *Derecho de acceso del interesado*); **3.ª Rectificación y supresión** (arts. 16. *Derecho de rectificación,* a 20. *Derecho a la portabilidad de los datos* --incluyendo el importante art. 17. *Derecho de supresión («el derecho al olvido»)*--; **4.ª Derecho de oposición y decisiones individuales automatizadas** (arts. 21. *Derecho de oposición,* y 22. *Decisiones individuales automatizadas, incluida la elaboración de perfiles*) y **5.ª Limitaciones** (art. 23. *Limitaciones*).

Capítulo IV. Responsable del tratamiento y encargado del tratamiento, dividido en 5 secciones: **1.ª Obligaciones generales** (art. 24. *Responsabilidad del responsable del tratamiento;* 25. *Protección de datos desde el diseño y por defecto;* 26. *Corresponsables del tratamiento;* 27. *Representantes de responsables o encargados del tratamiento no establecidos en la Unión;* 28. *Encargado del tratamiento;* 29. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento;* 30. *Registro de las actividades de tratamiento,* y 31. *Cooperación con la autoridad de control;* **2.ª Seguridad de los datos personales** (arts. 32. *Seguridad del tratamiento,* a 34. *Comunicación de una violación de la seguridad de los datos personales al interesado;* **3.ª Evaluación de impacto relativa a la protección de datos y consulta previa** (arts. 35. *Evaluación de impacto relativa a la protección de datos,* a 36. *Consulta previa*); **4.ª Delegado**

de protección de datos (arts. 37. *Designación del delegado de protección de datos*, a 39. *Funciones del delegado de protección de datos*) y **5.ª Códigos de conducta y certificación** (arts. 40. *Códigos de conducta,* a 43. *Organismo de certificación*)

Capítulo V. Transferencias de datos personales a terceros países u organizaciones internacionales (arts. 44. *Principio general de las transferencias,* a 50. *Cooperación internacional en el ámbito de la protección de datos personales*).

Capítulo VI. Autoridades de control independientes, dividido en 2 secciones: **1.ª Independencia** (arts. 51. *Autoridad de control,* a 54. *Normas relativas al establecimiento de la autoridad de control*) y **2.ª Competencia, funciones y poderes** (arts. 55. *Competencia,* a 59. *Informe de actividad*)

Capítulo VII. Cooperación y coherencia, dividido en 3 secciones, **1.ª Cooperación y coherencia** (arts. 60. *Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas,* a 62. *Operaciones conjuntas de las autoridades de control)*; **2.ª Coherencia** (arts. 63. *Mecanismo de coherencia,* a 67. *Intercambio de información)* y **3.ª Comité europeo de protección de datos** (arts. 68. *Comité Europeo de Protección de Datos,* a 76. *Confidencialidad*)

Capítulo VIII. Recursos, responsabilidad y sanciones (arts. 77. *Derecho a presentar una reclamación ante una autoridad de control*, a 84. *Sanciones*)

Capítulo IX. Disposiciones relativas a situaciones específicas de tratamiento (arts. 85. *Tratamiento y libertad de expresión y de información,* a 91. *Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas*)

Capítulo X. Actos delegados y actos de ejecución (arts. 92. *Ejercicio de la delegación,* y 93. *Procedimiento de comité*)

Capítulo XI. Disposiciones finales (arts. 94. *Derogación de la Directiva 95/46/CE,* a 99. *Entrada en vigor y aplicación*)

Principales novedades que incorpora el Reglamento

Según la **Jornada Enatic sobre el nuevo Reglamento Europeo de protección de datos**:

1, Principios aplicables al tratamiento de datos (**art. 5**): Licitud, lealtad y transparencia; recogidos con fines determinados, explícitos y legítimos («limitación de la finalidad»); limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); exactos y, si fuera necesario, actualizados («exactitud»); mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales («limitación del plazo de conservación»); tratados de tal manera que se garantice una seguridad adecuada de los datos personales («integridad y

confidencialidad»); el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

2. Condiciones para entender válidamente prestado el consentimiento (**art. 7**)

3. Necesidad de que el responsable del tratamiento pueda probar que se prestó el consentimiento

4. Regulación específica del conocido como Derecho al olvido o, más propiamente, derecho de supresión (**art. 17**)

5. Principio de portabilidad de los datos (**art. 20**)

6. Responsabilidad del responsable del tratamiento de los datos por la adopción y actualización de las medidas adecuadas (**art. 24**)

7. Registro de las actividades de tratamiento (**art. 30**)

8. Notificación a los interesados de las violaciones de seguridad (**art. 33**)

9. Evaluación de impacto relativa a la protección de datos (**art. 35**)

10. Consulta previa a la autoridad de control en caso de identificarse riesgos en el tratamiento (**art. 36**)

11. Introducción de la figura del Delegado de protección de datos (**arts. 37** a **39**)

12. Regulación de las transferencias internacionales de datos (**arts. 45** y **47**)

13. Criterio "One stop shop" para la reclamación de la violación de las obligaciones de protección de datos por parte de una multinacional (**arts. 60** a **67**)

Convivencia con la LOPD

La entrada en vigor de este nuevo Reglamento plantea la duda de cómo va a convivir en España con la LOPD.

A este respecto, el tanto **Piñar Mañas** como **Pablo García-Mexia**, apuntaron recientemente a que parece que la ley española podrá seguir siendo aplicable en lo que esté fuera del Derecho de la UE, pues, además, el Reglamento hace numerosas remisiones a la legislación nacional de los Estados miembros.

Pero se suscitan dudas en materias como el registro de ficheros ¿Habrá que seguir realizándolo en nuestro país por efecto de la LOPD o cabe entender una derogación tácita de sus disposiciones en este sentido?

Igualmente también cabe preguntarse en qué papel quedará al AEPD y qué valor tendrán sus circulares en el nuevo contexto.