EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Julián Prieto Hergueta
Agencia Española de Protección de Datos
XI Congreso de Actualidad Laboral
Colegio Oficial de graduados Sociales de Madrid
13/12/2017

NUEVO MARCO JURÍDICO

El Reglamento 2016/679 sustituirá a la Directiva 95/46

- Publicado 4 de mayo 2016
- Entrada en vigor a los 20 días de publicación
- 2 años hasta inicio de aplicación: 25 de mayo de 2018

Proyecto de Ley Orgánica de Protección de Datos (PLOPD)

- Previsión entrada en vigor 25 mayo de 2018

PRINCIPIOS

Principios se mantienen similares a los de la Directiva, con refuerzo en algunos matices

- Licitud, lealtad y transparencia
- Limitación de finalidad
- Minimización de datos
- Exactitud (PLOPD no imputación al responsable)
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva

LEGITIMACIÓN

Art. 6.1

a) consentimiento para el tratamiento de sus datos personales para uno o más fines específicos

b) ejecución de un contrato en el que el interesado es parte o para la aplicación, a petición de éste, de medidas precontractuales

c) cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento

d) intereses vitales del interesado o de otra persona física

LEGITIMACIÓN

e) cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los interés o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales, en particular, cuando el interesado sea un niño. Ello no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones

LEGITIMACIÓN

PLOPD: Interés legítimo ponderado por el propio legislador

- Datos de contacto de personas jurídicas y de empresarios individuales
  - ✓ Necesarios para su localización profesional
  - ✓ Finalidad relacionarse con la persona jurídica, no como persona física
  - ✓ Referidos a su condición de empresarios
- Sistemas de información crediticia
- Videovigilancia
- Sistemas de exclusión publicitaria ("listas Robinson")
- Denuncias internas en el sector privado...

Categorías especiales de datos

Se incluyen datos genéticos y biométricos. Se excluyen datos de infracciones y sanciones administrativas.

Regla general: queda prohibido su tratamiento (igual que en la Directiva). Excepciones a la prohibición (algunas)

- Consentimiento
- Obligaciones y ejercicio derechos de los responsables en el ámbito del derecho laboral y de seguridad o protección social
  - Puede basarse en Convenio Colectivo
- Protección de intereses vitales del afectado o un tercero
- Datos manifiestamente públicos
- Fundación o asociación sin ánimos de lucro: política, filosófica, religiosa o sindical respecto de sus miembros
- Por razones de Interés público esencial según Ley UE o Nacional siempre que sea proporcional a la finalidad perseguida
- Razones de interés público en el ámbito de la salud pública

CONSENTIMIENTO

- Libre, específico, informado e "inequívoco" → A través de declaraciones o "claras acciones afirmativas"
- Consentimiento de menores con autorización → 16 años, pudiendo EEMM reducir hasta 13 (PLOPD 13 años)
- Revocable

CONSENTIMIENTO

- El RGPD no implica necesariamente una obligación de recabar un nuevo consentimiento si el que se hubiera obtenido antes de su aplicación fuese conforme a los requisitos que establece
  - Siguen siendo válidos los consentimientos expresos y los consistentes en una manifestación o clara acción afirmativa
  - En ningún caso hay aplicación retroactiva, dado que las normas del RGPD no se aplican a tratamientos anteriores al momento en que produce plenos efectos
- Cuando se preste el consentimiento para el tratamiento de datos con múltiples finalidades será preciso dar el consentimiento para todos ellos (Cdo. 32). En particular:
  - Consentimientos específicos en el marco de un contrato
  - Consentimientos específicos en el marco de declaraciones

DERECHOS

- **Catálogo tradicional con** novedades
  - **Información**
  - **Acceso (copia de los documentos)**
  - **Rectificación**
  - **Derecho al borrado y al olvido**
  - **Limitación del tratamiento**
  - **Portabilidad**
  - **Oposición**
- **Previsiones sobre ejercicio de estos derechos**
  - **Lenguaje claro e inteligible**
  - **Obligación de "facilitar el ejercicio"**
  - **Plazos de respuesta → 1 mes**
  - **Formas de ejercicio → Posible vía electrónica**
  - **Gratuidad**

INFORMACIÓN

Configuración de la información como derecho del interesado y no como obligación del responsable

Se incrementa la información que habrá de facilitarse cuando los datos se recaban del afectado

