



PROTECCIÓN DE DATOS

DATU-BABESA

UNA MIRADA ADAPTADA AL MUNDO
DE LAS AMPAS

DATU-BABESA IGE BATEN
IKUSPUNTUTIK

Azaroak 10 | 10 de noviembre

9:30 - 13:30

"La Bolsa" (Salón de actos)

Pelota kalea 10, Bilbo

Naiara Souto, Abogada experta en protección de datos.
Abokatua, Datu-babesen aditua.

bige@bige.eus / 94 416 93 60



Bilbao Gurasoen Elkarteak

- ¿Qué **novedades** supone la nueva normativa?
- ¿Qué **es** eso de la protección de datos personales?
- ¿**Por qué** es importante?
- ¿Qué **obligaciones** genera? ¿Cómo podemos **cumplirlas**?
- ¿**Quién** tiene que cumplir las obligaciones?
- ¿Qué pasa **si no cumplimos**?
- Supuestos prácticos



The diagram consists of two large, light blue arrows that overlap in the center. The left arrow points to the left and contains the text 'En mi trabajo'. The right arrow points to the right and contains the text 'En mi vida privada'. The arrows are stylized with a slight 3D effect, featuring a darker blue shadow on the right side of the left arrow and the left side of the right arrow.

En mi trabajo

En mi vida privada

¿Qué es? ¿Por qué es importante?

edefundazioa

Derecho Fundamental a la Protección de Datos Personales

¿Qué es? ¿Por qué es importante?

Reconoce a cada persona:

- Facultad de **controlar** sus datos.
- Capacidad de **disponer** y decidir sobre ellos.

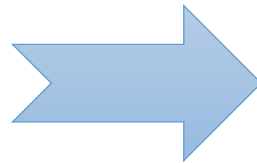
Redes Sociales, *Big data*, Internet de las Cosas, la “Nube”



Mayores riesgos - Más garantías

MARCO NORMATIVO

- ~~Directiva Europea 95/46/CE~~
- ~~LOPD = Ley Orgánica de Protección de Datos (1999)~~
- ~~Reglamento de Desarrollo de LOPD (2007)~~



25 mayo 2018

**Reglamento Europeo de
Protección de Datos:**
RGPD = GDPR

MARCO NORMATIVO

REGLAMENTO EUROPEO DE PROTECCION DE DATOS

Aplicación **directa** a partir **25 de mayo de 2018**

En vigor el 25 de mayo 2016



RD-Ley de medidas urgentes de adaptación a la normativa española (julio 2018)

(vigente hasta nueva Ley Orgánica: proyecto en tramitación)

**Publicaciones de las
Agencias de Protección
de Datos**



¿Qué podemos hacer?

edefundazioa



**CULTURA DE
LA PRIVACIDAD**

Dos modelos contrapuestos

edefundazioa



≡ EL PAIS

27 MAY 2018 - 10:54 CEST

Zuckerberg anuncia que Facebook extiende la ley de protección de datos europea a sus usuarios de todo el mundo

En sus esfuerzos por recuperar la confianza tan erosionada por los escándalos de filtración de datos de millones de sus usuarios, Facebook ha anunciado este jueves que ha decidido extender a los 2.000 millones de usuarios que tiene en el mundo entero [el reglamento europeo sobre protección de datos \(RGPD\) que entra en vigor este viernes](#). El máximo jefe y fundador de la red social, Mark Zuckerberg, ha ido más allá aún al afirmar, desde París, que se trata de una normativa que está en sintonía con los valores de Facebook.

elPeriódico

Viernes, 25/05/2018 a las 17:29 CEST

Webs de diarios de EEUU no son accesibles desde Europa por el nuevo reglamento de protección de datos

Medios como el 'Chicago Tribune' o el 'LA Times' tienen restringido el acceso a los ciudadanos europeos

Chicago Tribune

Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.

¿Cómo nos afecta la nueva normativa?

¿Qué tenemos que hacer?

¿Nos vale con lo que ya hemos hecho?



