

JORNADA DE FORMACIÓN DPD ADMINISTRACIÓN AUTONÓMICA Y LOCAL

Sevilla, 29 de marzo de 2019

EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

José Luis Falcón Pliego

Gabinete de Publicidad Activa

Delegado de Protección de Datos del CTPDA

1

INTRODUCCIÓN

INTRODUCCIÓN

PRINCIPIOS APLICABLES AL TRATAMIENTO

LICITUD, LEALTAD Y
TRANSPARENCIA

LIMITACIÓN DE LA
FINALIDAD

MINIMIZACIÓN DE DATOS

EXACTITUD

LIMITACIÓN DEL PLAZO
DE CONSERVACIÓN

INTEGRIDAD Y
CONFIDENCIALIDAD

Art. 5.1
RGPD

Responsabilidad proactiva: *El responsable del tratamiento será responsable del cumplimiento de lo anterior y capaz de demostrarlo.*

Art. 5.2
RGPD

PRINCIPIOS APLICABLES AL TRATAMIENTO

Responsabilidad proactiva: *El responsable del tratamiento será responsable del cumplimiento de lo anterior y capaz de demostrarlo.*

Art. 5.2
RGPD

HACER COSAS CONSTANTEMENTE PARA CUMPLIR LOS PRINCIPIOS Y DOCUMENTAR ACREDITAR QUE SE HACEN

TRATAMIENTO



OBLIGACIONES DEL RESPONSABLE

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.

Art 24.1

INTRODUCCIÓN

Protección de datos desde el diseño

Art 25.1 RGPD

Protección de datos por defecto

Art 25.2 RGPD

*Más vale prevenir
que curar*

Protección de datos **desde el diseño**

Art 25.1 RGPD

¿Qué?

Aplicación por parte del responsable de **medidas técnicas y organizativas apropiadas** a fin de **cumplir** los principios y requisitos del RGPD

¿Cuándo?

Tanto **en el momento de determinar los medios** del tratamiento como en el propio tratamiento

¡Ojo!

- **Estado** de la técnica
- **Coste** de la aplicación
- **Características** del tratamiento
- **Riesgos** del tratamiento para derechos y libertades

INTRODUCCIÓN

Protección de datos **desde el diseño**

Art 25.1 RGPD

MEDIDAS TÉCNICAS

- infraestructura tecnológica y herramientas a utilizar
- necesidad de encriptar información
- valorar uso alta disponibilidad en sistemas informáticos / centro de respaldo
- uso de dispositivos móviles y los riesgos asociados
- políticas de salvaguardia de la información

...

- determinar los recursos humanos que serán necesarios para el tratamiento / formación
- diseñar formularios
- prever los procedimientos (o normas) que han de establecerse para el tratamiento
- analizar la posible necesidad de encargos de tratamiento

MEDIDAS ORGANIZATIVAS

...

Protección de datos **por defecto**

Art 25.2 RGPD

¿Qué?

Aplicación por parte del responsable de **medidas técnicas y organizativas apropiadas** a fin de garantizar que, por defecto, **solo** sean objeto de **tratamiento** los **datos** personales que sean **necesarios** para cada uno de los **finés** específicos del tratamiento

Cantidad de datos recogidos / **Extensión** de su tratamiento / Plazo de **conservación** / **Accesibilidad**

Aplicable a

Garantizar

Datos personales no accesibles, sin intervención, a un número indiscriminado de personas físicas

INTRODUCCIÓN

Protección de datos **por defecto**

Art 25.2 RGPD

MEDIDAS TÉCNICAS

- habilitar pantallas o informes específicos para las distintas finalidades del tratamiento
- implementar perfiles de usuarios para el acceso
- prever limitaciones en la difusión (Intranet)

...

- establecer limitaciones físicas para el acceso
- determinar plazos para cancelar información
- establecer políticas de manejo de documentación
- uso de categorías especiales de datos

...