- **Datos de contacto del delegado de protección de datos**
- **Fines y base jurídica del tratamiento**
- **Intereses legítimos del responsable o de un tercero**
- **Destinatarios o las categorías de destinatarios de los datos personales**
- **Transferencias previstas**
- **Plazo de conservación**
- **Existencia de decisiones automatizadas, incluida la elaboración de perfiles la lógica aplicada y las consecuencias previstas**

INFORMACIÓN

Si los datos no se recaban del interesado deberá además informársele de:

- Categorías de datos que se van a tratar
- Fuente de la que proceden los datos personales y, en su caso, si proceden de "fuentes de acceso público"

Excepciones al deber de información

- Si los datos no proceden del interesado
  - Aclaración del esfuerzo desproporcionado en caso de tratamiento con fines de archivo, estadísticos o de investigación científica o histórica
  - Previsión legal expresa de tratamiento o revelación, con medidas oportunas de protección
  - Obligación de secreto legal o profesional

Exigencia de claridad, concisión y fácil acceso

INFORMACIÓN

Información por capas (PLOPD art. 11)

- Información en la primera capa
  - En todo caso
    - Identidad del responsable del tratamiento o su representante
    - Finalidad del tratamiento
    - Modo de ejercicio de los derechos
    - En su caso:
      - Uso de los datos para la elaboración de perfiles
      - Derecho de oposición a decisiones automáticas
  - Si los datos no se han obtenido del afectado, además deberá informarse de:
    - Categorías de datos objeto de tratamiento
    - Fuentes u orígenes de los datos

CUESTIONES GENERALES

Condiciones generales

- Obligación de atender los derechos a menos que se acredite la imposibilidad de identificar al interesado
- Respuesta por medios electrónicos si el derecho se ejercitó por dichos medios salvo que el interesado manifieste lo contrario
- Gratuidad salvo en caso de solicitudes "manifiestamente infundadas o excesivas
  - Cobrar un canon
  - Negarse a actuar respecto de la solicitud.
- Posibilidad de solicitar información adicional para garantizar la identificación del solicitante

LIMITACIÓN DEL TRATAMIENTO

- Casos en que existe derecho a solicitar la limitación
  - Mientras se verifica de la exactitud de los datos en casos de impugnación por el interesado
  - Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales
  - Cuando el interesado necesite que el responsable conserve los datos para la formulación, el ejercicio o la defensa de reclamaciones
  - Mientras se verifican circunstancias en derecho de oposición

DERECHO A LA PORTABILIDAD

Derecho del interesado a

- Recibir los datos personales que le incumban,
- Que haya facilitado a un responsable del tratamiento,
- En un formato estructurado y de uso habitual y de lectura mecánica
- Y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos

Requisitos para que pueda ejercitarse (acumulativos):

- El tratamiento esté basado en el consentimiento o en un contrato
- El tratamiento se efectúe por medios automatizados

OTROS DERECHOS

Decisiones automatizadas

- Referencia expresa a la elaboración de perfiles
- Derecho a no ser objeto de una decisión que "produzca efectos" sobre el afectado o "le afecte significativamente de modo similar
- Excepciones
  - Vinculación a contrato
  - Autorización por el derecho Nacional o de la UE
  - Consentimiento explícito
- Salvo en caso de habilitación legal, el interesado tiene derecho a obtener intervención humana en la decisión y que el interesado pueda dar su opinión e impugnar la decisión
- Salvo que exista consentimiento o interés público, no podrá implicar datos sensibles

Obligación de comunicación de la rectificación, supresión o limitación del tratamiento a los cesionarios

RESPONSABILIDAD ACTIVA

- El Reglamento prevé que los responsables aplicarán las medidas técnicas y organizativas apropiadas para **garantizar** y **estar en condiciones de demostrar** que el tratamiento de datos personales se lleva a cabo de conformidad con el presente Reglamento. Tales medidas se revisarán y actualizarán cuando sea necesario

RESPONSABILIDAD ACTIVA

Tipos de medidas

- Mantener "registro de actividades de tratamiento"
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Aplicar medidas de seguridad adecuadas
- Llevar a cabo Evaluaciones de Impacto
- Autorización previa o consultas previas con APD
- Designación Delegado Protección de Datos (DPD)
- Notificación de Quiebras de Seguridad
- Códigos de conducta y esquemas de certificación