Recordando CONCEPTOS IMPORTANTES

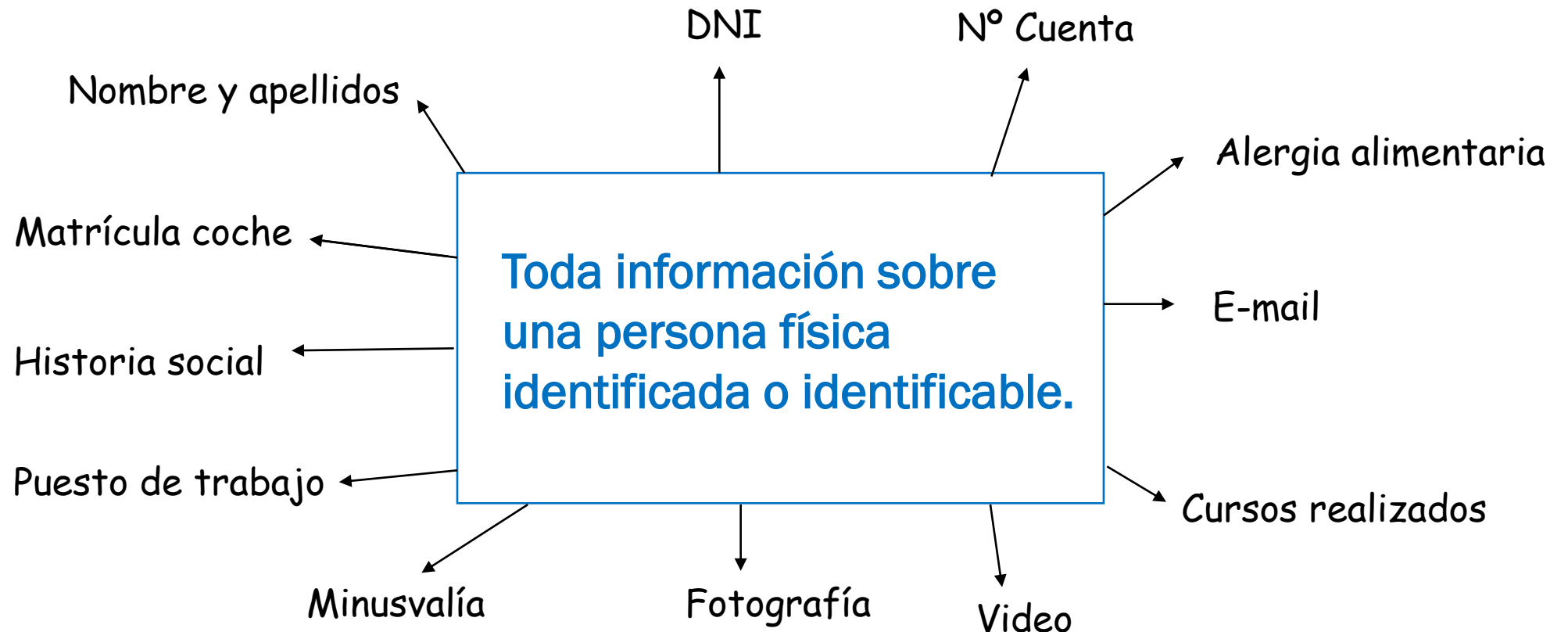
¿Qué es un dato personal?

En mi trabajo, ¿manejo datos personales?

¿Todos los datos son iguales?

Recordando CONCEPTOS IMPORTANTES

DATO PERSONAL



Recordando CONCEPTOS IMPORTANTES

TRATAMIENTO DE DATOS

Cualquier operación o conjunto de operaciones realizadas **sobre datos personales** o conjuntos de datos personales, ya sea **por procedimientos automatizados o no**, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Trato datos personales continuamente en mi trabajo diario. Cuando:

- *Recojo datos de las personas usuarias de servicios.*
- *Gestiono datos de personal (nóminas, contratos, formación).*
- *Utilizo datos de personas de contacto (proveedores).*
- *Facilito datos de las personas socias de mi entidad a terceros.*

¿Por qué es importante? ¿Qué pasa si no cumplimos?

¿Los datos que utilizo en mi trabajo son míos? ¿De quién sino?

¿Tengo que preocuparme por cumplir con la protección de datos? ¿O no es asunto mío?

¿Y si paso de hacer caso de la normativa? ¿Me pueden poner una multa?

¿Puedo ir a la cárcel?

¿Qué figuras intervienen en protección de datos?