MEDIDAS ORGANIZATIVAS

ALGUNAS OBLIGACIONES DEL RESPONSABLE

R
E
S
P
O
N
S
A
B
I
L
I
D
A
D

REGISTRO DE
ACTIVIDADES DE
TRATAMIENTO

ADAPTAR CLAÚSULAS
INFORMATIVAS Y
CONTRACTUALES

ANÁLISIS DE RIESGOS

MEDIDAS DE SEGURIDAD

FORMACIÓN E
INSTRUCCIONES AL
PERSONAL

DESIGNAR DELEGADO DE
PROTECCIÓN DE DATOS

EVALUACIONES DE
IMPACTO

NOTIFICAR VIOLACIONES
DE SEGURIDAD

ATENDER EJERCICIO DE
DERECHOS DE LOS
INTERESADOS

COOPERAR CON AUTORIDADES
DE CONTROL

P
R
O
A
C
T
I
V
A

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

ALGUNAS CONSIDERACIONES:

- s/ protección de datos 'POR DEFECTO'
- s/ 'ADECUARSE' vs 'ESTAR ADECUADO'

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

2

**REGISTRO DE ACTIVIDADES
DE TRATAMIENTO**

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Cada **responsable** llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, con indicación de:

- Nombre y contacto del **responsable** (corresponsable / representante)
- Nombre y contacto del **DPD** (en su caso)
- **Fines** del tratamiento
- **Categorías de interesados** y de **datos personales**
- **Categorías de destinatarios**
- Destino **transferencias internacionales** de datos (y, en su caso, garantías)
- **Plazos** previstos para la **supresión** de las diferentes categorías de datos (cuando sea posible)
- **Medidas técnicas** y organizativas **de seguridad** (cuando sea posible)

Art 30.1

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Cada **encargado** llevará un registro de las categorías de actividades de tratamiento efectuadas por cuenta de un responsable, con indicación de:

- Nombre y contacto del **encargado** (representante)
- Nombre y contacto del **DPD** (en su caso)
- Nombre y contacto de **cada responsable**
- **Categorías de tratamiento** efectuadas por cuenta de cada responsable
- Destino **transferencias internacionales** de datos (y, en su caso, garantías)
- **Medidas** técnicas y organizativas **de seguridad** (cuando sea posible)

Art 30.2

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Art 30.3

- Los registros anteriores **constarán por escrito**, inclusive en formato electrónico

Art 30.4

- Se pondrán **a disposición de la autoridad de control** que lo solicite

Excepciones

Art 30.5

- Empresa u organización que emplee a **menos de 250 personas, a menos que** el tratamiento que realice pueda **entrañar un riesgo** para los derechos y libertades de los interesados, **no sea ocasional**, o incluya **categorías especiales de datos** personales o relativos a **condenas e infracciones penales**

¿QUÉ APORTA LA LOPDGDD?

Art 31 LOPDGDD

- El registro podrá organizarse en torno a **conjuntos estructurados** de datos
- El responsable/encargado deberá **comunicar** cualquier alta, modificación o baja **al DPD**
- Los sujetos art. 77.1 deberán **hacer público** un inventario de actividades de tratamiento **por medios electrónicos** con: **INFORMACIÓN ART. 30 RGPD + BASE LEGAL**

DF 11ª LOPDGDD

- Modifica la Ley 19/2013 para convertir en una obligación de **Publicidad Activa** la publicación del inventario de actividades de tratamiento

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

CONDICIONES PARA LA LICITUD DE TRATAMIENTO

CONSENTIMIENTO	INTERESES VITALES
CONTRATO	INTERÉS PÚBLICO O EJERCICIO DE PODERES PÚBLICOS
OBLIGACIÓN LEGAL	INTERÉS LEGÍTIMO

¿QUÉ INDICA LA LOPDGDD?