REGISTRO DE TRATAMIENTOS

- Obligación para responsable y encargado
- PLOPD Art.31 "El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento."
- La desagregación de las actividades de tratamiento
- La incidencia en las medidas de cumplimiento normativo
- Contenido (responsable)
  - Identificación y datos contacto de responsable, corresponsable, representante y DPO
  - Fines

REGISTRO DE TRATAMIENTOS

- Descripción de **categorías de interesados y datos** personales
- **Categorías de destinatarios** existentes o previstos (inclusive en terceros países u organizaciones internacionales)
- **TID a terceros países u organizaciones internacionales** y documentación de garantías para TID exceptuadas sobre base de intereses legítimos imperiosos
- Cuando sea posible, plazos previstos para supresión de datos
- Cuando sea posible, descripción general de medidas de seguridad

REGISTRO DE TRATAMIENTOS

- **REGISTRO ENCARGADOS:**
  - Categorías de tratamiento efectuadas por cuenta del responsable
  - Nombre y datos contacto encargado y responsables
  - Transferencias internacionales, en su caso
  - Cuando sea posible, descripción general de medidas de seguridad

ENFOQUE DE RIESGO

- Medidas aplicables en función del riesgo para los derechos y libertades de los interesados
  - Alto riesgo vs. riesgo estándar
  - El riesgo como criterio de ponderación
- Problema de determinación del nivel de riesgo

Protección de Datos desde el diseño

- **Medidas técnicas y organizativas adecuadas** (p.ej. seudonimización, minimización) para aplicar principios de PD de forma eficaz y proteger los derechos
- **En el momento de determinar los medios para el tratamiento y en el momento del tratamiento** (integrar necesarias garantías)
- Teniendo en cuenta
  - Naturaleza, ámbito, contexto y fines del tratamiento
  - Riesgos de diversa probabilidad y gravedad (no sólo alto riesgo)
  - Estado de la técnica y coste

PRIVACIDAD por DEFECTO

Protección de Datos por defecto

- Medidas técnicas y organizativas apropiadas
- Tratamiento **por defecto sólo de datos personales necesarios para cada fin específico**
  - Cantidad de datos recopilados
  - Extensión del tratamiento
  - Periodo de almacenamiento
  - Accesibilidad
  - En particular, evitar la accesibilidad a un número indeterminado sin intervención de alguien

MEDIDAS DE SEGURIDAD

- Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al **riesgo**, teniendo en cuenta
  - Estado de la **técnica y costes** de aplicación
  - **Naturaleza, alcance, contexto y fines** del tratamiento
  - **Riesgos** para los derechos y libertades de las personas
- La adhesión a un **código de conducta o a un mecanismo de certificación** podrá servir de elemento para demostrar el cumplimiento de los requisitos de seguridad

EVALUACIÓN DE IMPACTO

- Deberá realizarse cuando sea probable que el tratamiento previstos presente un alto riesgo específicos para los derechos y libertades de los interesados, entre otros casos, cuando:
    - elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
    - tratamiento a gran escala de las categorías especiales de datos
    - observación sistemática a gran escala de una zona de acceso público
- Las APD deberán establecer listas adicionales de tratamientos de alto riesgo y podrán establecer listas que no requieren EIPD
- El RGPD prevé un contenido mínimo de la evaluación
- Como novedad, se prevé que habrá de recabarse "cuando proceda" la opinión de los interesados

CONSULTA APD

- Consulta a APD cuando una EIPD muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo *"y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación"*
- APD podrá →
  - Asesorar por escrito al responsable, y en su caso al encargado
  - Utilizar cualquiera de sus poderes, incluido prohibir el tratamiento
- Obligación de consulta en elaboración de toda propuesta de medida legislativa o de una medida reglamentaria que la aplique
- El derecho nacional podrá establecer consulta y petición de autorización en tratamientos derivados del ejercicio de una misión realizada en interés público

BRECHAS DE SEGURIDAD

Notificación a APD

- Sin demora y a más tardar en 72 horas desde que se haya tenido constancia. Más tarde, justificación motivada
- No obligación cuando "sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas"
- Reglamento prevé contenido mínimo de notificación
- Documentación de todas las violaciones de seguridad
- Obligación del encargado de notificar sin dilación indebida violaciones de seguridad al responsable

