



# EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

*REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016 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 (RGPD)*

# 2016 - 2018 PERÍODO DE TRANSICIÓN

Entrada en vigor el 25 de mayo de 2016

Aplicación obligatoria a partir de mayo de 2018

Necesidad de adaptar las operaciones iniciadas antes de mayo de 2018

# PRINCIPALES NOVEDADES CON RESPECTO A LA LOPD



- Licitud del tratamiento: bases de legitimación
- Transparencia de las operaciones del tratamiento: cumplimiento del deber de informar
- Nuevos derechos de los interesados
- Seguridad de los datos: responsabilidad proactiva (accountability), privacidad desde el diseño y por defecto (Privacy by design and by default)
- Obligaciones materiales: RAT, Política de protección de datos, DPO, evaluación de impacto.
- Relaciones contractuales: encargo del tratamiento
- Transferencias internacionales
- Régimen sancionador

# CONCEPTO DE DATO PERSONAL

## ART. 4.1

Toda información sobre una persona física:

- Identificada: directamente
- Identifiable: directa o indirectamente

*“toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea (...)"*



# RESPONSABLE VS ENCARGADO DEL TRATAMIENTO

*RESPONSABLE DEL TRATAMIENTO:* la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento

*ENCARGADO DEL TRATAMIENTO:* la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento, bajo sus directrices en cuanto a los fines y los medios del tratamiento de los datos.

*EJEMPLO:* la empresa X es Responsable del tratamiento de los datos de sus empleados, en tanto recaba los datos en su propio nombre y decide sobre la modalidad del tratamiento de los mismos; la gestoría Y que X tiene contratada para la gestión de nóminas de sus empleados, es encargada del tratamiento en tanto tiene acceso a esos datos para prestar el servicio contratado.

# LICITUD DEL TRATAMIENTO

## ART. 6-10

El tratamiento de datos de carácter personal deberá estar legitimado por alguna de las siguientes bases

### TRATAMIENTO NECESARIO PARA

- Para la ejecución de un contrato o medidas precontractuales
- Para la satisfacción del interés legítimo
- Cumplimiento de una obligación legal
- Para proteger intereses vitales (interesado o tercero)
- Para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos

### CONSENTIMIENTO del interesado

- EXPRESO E INEQUÍVOCO mediante una manifestación del interesado o una clara acción afirmativa (excluye tácito o por omisión)
- EXPLÍCITO: datos sensibles, adopción de decisiones automatizadas y transferencias internacionales
- LIBRE E INFORMADO
- DEMOSTRABLE: el responsable debe poder demostrar que lo obtuvo
- REVOCABLE: deberá ser tan fácil retirar el consentimiento como darlo

# TRANSPARENCIA: CUMPLIMIENTO DEL DEBER DE INFORMAR

## ART. 13-1

El Responsable del tratamiento de los datos, ha de proporcionar al interesado antes de proceder al tratamiento de sus datos

## INFORMACIÓN

Concisa

Transparente

Inteligible

De fácil acceso

Con un lenguaje claro y sencillo,

Por escrito, verbalmente o por otros medios

## Información que se debe proporcionar al interesado:

- La existencia del fichero o tratamiento, su finalidad y destinatarios.
- El carácter obligatorio o no de la respuesta, así como de sus consecuencias.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y datos de contacto del responsable del tratamiento.
- Los datos de contacto del Delegado de Protección de Datos, en su caso,
- La base jurídica o legitimación para el tratamiento,
- El plazo o los criterios de conservación de la información,
- La existencia de decisiones automatizadas o elaboración de perfiles,
- La previsión de transferencias a Terceros Países
- El derecho a presentar una reclamación ante las Autoridades de Control
- El origen de los datos
- Las categorías de los datos

# DERECHOS DE LOS INTERESADOS

ACCESO  
Saber que datos son tratados

RECTIFICACIÓN  
Rectificar datos

SUPRESIÓN  
Eliminación de datos

OPOSICIÓN  
Oposición a una parte del tratamiento

OLVIDO  
Supresión de datos hechos públicos

LIMITACIÓN DEL TRATAMIENTO  
Para interponer una reclamación

PORTRABILIDAD DE LOS DATOS  
Facilitar los datos en un archivo

DECISIONES AUTOMATIZADAS  
No verse afecto y conocer la lógica aplicada

## OBJETIVO:



## PROCEDIMIENTO

PROTECCIÓN EFECTIVA



EXIGE QUE SE REFUERCEN Y ESPECIFIQUEN LOS DERECHOS (interesados) Y OBLIGACIONES (responsables)