Art 8

- El tratamiento solo podrá basarse en el cumplimiento de una **obligación legal** exigible al responsable **si lo prevé una Ley** (o norma de la UE)
- El tratamiento solo podrá basarse en el cumplimiento de una misión realizada en **interés público** o en el **ejercicio de poderes públicos** si deriva de una competencia con rango de Ley.

ALGUNOS COMENTARIOS:

- **Publicación inventario ‘SUSTITUYE’ RGPD**
- **‘MODELOS’ ya publicados; se van publicando**
- **Nombre DPD?**
- **Buen momento para ‘REFLEXIONAR’**
- **IMPORTANTE para otras tareas del responsable**
- **Inicio de la documentación sobre el cumplimiento**

3

CLÁUSULAS INFORMATIVAS

INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTENGAN DEL INTERESADO

Art 13

- El **responsable** ofrecerá, en el momento en que se obtengan los datos (salvo que el interesado ya disponga de la información):

- **Identidad** y datos de contacto del **responsable**
- Datos de **contacto** del **Delegado de Protección de Datos** (DPD/DPO) 
- **Fines y base jurídica** del tratamiento (o intereses legítimos en que se basa) 
- **Destinatarios** o categorías de destinatarios, en su caso
- Información s/ **transferencias internacionales** de datos, en su caso

Art 13.1

...

INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTENGAN DEL INTERESADO

Art 13

GARANTIZAR TRATAMIENTO
LEAL Y TRANSPARENTE

- **Plazo o criterios de conservación** de los datos 
- **Derecho a solicitar:** acceso, rectificación, supresión, limitación del tratamiento, oposición, portabilidad
- Derecho a **retirar el consentimiento** otorgado previamente
- Derecho a presentar **reclamación ante una autoridad de control** 
- Si la comunicación de datos es un **requisito legal o contractual** (o necesario para suscribir un contrato); si hay **obligación** de facilitar los datos y las **consecuencias de no hacerlo**.
- Existencia de **decisiones automatizadas**, incluida la elaboración de perfiles, lógica aplicada e importancia y **consecuencias** para el interesado 

Art 13.2

INFORMACIÓN A FACILITAR CUANDO LOS DATOS NO SE OBTENGAN DEL INTERESADO

Art 14

- El responsable facilitará la siguiente información:

- **IDEM ANTERIOR** (**salvo** la relativa a la obligatoriedad de aportar datos y consecuencias de no hacerlo)
- Las **categorías de datos** que se tratan
- La **fuentes** de la que proceden los datos

¿CUÁNDO?

- como **máximo**, en **un mes** desde su obtención
- si hay comunicación con el interesado, a más tardar, **en la primera comunicación**
- si se comunican a otros, a más tardar, **cuando se comuniquen por primera vez**

INFORMACIÓN A FACILITAR CUANDO LOS DATOS NO SE OBTENGAN DEL INTERESADO

Art 14

- Excepciones:

- El interesado **ya dispone** de la información
- La comunicación resulte **imposible** o suponga un esfuerzo **desproporcionado** (en particular para fines de archivo, investigación o estadística)
- **Lo establezca el Derecho** de la UE o los EM
- Cuando los datos deban seguir teniendo **carácter confidencial** sobre la base del **secreto profesional** regulado por el Derecho de la UE o los EM

Las exigencias del RGPD obligan a **modificar las cláusulas** informativas que aparecían en formularios, carteles informativos, páginas web, etc.



“GUÍA PARA EL CUMPLIMIENTO
DEL DEBER DE INFORMAR”

AEPD / APDCAT / AVPD



“GUÍA PARA EL CUMPLIMIENTO DEL DEBER DE INFORMAR”
AEPD / APDCAT / AVPD

1	¿A quién va dirigida esta guía?	2
2	¿Qué cambia el RGPD sobre el deber de informar?.....	2
3	¿Quién y cuándo debe informar?	3
4	¿Dónde y cómo informar?	4
5	Información por capas	5
6	Información básica (primera capa)	6
7	Información adicional (segunda capa)	8
7.1	Epígrafe “Responsable”	9
7.2	Epígrafe “Finalidad”	10
7.3	Epígrafe “Legitimación”	11
7.4	Epígrafe “Destinatarios”	13
7.5	Epígrafe “Derechos”	14
7.6	Epígrafe “Procedencia”	15