Notificación a interesados

- Cuando es probable que la quiebra entrañe alto riesgo para los derechos y libertades de interesados
- Sin dilación indebida
- Contenido mínimo, que no incluye posibles medidas paliativas
- Excepciones
  - Implementación de medidas de protección tecnológica que haga ininteligibles los datos a terceros no autorizados (p.ej.: datos encriptados)
  - medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado
  - Esfuerzos desproporcionados, alternativa comunicación pública
- APD puede obligar a notificar a interesados

Responsable y encargado del tratamiento

- **Obligación general de diligencia en selección de encargado**
- **Regulación más detallada que en Directiva → Contrato que fije**
  - **Objeto, duración, naturaleza y finalidad del tratamiento, tipo de datos personales, categorías de interesados afectados, obligaciones y derechos del responsable del tratamiento**
  - **Obligación de tratar los datos únicamente siguiendo instrucciones documentadas del responsable**

Responsable y encargado del tratamiento

- Confidencialidad de personas que manejen datos
- Medidas de seguridad
- Contratación de subencargados con autorización previa, general o específica, del responsable, y posibilidad de rechazar subencargados
- Asistencia al responsable en ejercicio de derechos y en cumplimiento de obligaciones de arts. 32 a 36 (seguridad, notificación de violaciones de seguridad, evaluaciones de impacto, consulta previa a la AEPD)

- **PLOPD, DISPOSICIÓN TRANSITORIA QUINTA: LOS CONTRATOS SUSCRITOS ANTES 25.05.2018 MANTENDRÁN VALIDEZ HASTA SU VENCIMIENTO O PRÓRROGA Y EN TODO CASO POR 4 AÑOS**

Responsable y encargado del tratamiento

- Algunas peculiaridades

- Previsión de que el responsable "realice **auditorías** y contribuya a ellas, incluidas las inspecciones dirigidas por el responsable o por otro auditor autorizado por dicho responsable"
- Fin de la prestación implica **borrado o devolución** de datos, sin incluir transferencia a otro encargado
- Obligación de **informar** al responsable "si, en su opinión, una **instrucción infringe el presente Reglamento** o las disposiciones nacionales o de la Unión en materia de protección de datos"
- Posibilidad de **"contratos modelo"**

¿Qué entidades están obligadas a designar un DPD?

El RGPD requiere la designación de un DPD en tres casos específicos:

- Cuando el tratamiento se realice por una autoridad u organismo público (independientemente de los datos que se estén procesando);
- Cuando las actividades principales del responsable del tratamiento o del procesador consisten en operaciones de tratamiento que exigen un control periódico y sistemático de los datos a gran escala;
- Cuando las actividades principales del responsable del tratamiento o del procesador consisten en procesar a gran escala categorías especiales de datos o datos personales relativos a condenas y delitos penales.

PLOPD establece en el art. 34 las entidades que tienen que designar un DPD

DPD

¿Es posible nombrar un DPD externo?

- El **DPD** puede ser un miembro del personal del responsable del tratamiento o del encargado del tratamiento (DPD interno) o «cumplir las tareas sobre la base de un contrato de servicios». Puede ejercerse sobre la base de un contrato de servicios celebrado con un individuo u organización
  - Equipo de personas bajo la responsabilidad del contrato designado
  - Cada miembro del equipo debe cumplir los requisitos del RGPD
- En las Administraciones Públicas puede nombrarse un solo **DPD** para varias entidades

DPD

Funciones

- **Informar y asesorar** a responsable y encargado, documentando esa actividad
- **Supervisar** la puesta en práctica de las **políticas de protección de datos**, incluidas la formación y la auditoría
- **Supervisar** la aplicación del Reglamento en lo relativo a **PbD**, **PbDef y derechos de los interesados**
- Asegurar la existencia y mantenimiento de documentación obligatoria
- **Supervisar gestión de quiebras de seguridad**

DPD

- **Supervisar** la realización de **Evaluaciones de Impacto y la solicitud de autorizaciones o consultas** que se requieran
- Supervisar respuestas a requerimientos de APD
- Cooperar con la APD en el marco de sus tareas
- Actuar como **punto de contacto para la APD y los interesados**
- Comunicación **de su identidad al público**
- Derecho **de acceso por los interesados**
- Información **directa a la dirección**

DPD

¿Cuáles son las cualidades profesionales que debería tener el DPD?