GRATUITO

SENCILLO

PLAZO ÚNICO

# PROCEDIMIENTO PARA ATENDER DERECHOS:

- Todos los interesados de los tratamientos de datos (clientes, empleados, contactos, etc.) podrán ejercer sus derechos ante el responsable del tratamiento (LCC SPAIN) que deberá ser capaz de contestar y proceder a lo solicitado dentro del plazo establecido.
- Para ello existe un procedimiento concreto que debe ser conocido por todos los integrantes de la entidad. No obstante, la obligación de contestar la ostenta la organización como responsable del tratamiento.
- Es importante que, cuando tengamos conocimiento de un ejercicio o solicitud de derechos, se envíe al canal de comunicación establecido al efecto, para proceder a dar respuesta en tiempo y forma.



# SEGURIDAD DE LOS DATOS

## PERSPECTIVA PREVENTIVA



Desaparecen las medidas de seguridad que el Reglamento de desarrollo de la LOPD imponía en función del nivel de seguridad de los datos tratados.

Habrá que documentar los riesgos teniendo en cuenta las medidas ya implantadas, y analizar la efectividad de las mismas. ¿Responden a los riesgos y a lo previsto en el RGPD?

Gestión del riesgo: definir las medidas a implantar en función de las debilidades detectadas (posibilidad de destrucción, pérdida o alteración accidental o ilícita, comunicación o acceso no autorizado, etc.)

Medidas de seguridad: deben garantizar la confidencialidad, integridad, disponibilidad, y recuperación de forma rápida de la información.

ACCOUNTABILITY

PRIVACY BY DESIGN

PRIVACY BY DEFAULT

# MEDIDAS DE SEGURIDAD



La protección de datos aplica a todo el personal de LCC en sus respectivas rutinas de trabajo, en la medida en que puedan tratar, en mayor o menor medida, datos de carácter personal, por lo que deben cumplirse las siguientes medidas

- El archivo en papel deberá estar guardado en armarios cerrados con llaves para evitar el acceso no autorizado. En caso de encontrarse en un despacho o sala, éste espacio debe estar custodiado y cerrado con llave.
- Los archivos en papel deberán estar clasificados con una nomenclatura que sólo pueda ser conocido por quien gestiona o trabaja con ellos, evitando una clasificación estándar de fácil consulta (Ej: ficheros laborales clasificados por nombres y apellidos de empleados).
- Deberá respetarse la política de mesas limpias de manera que no se depositen datos personales en los puestos de trabajo, salvo consulta custodiada.
- Está prohibido extraer documentación sin la debida autorización fuera de las instalaciones de LCC.



# MEDIDAS DE SEGURIDAD II

- Acceso a los archivos o carpetas de red deberá ser repasado periódicamente por el encargado para verificar que cada empleado tenga acceso sólo a la información necesaria para el desempeño de sus funciones.
- Deberá trabajarse en local sólo para documentos en producción o consulta, una vez finalizada la jornada los documentos confeccionados o tratados deberán subirse al sistema establecido como autorizado y eliminar los ficheros temporales.
- Política de contraseñas: periodicidad de cambio (mínimo cada seis meses, robustez de la contraseña, confidencialidad de la contraseña).
- Está prohibido subir documentos de trabajo a sistemas o plataformas no autorizados por LCC.
- No está permitido descargar software no autorizado en los equipos/dispositivos de trabajo de LCC.
- Los equipos deberán ser debidamente bloqueados cuando un trabajador se ausente de su puesto de trabajo para evitar accesos indebidos.



# GESTIÓN DE INCIDENCIAS

**OBLIGACIÓN LEGAL: ART. 33-34.**  
**Obligación de notificar a la autoridad de control las violaciones de seguridad:**

- En caso de producirse una violación de la seguridad de los datos, esta debe notificarse si la violación de la seguridad constituye un **riesgo** para los derechos y libertades de las personas afectadas.
- Si la detecta el encargado de tratamiento debe notificarlo al responsable del tratamiento “sin dilación indebida” en el plazo establecido en el contrato de encargo del tratamiento.