Se consolida en el art. 11 LOPDGDD

INFORMACIÓN A FACILITAR **EN PRIMERA CAPA**

Art 11 LOPDGDD

- IDENTIDAD DEL RESPONSABLE
- FINALIDAD DEL TRATAMIENTO
- POSIBILIDAD EJERCICIO DE DERECHOS

1ª CAPA

Si no se han obtenido del interesado, además:

- CATEGORÍAS DE DATOS QUE SE TRATAN
- FUENTES DE LA QUE PROCEDEN LOS DATOS

Dirección electrónica u otro medio para acceder al resto de la información (2ª capa)

ALGUNOS COMENTARIOS:

- s/ **'PELIGROS'** de la 2ª capa
- s/ datos suministrados **POR EL INTERESADO SIN** posibilidad de recibir **INFORMACIÓN**
- s/ información **'CONFUSA'** sobre el tratamiento principal (paso por **REGISTRO**)

4

ADAPTACIÓN DE CONTRATOS

EL ENCARGADO DEL TRATAMIENTO

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales **por cuenta del responsable** del tratamiento

¡¡ IMPRESCINDIBLE VINCULACIÓN JURÍDICA CON EL RESPONSABLE !!

Puede no existir o puede haber varios por cada tratamiento

EL ENCARGADO DEL TRATAMIENTO

- Elegido por el responsable **solo si ofrece garantías suficientes** para que el tratamiento sea conforme con el Reglamento
- El encargado no recurrirá a otro encargado sin **autorización previa del responsable**, tanto para el inicio de la actividad como para posibles cambios de encargados
- El tratamiento por el encargado se registrará por un **contrato u otro acto jurídico** que vincule al encargado respecto del responsable y establezca:

Objeto, duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable

El vínculo jurídico deberá estipular

- **Instrucciones** del responsable sobre el tratamiento
- El compromiso del deber de **confidencialidad**
- Las **medidas de seguridad** que se han de aplicar
- Condiciones a aplicar en caso de **subcontratación**
- Cómo abordar la posible **solicitud de derechos** de los interesados
- Cómo **asistir**, en su caso, al cumplimiento de obligaciones del **responsable**
- El destino de los **datos** cuando **finalice 'el contrato'**
- La **colaboración** con el responsable para **demostrar el cumplimiento** de la normativa

Las exigencias del RGPD obligan a **modificar las cláusulas** que solían utilizarse en contratos y otros vínculos jurídicos.



“DIRECTRICES PARA LA
ELABORACIÓN DE CONTRATOS
ENTRE EL RESPONSABLES Y
ENCARGADOS DEL TRATAMIENTO”

AEPD / APDCAT / AVPD



“DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE EL RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO”

AEPD / APDCAT / AVPD

ANEXO I

Ejemplo de cláusulas contractuales para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas

1. Objeto del encargo del tratamiento
2. Identificación de la información afectada
3. Duración
4. Obligaciones del encargado del tratamiento
5. Obligaciones del responsable del tratamiento

¿QUÉ APORTA LA LOPDGDD?

Art 33 LOPDGDD

- **No** se considera **'comunicación'** de datos el acceso por parte del encargado
- Posibilidad de que **un órgano de la Admón. Pública sea encargado** mediante una norma reguladora que incorpore lo exigido en el 28.3 RGPD

DT 5ª LOPDGDD

- **Contratos anteriores a 25/05/2018, vigentes hasta su vencimiento (salvo indefinidos, hasta 25/05/2022)**
- Durante dicho plazo cualquier de las partes podrá **instar a la otra la modificación** del contrato.

