AUXILIAR ADMINISTRATIVO AYTO. QUISMONDO 2019

TELEOPOSICIONES
Avda. Maisonnave 28, bis 4ª Planta. Alicante
temarios@teleoposiciones.es

TEMA: Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su Reglamento de desarrollo.

La ley orgánica objeto de este epígrafe tiene una parada obligatoria sobre el nuevo Reglamento General de Protección de datos, proveniente de la legislación comunitaria.

El RGPD nació con un triple objeto:

- ✓ establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.
- ✓ proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
- ✓ pretende que la libre circulación de los datos personales en la Unión no pueda ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

En relación con su ámbito de aplicación, se establecen dos distinciones:

- Ámbito de aplicación material (artículo 2) . El Reglamento se aplicará 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. Por el contrario, no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b)por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d)por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

- Ámbito territorial (artículo 3). Como matiza el art. 3 del 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.

Adquiriendo especial relevancia el punto 3 del citado artículo al matizar la aplicación: "al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público."

Es decir, el Reglamento UE 2016/679, de 27 de abril de 2016 será aplicable al tratamiento de datos fuera de la Unión.

* Principales novedades del RGPD.

La extensa regulación del Reglamento presentará novedades en aspectos como:

Los principios aplicables al tratamiento de datos y condiciones para el consentimiento.

La regulación del denominado «derecho al olvido» o derecho de supresión de los datos personales.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida

los datos personales cuando concurra alguna de las circunstancias citada en el artículo 17.

Derecho a la portabilidad de los datos.

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se den las circunstancias citadas en el artículo 20.

Responsabilidad del responsable del tratamiento. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Registro de las actividades de tratamiento. Cada responsable o encargado del tratamiento de datos (o su representante) realizarán un registro que deberá contener toda la información indicada en el artículo 30.

Notificación de una violación de la seguridad de los datos personales a la autoridad de control. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

Evaluación de impacto relativa a la protección de datos. El responsable del tratamiento de los datos realizará (en particular si utiliza nuevas tecnologías), antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de

operaciones de tratamiento similares que entrañen altos riesgos similares.

Consulta previa a la autoridad de control en caso de identificarse riesgos en el tratamiento. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

Regulación de las transferencias internacionales de datos. Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado (artículos 45 a 47)

Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas (artículos 60 a 67)

LEY ORGANICA DE PROTECCION DE DATOS Y GARANTÍA DE LOS DERECHOS DIGITALES.

Esta nueva Ley Orgánica consta de 97 artículos estructurados en diez títulos, 22 disposiciones adicionales, 6 disposiciones transitorias, 1 disposición derogatoria y 16 disposiciones finales.

La LOPDGDD deroga en su totalidad a la tan conocida LOPD 15/1999, no obstante, 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 se mantiene en tanto no se oponga o resulte incompatible con el RGPD y la presente LOPDGDD. Esta nueva LO aporta algo de luz al marco normativo de la protección de datos

personales si bien, siguen quedando lagunas que previsiblemente se disiparán con el desarrollo reglamentario de la ley en el futuro.

Básicamente, además de transponer la directiva europea, añade una serie de novedades destacables tales como:

Protección de datos de las personas fallecidas (artículo 3) -> contempla que las personas vinculadas al fallecido por razones familiares o de hecho, herederos, así como las personas o instituciones que el fallecido hubiese designado al efecto, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

No podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. También se contemplan las especialidades en el caso de fallecimiento de menores y de personas con discapacidad. A su lado y como uno de los derechos digitales en el art. 96, el "Derecho al testamento digital".

Tratamiento de datos por obligacion legal, interés público o ejercicio de poderes públicos (artículo 8) -> aclara que podrá considerarse fundado el cumplimiento de una obligación legal exigible al responsable cuando lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras.

Reconocimiento del Delegado de Protección de Datos como órgano intermedio de control (artículo 37) -> se permite que el afectado, cuando se hubiese nombrar un DPD, con carácter previo a la presentación de una reclamación, se dirija con el Delegado de la entidad contra la que reclame, que deberá comunicar su decisión en el plazo máximo de 2 meses desde la recepción de la reclamación.

Obligación de nombramiento del DPD -> se incorpora un extenso listado de entidades obligadas a nombrar un Delegado de Protección de Datos y se estipula el plazo máximo de 10 días para su comunicación a la AEPD desde su nombramiento.

Derecho de acceso (artículo 13) -> plantea la posibilidad de que se cree una aplicación o módulo en el que el interesado pueda acceder a sus datos de forma remota, directa segura y fácil.

Información por capas (artículo 11) -> se regula la posibilidad de su uso para facilitar la información a los interesados en cualquier situación en la que sea conveniente, y no solo, como ya se venía realizando, en las cookies o en la información de videovigilancia. Además se reduce el contenido mínimo de la primera capa.