¿QUÉ DEBE NOTIFICARSE?  
TODA VIOLACIÓN DE LA SEGURIDAD QUE SUPONGA

LA DESTRUCCIÓN O PERDIDA DE DATOS

ALTERACIÓN ACCIDENTAL O ILCITA

EL ACCESO NO AUTORIZADO

PONER EN CONOCIMIENTO DEL DEPARTAMENTO O EXTERNO QUE ANALIZARÁ QUE HA SUCEDIDO Y SU ALCANCE (VALORACIÓN DE LA BRECHA)

¿QUÉ TENEMOS QUE HACER?

PLANEAR MEDIDAS CORRECTIVAS

NOTIFICARLO EN 72 HORAS A LA AEPD

NOTIFICARLO A LOS AFECTADOS

# POLÍTICA DE PROTECCIÓN DE DATOS

## ART. 24.2

Constituye una obligación para el Responsable del tratamiento cuando resulte proporcionado a las actividades del tratamiento.

## CONTENIDO MÍNIMO

1. Ámbito subjetivo de aplicación
2. Alcance
3. Protocolos para la creación y modificación de tratamientos
4. Respeto de los principios de protección de datos
5. Respeto de los derechos de las personas interesadas
6. Responsabilidades de la dirección
7. Responsabilidades de los empleados
8. La gestión de riesgos
9. Declaraciones sobre la seguridad de los datos
10. Aplicación del principio de responsabilidad proactiva
11. Organización para la gestión de la protección de datos
12. Verificación del cumplimiento de la política y su revisión

# REGISTRO DE ACTIVIDADES DEL TRATAMIENTO (RAT)

OBLIGACIÓN MATERIAL DEL RESPONSABLE QUE SUSTITUYE LA OBLIGACIÓN DE LA LOPD

15/1999 DE NOTIFICAR FICHEROS JURÍDICOS A LA AEPR

## ¿CUÁNDO?

A) >250 empleados (siempre)

B) < 250 empleados:

- 1.Si entraña riesgo para los derechos y libertades
- 2.Si el tratamiento no es ocasional
- 3.Si se tratan categorías especiales de datos (art.9.1)
- 4.Si se tratan datos relativos a condenas o infracciones penales (art. 10)

## ¿CÓMO?

A partir de los ficheros ya registrados (detallando las operaciones)

- En torno a operaciones de tratamiento concretas que tienen una finalidad común
- Podrá organizarse en torno a conjuntos estructurados de datos
- por “escrito”, lo que obviamente incluye el formato electrónico

## UTILIDAD

Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.”

# CONTENIDO MÍNIMO DEL RAT (ART. 30)

	Responsable (actividades)	Encargado (categorías de actividades)
Datos identificativos y de contacto	<ul style="list-style-type: none"><li>• Responsables</li><li>• Corresponsables</li><li>• Representante del responsable</li><li>• Delegado de protección de datos</li></ul>	<ul style="list-style-type: none"><li>• Encargado</li><li>• Otros encargados</li><li>• Representante del encargado</li><li>• Responsables</li><li>• Representantes de responsables</li><li>• Delegado de protección de datos</li></ul>
Descripción del tratamiento	<ul style="list-style-type: none"><li>• Finalidades</li><li>• Descripción categorías personas</li><li>• Descripción categorías datos</li><li>• Descripción destinatarios</li><li>• Descripción general de las medidas</li><li>• Plazos de supresión</li></ul>	<ul style="list-style-type: none"><li>• Categoría de tratamientos efectuados por cuenta responsable</li><li>• Descripción general de las medidas</li></ul>
Transferencias internacionales	<ul style="list-style-type: none"><li>• Descripción de las transferencias</li><li>• Identificación de los países de destino</li><li>• Identificación de organización internacional</li><li>• La documentación que aporte garantías adecuadas para supuestos art. 49.1</li></ul>	<ul style="list-style-type: none"><li>• Descripción de las transferencias (encargo)</li><li>• Identificación de los países de destino</li><li>• Identificación de organización internacional</li><li>• La documentación que aporte garantías adecuadas para supuestos art. 49.1</li></ul>

# DESIGNACIÓN del DPO

Atendiendo a sus cualidades profesionales

INTERNO (en plantilla) o EXTERNO (prestador de servicios)

La no designación en caso de ser necesaria, será constitutiva de infracción

Sector público (no tribunales)

Responsables y encargados del tratamiento cuya actividad principal consista en

Observación habitual y sistemática a **gran escala**

Categorías especiales de datos y relativos a condenas penales e infracciones penales a gran escala

Otros supuestos previstos por los estados o derecho de la UE. En España, aquellos casos contemplados en el artículo 34 LOPD.