**Responsable de
Tratamiento**

**Encargado de
Tratamiento**

Delegado de
Protección de
Datos

Interesado

Personas que
tratan datos

¿Responsable de
Seguridad?
¿Otras?

Recordando CONCEPTOS IMPORTANTES

INTERESADO

Persona física identificada o identificable cuyos datos personales se tratan.

Yo soy el interesado, respecto de mis datos personales:

- *mi nombre y apellidos*
- *mi dirección*
- *mi número de cuenta bancaria*
- *mi DNI*
- *mi experiencia laboral*
- *mi diagnóstico médico*
- *Fotos y vídeos en los que aparezco*

¿Quién tiene que cumplir?

RESPONSABLE DEL TRATAMIENTO

Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento.**

Cada entidad (empresa, asociación, fundación, etc) es **responsable** de los tratamientos de datos sobre los que **decide**.

- *Un grupo de danzas es responsable de los datos de su voluntariado.*
- *Un centro educativo es responsable de los datos de su alumnado.*
- *Un gimnasio es responsable de los datos de las personas que asisten.*
- *Una entidad o empresa es responsable de los datos de su personal.*

¿Quién tiene que cumplir?

ENCARGADO DEL TRATAMIENTO

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

Es un **prestador de servicios** – Necesidad de **CONTRATO**

- *La gestoría externa que nos realiza las nóminas.*
- *La empresa informática que nos desarrolla una base de datos.*
- *La empresa que contratamos para hacer una auditoría de calidad.*
- *La empresa que imparte clases de inglés al alumnado.*

¿Responsable o Encargado?

Cuando en mi entidad tratamos datos...

¿somos Responsable del Tratamiento?

¿o Encargado del Tratamiento?

¿Responsable o Encargado?

Cuando en mi entidad tratamos datos...

- somos **Responsable si decidimos** fines y medios del tratamiento.



Posibilidad de Corresponsables

- somos **Encargado si tratamos datos por cuenta del responsable:**

respetando sus instrucciones, les prestamos un servicio

Relación Responsable - Encargado

ENTRE RESPONSABLE Y ENCARGADO:

CONTRATO BILATERAL: Encargo de Tratamiento

O “acto jurídico unilateral” del responsable, vinculante para encargado

Con contenido obligatorio

Constancia escrita – válido formato electrónico

Relación Responsable - Encargado

CONTENIDO MÍNIMO DEL CONTRATO

LOPD

- ✓ Objeto
 - ✓ Duración
 - ✓ Naturaleza y finalidad del **tratamiento**
 - ✓ Tipo de **datos** personales
 - ✓ Categoría de **interesados**
- ✓ Obligaciones y derechos del **responsable**
 - ✓ Obligaciones y derechos del **encargado**

- Seguir instrucciones del Responsable.
- No utilizar los datos con fin distinto al que figure en contrato.
- No comunicar los datos a terceros, ni siquiera para su conservación.
- Implantar las medidas de seguridad.
- Finalizada la prestación, devolver o destruir los datos.

Relación Responsable - Encargado

OBLIGACIONES DEL ENCARGADO (1):

- Seguir **instrucciones** del responsable: tratamiento y comunicaciones.
- Personas con acceso a datos: **formación** y compromisos de **confidencialidad**
- **Medidas de seguridad:** En función de la evaluación de riesgos
- **Subcontratación.** Se permiten subencargados, con autorización.
- Destino de los datos, **al finalizar la prestación:** supresión o devolución

Relación Responsable - Encargado

OBLIGACIONES DEL ENCARGADO (2):

- **Colaboración en cumplir con las obligaciones del responsable:**
Información, Consentimiento, Notificación de violaciones de seguridad,
Derechos de interesados, Evaluaciones de Impacto de Privacidad
- **Colaboración para demostrar el cumplimiento:** en auditorías, inspecciones

Relación Responsable - Encargado

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



Relación Responsable - Encargado

ELECCIÓN DE ENCARGADO:

¿Encargado garantiza el cumplimiento de protección de datos?