El RGPD exige que el DPD «se designe sobre las base de cualidades profesionales y, en particular, conocimientos especializados sobre la legislación y las prácticas en materia de protección de datos y sobre la capacidad para cumplir las tareas a que se refiere el artículo 39»

- No se prevé cómo acreditar cualidades profesionales
- El mecanismo de certificación de ENAC

DPD

¿Cuáles son los recursos que se deben proporcionar al DPD para llevar a cabo sus tareas?

Dependiendo de la naturaleza de las operaciones de procesamiento y las actividades y tamaño de la organización, deben ser proporcionados al DPD los siguientes recursos:

- **Apoyo activo de la función del DPD por parte de la alta dirección**

DPD

- Tiempo suficiente para que los **DPD** cumplan sus obligaciones
- Apoyo adecuado en términos de recursos financieros, infraestructura (locales ,instalaciones, equipo) y personal, cuando corresponda
- Comunicación oficial de la designación del **DPD** a todo el personal
- Acceso a otros servicios dentro de la organización para que los **DPD** puedan recibir apoyo esencial, aportaciones o información de esos otros servicios
- formación continua

DPD

¿Cuáles son las salvaguardias que permiten al DPD realizar sus tareas de manera independiente?

- Ninguna instrucción de los controladores o procesadores sobre el ejercicio de las tareas del **DPD**
- Ningún despido o sanción por parte del controlador para el desempeño de las tareas del **DPD**
- No hay conflicto de intereses con otras posibles tareas y deberes

DPD

¿Cuáles son las «otras tareas y obligaciones» de un DPD que pueden dar lugar a un conflicto de intereses?

- El DPD no puede ocupar un puesto dentro de la organización que lo conduzca a determinar los propósitos y los medios del tratamiento de los datos personales. Debido a la estructura organizativa específica en cada organización, esto debe ser considerado caso por caso.
- Como regla general, las posiciones conflictivas pueden incluir posiciones de alta dirección, jefe de Recursos Humanos o jefe de departamentos de TI, pero también otros roles más bajos en la estructura organizativa si tales posiciones o roles conducen a la determinación de propósitos y medios de procesamiento

DPD

¿El DPD es personalmente responsable del incumplimiento del RGPD?

No, los DPD no son personalmente responsables por el incumplimiento del RGPD. El RGPD deja claro que es el responsable del tratamiento o del procesador quien debe garantizar y demostrar que el tratamiento se realiza de conformidad con el presente Reglamento. El cumplimiento de la protección de datos es responsabilidad del controlador o del procesador.

CÓDIGOS DE CONDUCTA Y CERTIFICACIONES

- ***Códigos*** → **"facilitar la aplicación efectiva, del RGPD teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las PYMES"**
- ***Certificaciones*** → ***"permitir a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes"***
- ***Demostrar el cumplimiento de lo dispuesto en el RGPD***

SUPERVISIÓN

- **Acciones correctivas →**
  - **Sancionar con una advertencia cuando las operaciones de tratamiento previstas puedan infringir RGPD**
  - **Sancionar con apercibimiento cuando las operaciones de tratamiento hayan infringido RGPD**
  - **Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos**
  - **Ordenar que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, de una determinada manera y dentro de un plazo especificado**
  - **Ordenar al responsable que comunique al interesado las violaciones de la seguridad de los datos personales**
  - **Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición**

SUPERVISIÓN

- Multas deberán ser efectivas, proporcionadas y disuasorias
- Cantidad deberá modularse atendiendo a circunstancias del caso
- Aplicables a responsables y encargados
- Clasificación de infracciones y sanciones
    - Multa hasta 10 M € o para empresas, optándose por la de mayor cuantía, hasta el 2 % de volumen de negocio anual a nivel mundial
        - Obligaciones de responsable o encargado
        - Obligación de organismos de certificación
        - Obligaciones de los organismos de supervisión de códigos de conducta

SUPERVISIÓN

- Multa hasta 20 M € o hasta el 4%
  - Principios básicos
  - Derechos
  - Transferencias internacionales..
- Multa hasta 20 M € o hasta el 4%
  - Incumplimiento de resoluciones de APD

PLOPD , Título IX, Régimen sancionador:

- Tipificación infracciones
- Graduación
- Prescripción

¡MUCHAS GRACIAS!