Consentimiento de menores -> se establece en 14 años la edad necesaria para prestar el consentimiento para el tratamiento de los datos. No obstante, podrán tratarse los datos de menores de 14 años en tanto se cuente con el consentimiento por parte del titular de la patria potestad.

Además se refuerza la protección del menor garantizando la seguridad de los menores frente a internet y promoviendo la lucha contra la discriminación y la violencia ejercida sobre estos mediante el uso o abuso de las nuevas tecnologías.

Denuncias anónimas -> las empresas podrán establecer canales internos y anónimos para que los empleados y terceros puedan efectuar denuncias con respecto a esta materia, aplicando además importantes medidas de confidencialidad.

Bloqueo de datos (artículo 32) -> se introduce como una nueva obligación cuando un interesado ejercite el derecho de rectificación o supresión. Se deberán bloquear los datos, identificándolos e impidiendo su tratamiento, inclusive su visualización, mientras no se haya resuelto la solicitud del referido ejercicio de derechos. Los datos tratados no podrán ser tratados para ninguna finalidad distinta.

Cuando la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos

Evaluación de impacto (artículo 28)-> facilita una serie de supuestos concretos en los que sería necesario realizar una EIPD al ser tratamientos que implican un alto riesgo para los derechos y libertades de los ciudadanos.

Videovigilancia y grabación de audio en el ámbito laboral -> se precisan los límites y cómo y cuando se debe informar a los empleados de esta circunstancia.

Se podrá realizar siempre que la finalidad sea preservar la seguridad de las personas y bienes e instalaciones o control laboral. Las imágenes deberán suprimirse a los 30 días, salvo si se cometen actos contra la seguridad. En este caso, las grabaciones deberán ser puestas a disposición de las fuerzas de seguridad antes de las 72 horas desde el suceso. En caso de la videovigilancia de empleados, éstos siempre deberán tener información previa, expresa, clara y concisa.

Sobre la licitud -> se recogen una serie de supuestos concretos en los que se consideraría lícito el tratamiento sin necesidad de haber obtenido el consentimiento del interesado por ejemplo porque exista un interés público para su tratamiento.

Desarrolla el régimen sancionador y el catálogo de sanciones, diferenciando entre leves, graves y muy graves, así como los plazos de prescripción y los supuestos de suspensión.

Se amplían las exigencias y condiciones exigidas para el tratamiento de determinadas categorías de datos especiales -> se limita la validez del consentimiento

Competencia desleal en materia de protección de datos -> la Disposición Adicional decimosexta define el concepto de prácticas agresivas por parte de consultoras.

Introduce un nuevo título referente a los Derechos Digitales -> La nueva LOPDGDD desarrolla el artículo 18.4 de la Constitución Española, en cuanto a garantizar el uso de la informática para garantizar el derecho al honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, entre los que destacan el testamento digital y el derecho a la desconexión digital del empleado, desarrollando también la protección de su intimidad en el ámbito laboral.

A grosso modo las arriba mencionadas serías las novedades más significativas de la nueva normativa española, si bien, no podemos dejar de tener presente que en sus Disposiciones Finales se introducen modificaciones relevantes en otras normas (tales como LOPJ, LEC, ET, LOREG, LPAC, TTBG, LGS, etc).

Transparencia y buen gobierno.

El concepto de este epígrafe se solventa con el estudio del espíritu de La ley de transparencia de España es una norma que tiene como objetivo reforzar el derecho de los ciudadanos a acceder a la información sobre actividades públicas.

Su nombre completo es Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Se publicó en el Boletín Oficial del Estado el 10 de diciembre de 2013.

La ley entra en vigor en dos momentos: el título de Transparencia y el del Consejo de Transparencia y Buen Gobierno al año de su publicación en el Boletín Oficial del Estado y el título de Buen Gobierno al día siguiente.

La ley afecta, entre otras, a entidades como la Administración General del Estado, la de las comunidades autónomas, Ceuta y Melilla y administraciones locales. También a la Casa Real, el Congreso, el Senado, el Tribunal Constitucional, el Banco de España, el Defensor del Pueblo, agencias estatales, entidades públicas empresariales, entidades gestoras de la Seguridad Social, fundaciones del sector público, etc.4 Se incluye a sociedades mercantiles en las que participen entidades públicas con un capital superior al 50%. Sin embargo, no todas tienen las mismas obligaciones.

Sólo ciertas disposiciones de la ley se aplican a partidos políticos, sindicatos, organizaciones empresariales y entidades privadas con subvenciones públicas de más de 100.000 € o cuando al menos un 40% de sus ingresos anuales provienen de fondos públicos, siempre que alcancen 5.000 € de cantidad mínima.