- **RESPONSABLE:** Obligación de **diligencia en elección y supervisión.**
- **ENCARGADO:** Ofrecer **garantías** de las medidas técnicas y organizativas
 - Códigos de conducta
 - Certificados de protección de datos
 - Auditorías

CONCEPTOS IMPORTANTES

DELEGADO/A DE PROTECCIÓN DE DATOS (DPD = DPO)

- ✓ Necesario en la mayoría de los tratamientos:
Administraciones Públicas / “gran escala” / “alto riesgo”
- ✓ Funciones concretas: Supervisar. Asesorar. Cooperar con Agencias Protección Datos.
- ✓ Perfil profesional y posición definidos
- ✓ Publicar sus datos de contacto

OBLIGACIONES: cambio de paradigma

LOPD ↔ **RGPD**

CAMBIO DE ESQUEMA MENTAL

Cumplir

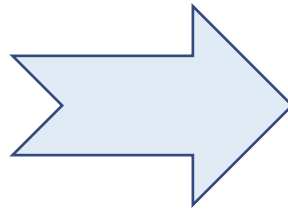
Cumplir +
Demostrar

OBLIGACIONES: cambio de paradigma

LOPD

CUMPLIMIENTO PASIVO

- Declarar ficheros
- Cláusulas LOPD
- Documento de Seguridad
- Auditorías
- Medidas de seguridad



RGPD

RESPONSABILIDAD PROACTIVA

- Registro interno de tratamientos
- Evaluaciones de Impacto de Privacidad
- Privacidad desde el diseño y por defecto
- Delegado/a de Protección de Datos
- Análisis y gestión de riesgos
- Códigos de conducta. Certificaciones

Entonces, ¿Qué hay que hacer?

OBLIGACIONES

- Información
- Legitimación para tratar los datos: Consentimiento
- Garantizar el ejercicio de los derechos del interesado
- Deber de confidencialidad
- Contrato entre responsable y encargado
- Nuevas medidas de responsabilidad proactiva

¿Cómo cumplimos con la obligación de informar?

¿**Cómo** informamos a las personas usuarias de que utilizamos sus datos?

¿**Quién** tiene que informar? ¿El responsable o el encargado?

¿**De qué** tenemos que informarles? ¿Cómo redacto la **clausulita**? ¿Nos vale con una estándar?

¿**Cuándo** hay que informar? ¿En qué casos no hace falta que informemos?

¿Cómo cumplimos con la obligación de informar?

DEBER DE INFORMACION

¿Cómo informar?

Información concisa, transparente, inteligible y de fácil acceso.

Lenguaje claro y sencillo.

Diferentes medios, según el tratamiento

INFORMACIÓN POR CAPAS O NIVELES:

- 1) Básica y resumida.
- 2) Más detallada.

¿Cómo cumplimos con la obligación de informar?

DEBER DE INFORMACION

¿De qué informar?

- ✓ Datos de Responsable y de Delegado de Protección de Datos
- ✓ Existencia de tratamiento y su finalidad
- ✓ Legitimación para el tratamiento
- ✓ Plazo de conservación de los datos, o los criterios para determinarlo
- ✓ Existencia de decisiones automatizadas o elaboración de perfiles
- ✓ Cesiones y transferencias internacionales: Destinatarios y fin
- ✓ Cómo ejercer derechos.

¿Cómo cumplimos con la obligación de informar?

DEBER DE INFORMACION

¿Cuándo hay que informar?

Cuando se solicitan los datos.

Si no se obtienen del titular:

- Antes de un mes
- La primera vez que contactamos

¿Quién debe informar?

El **responsable**



El **encargado**

¿Cómo cumplimos con la obligación de informar?

GUÍA PARA EL
CUMPLIMIENTO
DEL DEBER
DE INFORMAR



ZONA VIDEOVIGILADA



LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

¿Y que pasa con el consentimiento?

Además de informar, ¿tengo que pedir el **consentimiento** para gestionar datos?

¿Y si la persona **se niega**?

Una vez que tengo los datos, ¿puedo **utilizarlos para** lo que quiera?

¿Puedo **pasárselos a otras entidades** con las que colaboramos?

¿Y si son los datos de un **menor de edad**? ¿Le pregunto a sus padres?

¿Puedo hacer **fotos** de mis actividades y colgarlas en la página web?

Entonces, ¿Qué hay que hacer?

OBLIGACIONES

- Información
- **Legitimación para tratar los datos: Consentimiento**
- Garantizar el ejercicio de los derechos del interesado
- Deber de confidencialidad
- Contrato entre responsable y encargado
- Nuevas medidas de responsabilidad proactiva

Consentimiento y otras legitimaciones

Además de informar ...