Designación voluntaria

# FUNCIONES DEL DPO

## Respecto de RT y ET, asesorar, informar y supervisar

- En relación a las obligaciones previstas en el RGPD y otras disposiciones
- En relación al cumplimiento
- En relación a las Evaluaciones de Impacto

## Respecto de la autoridad de control

- Cooperar
- Servir de punto de contacto

## Respecto de las personas afectadas:

- Atender ejercicio de derechos y cuestiones relacionadas con el tratamiento de los datos

# TRATAMIENTOS DE DATOS ENCARGADOS A TERCEROS



SON CASOS EN LOS QUE EXISTE UNA RELACIÓN ENTRE UN TERCERO (EMPRESAS PRESTADORAS DE SERVICIOS) Y EL RESPONSABLE EN VIRTUD DE LA CUAL AQUÉL PRESTA UN SERVICIO, CUALQUIERA QUE SEA SU NATURALEZA, QUE EXIGIRÁ, EN MUCHOS CASOS, QUE LOS DATOS PERSONALES DEBAN SER CONOCIDOS Y TRATADOS POR EL TERCERO O POR SU PERSONAL



EL ACCESO A LOS DATOS POR CUENTA DE TERCEROS DEBERÁ SIEMPRE REGULARSE A TRAVÉS DE UN CONTRATO POR ESCRITO:

**BEBEMOS TENER UNA LISTA CON TODOS LOS ENCARGADOS DE TRATAMIENTO Y TENER FIRMADO LOS CONTRATOS SOBRE ENCARGO DE DATOS.** El contenido debe ser el siguiente:

- Objeto, duración, naturaleza y la finalidad del tratamientos
- Tipo de datos personales y categorías de interesados
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados

# EVALUACIÓN DE IMPACTO

## ART. 35

Definición: PIA (Privacy Impact Assessment) : proceso mediante el cual se evalúan cuestiones relacionadas con el tratamiento de datos de carácter personal, con la finalidad de controlar el impacto negativo que, sobre la privacidad de las personas afectadas, puedan tener las operaciones de tratamiento.

Régimen jurídico: “Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas”

Casos previstos: El RGPD no establece una lista exhaustiva:

- evaluación “sistemática y exhaustiva” de aspectos personales relativos a personas físicas
- tratamiento a gran escala de las denominadas categorías especiales de datos
- observación sistemática a gran escala de áreas de acceso público

Autoridades de control: deberán determinar y publicar, la lista de los tipos de operaciones de tratamiento que estarán sujetas a la exigencia de PIA; podrán establecer y publicar la lista de los tipos de operaciones de tratamiento que **no** requerirán PIA.

Con carácter general habrá que llevar a cabo una PIA si es probable que el tratamiento suponga un alto riesgo para los derechos y libertades de las personas, especialmente si se utilizan nuevas tecnologías, o si las operaciones de tratamiento por su naturaleza, alcance, contexto o finalidades generan alto riesgo

# TRANSFERENCIAS INTERNACIONALES

- Se mantienen los criterios ya establecidos en la Directiva 95/46
- El exportador de datos puede ser tanto un responsable del tratamiento, como un encargado
- Se amplían los mecanismos para aportar garantías adecuadas
- Códigos de conducta
- Certificaciones, sellos y marcas como mecanismos para ofrecer garantías adecuadas
- Normas corporativas vinculantes (se reconocen)
- Se reducen los supuestos en que se precisa de autorización expresa de la autoridad de control

# RÉGIMEN SANCIONADOR



Advertencia (infracción potencial)



Apercibimiento



Suspensión del tratamiento



MULTAS

- Atendiendo a cada caso individual
- Cada Estado podrá decidir si impone multas administrativas al sector público
- Posibilidad de adopción de otras sanciones por parte de los Estados

# RÉGIMEN SANCIONADOR

- Multas administrativas: efectivas, proporcionadas y disuasorias. Los responsables del tratamiento podrían ser multados con hasta 20 millones de euros o el 4 % de su volumen de negocios total anual.
- Medidas adicionales o sustitutorias de los “poderes correctivos”
  - Advertencia (infracción potencial)
  - Apercibimiento
  - Atender ejercicio de derechos
  - Adecuar los tratamientos
- Criterios para decidir la imposición, atendiendo a cada caso individual
- Cada Estado podrá decidir si impone multas administrativas al sector público
- Posibilidad de adopción de otras sanciones por parte de los Estados