ALGUNOS COMENTARIOS:

- Atención a 'NO CONTRATOS'
- Un modelo es 'UN MODELO'
- Finalidad principal del contrato vs actuaciones como encargo del tratamiento
- Desplazamiento a PPT vs PCAP?

CONSIDERACIONES FINALES

5

CONSIDERACIONES FINALES

CONSIDERACIONES FINALES

ALGUNAS OBLIGACIONES DEL RESPONSABLE

R
E
S
P
O
N
S
A
B
I
L
I
D
A
D

REGISTRO DE
ACTIVIDADES DE
TRATAMIENTO

ADAPTAR CLAÚSULAS
INFORMATIVAS Y
CONTRACTUALES

ANÁLISIS DE RIESGOS

MEDIDAS DE SEGURIDAD

ATENDER EJERCICIO DE
DERECHOS DE LOS
INTERESADOS

FORMACIÓN E
INSTRUCCIONES AL
PERSONAL

DESIGNAR DELEGADO DE
PROTECCIÓN DE DATOS

EVALUACIONES DE
IMPACTO

NOTIFICAR VIOLACIONES
DE SEGURIDAD

COOPERAR CON AUTORIDADES
DE CONTROL

P
R
O
A
C
T
I
V
A

Hay que hacer “muchas cosas”, pero...

¿QUIÉN LO HACE?

Todo el personal de la organización, **BAJO EL IMPULSO DE LA DIRECCIÓN**, ha de involucrarse, a distinto nivel y con distintas funciones

- **PLAN DE COMUNICACIÓN, CONCIENCIACIÓN Y FORMACIÓN DEL PERSONAL**
- **INSTRUCCIONES CLARAS EN RELACIÓN CON SUS FUNCIONES Y OBLIGACIONES RESPECTO AL TRATAMIENTO DE DATOS PERSONALES EN SU PUESTO DE TRABAJO**

Hay que hacer “muchas cosas”, pero...

¿QUIÉN LO HACE?

Un grupo de trabajo o una estructura permanente

LLEVAR LA INICIATIVA Y MARCAR LAS PAUTAS
DE LAS ACTIVIDADES DEL ORGANISMO PARA LA
ADECUACIÓN A LA NORMATIVA

CON EL ASESORAMIENTO DEL
DPD

COORDINACIÓN DENTRO DE UNA ORGANIZACIÓN 'GRANDE' Y COLABORACIÓN ENTRE ORGANISMOS 'PEQUEÑOS', PARA:

- **DISEÑO Y HOMOGENEIZACIÓN DE PROCEDIMIENTOS Y MODELOS; DEFINIR LA DOCUMENTACIÓN 'A LLEVAR' SOBRE EL CUMPLIMIENTO**
- **HOMOGENEIZAR PROCEDIMIENTOS Y DOCUMENTOS ESTABLEZCAN**
- **PAUTAS PARA LA METODOLOGÍAS DE ANÁLISIS DE RIESGO Y EVALUACIÓN DE IMPACTO**
- **ASESORAR Y RESUELVAR CONSULTAS**
- **APROVECHAMIENTO DE RECURSOS vs DISPERSIÓN**
- **COMPARTIR Y REUTILIZAR EXPERIENCIAS**
- **DETECTAR Y PROPONER ACTIVIDADES DE FORMACIÓN**
- **EFICACIA Y EFICIENCIA Y BUEN GOBIERNO**

ETC.
ETC.
ETC.

**TODO ELLO REFORZARÍA LA
DEMOSTRACIÓN DE LA
RESPONSABILIDAD PROACTIVA
DE LA ORGANIZACIÓN EN EL
CUMPLIMIENTO DEL RGPD**

ALGUNAS PROPUESTAS FINALES:

- Cláusulas informativas para el personal
- 'DOSSIER' Protección de Datos

FIN

¡Ánimo!

y...

...¡Muchas gracias!

José Luis Falcón Pliego

joseluis.falcon@juntadeandalucia.es