¿Puedo tratar los datos?

Identificar claramente:

- ☐ En base a qué podemos utilizar los datos (legitimación)
- ☐ Para qué los necesitamos (finalidad)

Consentimiento y otras legitimaciones

LEGITIMACIÓN PARA EL TRATAMIENTO por el Responsable

- **Consentimiento informado**
- **Relación contractual**
- **Intereses vitales** del interesado o de otras personas
- **Obligación legal** para el responsable
- **Interés público** o ejercicio de **poderes públicos**
- **Intereses legítimos** prevalentes del responsable o de cesionarios

Consentimiento

CONSENTIMIENTO

INEQUIVOCO

- NO se permite tácito, ni casillas premarcadas
- Una declaración o una clara acción afirmativa

Para **finalidades diferentes, consentimientos diferentes:**

- ✓ Imágenes
- ✓ Cesiones (publicaciones, redes sociales, ...)

Consentimiento de MENORES DE EDAD

¿A qué EDAD pueden decidir sobre sus datos?

- Regla general: **16** años
- Posible que Estados otra, no menos de **13**.
 - (**Proyecto LOPD: 14**)

Entretanto:

AEPD: Se sigue aplicando norma previa (LOPD): **14 años**

AVPD: Se aplica RGPD: **16 años**



Consentimiento de MENORES DE EDAD

¿Quién decide sobre sus datos?

- Si **menores** de la edad establecida: sus progenitores o tutores
- Si **mayores** de la edad establecida: capacidad para consentir directamente,

Salvo que ley exija asistencia de progenitores o tutores.



LA VANGUARDIA

NUEVA NORMATIVA

WhatsApp confirma que fijará los 16 años como edad mínima para su uso

Hasta hora el usuario debía tener un mínimo de 13 años para utilizar su servicio de mensajería

EFE, Dublín

25/04/2018 17:57 | Actualizado a 25/04/2018 20:31

WhatsApp, propiedad de la red social Facebook, confirmó hoy que **elevará desde los 13 hasta los 16 años la edad mínima** para registrarse en **Europa** como **usuario** de su popular servicio de mensajería online, tal y como [avanzó el portal de noticias WABetaInfo](#).

Entonces, ¿Qué hay que hacer?

OBLIGACIONES

- Información
- Legitimación para tratar los datos: Consentimiento
- Garantizar el **ejercicio de los derechos del interesado**
- **Deber de confidencialidad**
- **Contrato** entre responsable y encargado
- Nuevas medidas de responsabilidad proactiva

GARANTIZAR DERECHOS DEL INTERESADO

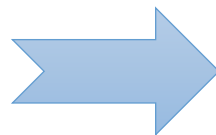
LOPD:

Acceso

Rectificación

Cancelación

Oposición



✓ De información

✓ Acceso

✓ Rectificación

✓ Supresión (**Al Olvido**)

✓ Oposición

✓ Limitación al tratamiento (nuevo)

✓ Portabilidad de los datos (nuevo)

LOS DERECHOS QUE TIENES PARA PROTEGER TUS DATOS PERSONALES

EL 25 DE MAYO DE 2018 SE APLICA EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ES IMPORTANTE QUE CONOZCAS CUÁLES SON TUS DERECHOS

1

DERECHO A CONOCER

- PARA QUÉ UTILIZAN TUS DATOS
 - Quién los tiene
 - Para qué los tienen
 - A quién los pueden ceder
 - Quiénes son sus destinatarios
- EL PLAZO DE CONSERVACIÓN DE TUS DATOS o Hasta cuándo van a ser utilizados
- QUE PUEDES PRESENTAR UNA RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
- LA EXISTENCIA DE DECISIONES AUTOMATIZADAS, LA ELABORACIÓN DE PERFILES Y SUS CONSECUENCIAS



2

DERECHO A SOLICITAR AL RESPONSABLE

- LA SUSPENSIÓN DEL TRATAMIENTO DE TUS DATOS
 - Si impugnamos la exactitud de los datos, mientras se verifica dicha exactitud por parte del responsable
 - Si hemos ejercitado nuestro derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre tus derechos
- LA CONSERVACIÓN DE TUS DATOS
 - Si el tratamiento es ilícito y nos oponemos a la supresión de los datos solicitando la limitación de su uso
 - Si los datos se necesitan para la formulación, ejercicio o defensa de reclamaciones
- LA PORTABILIDAD DE TUS DATOS A OTROS PROVEEDORES DE SERVICIOS
 - En un formato estructurado, de uso común y lectura mecánica, siempre que sea técnicamente posible para su portabilidad y cuando los hayan utilizado/tratado con tu consentimiento o por existir un contrato

3

DERECHO A RECTIFICAR TUS DATOS

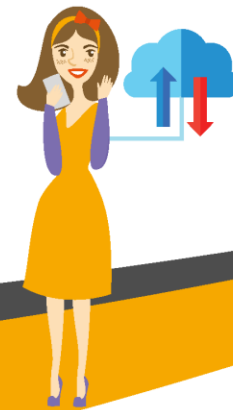
- CUANDO SEAN INEXACTOS
- CUANDO ESTÉN INCOMPLETOS



4

DERECHO A SUPRIMIR TUS DATOS

- POR TRATAMIENTO ILÍCITO DE DATOS
- POR LA DESAPARICIÓN DE LA FINALIDAD QUE MOTIVÓ EL TRATAMIENTO O RECOGIDA
- CUANDO REVOCAS TU CONSENTIMIENTO
- CUANDO TE OPONES A QUE SE TRATEN



5

DERECHO DE OPOSICIÓN AL TRATAMIENTO DE TUS DATOS

- POR MOTIVOS PERSONALES SALVO QUE QUIEN TRATA TUS DATOS ACREDITE UN INTERÉS LEGÍTIMO
- CUANDO EL TRATAMIENTO TENGA POR OBJETO EL MARKETING DIRECTO



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



www.agpd.es

DEBER DE CONFIDENCIALIDAD

¿QUIÉN?

Responsables

Encargados

Todas las personas que tratan datos

¿CUÁNDO?

Indefinidamente

Entonces, ¿Qué hay que hacer?

OBLIGACIONES

- Información
- Legitimación para tratar los datos: Consentimiento
- Garantizar el ejercicio de los derechos del interesado
- Deber de confidencialidad
- Contrato entre responsable y encargado
- **Nuevas medidas de responsabilidad proactiva**

Entonces, ¿Qué hay que hacer?

OBLIGACIONES

HERRAMIENTA FACILITA RGPD (www.aepd.es):

- Registro Actividades de Tratamiento
- Cláusulas informativas
- Modelo de contrato
- Medidas de Seguridad

MEDIDAS DE RESPONSABILIDAD ACTIVA

- ☐ DELEGADO/A DE PROTECCIÓN DE DATOS
- ☐ REGISTRO DE ACTIVIDADES DE TRATAMIENTOS
- ☐ ANALISIS DE RIESGOS
- ☐ PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO
- ☐ EVALUACIONES DE IMPACTO de PROTECCIÓN DE DATOS
- ☐ NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD
- ☐ CODIGOS DE CONDUCTA Y CERTIFICACIONES

DELEGADO/A DE PROTECCIÓN DE DATOS (DPD = DPO)

¿QUÉ ES? Nueva figura para [garantizar el cumplimiento de la protección de datos](#).

No es Responsable de Seguridad (LOPD)

¿OBLIGATORIO? En muchos casos, sí.

¿SE PUEDE NOMBRAR AUNQUE NO HAYA OBLIGACIÓN? SI.

Si se nombra, respetar sus funciones y sus requisitos de cualificación y posición.

Si hay dudas – Se recomienda analizar y documentar la decisión.

Novedades Reglamento Europeo

DELEGADO/A DE PROTECCIÓN DE DATOS (DPD = DPO)

¿CUÁNDO?

- ✓ **Autoridades u Organismos Públicos.** - ¿Y si Encargados de la Administración?
- ✓ Tratamientos “a gran escala”: nº interesados, volumen datos, territorio, duración...
- ✓ “Seguimiento regular y sistemático del interesado” (ej: fidelización de clientes, historia social...)
- ✓ **Categorías especiales de datos** y datos de condenas y delitos.

DELEGADO/A DE PROTECCIÓN DE DATOS (DPD = DPO)

¿CUÁNDO? **PROYECTO** LEY ORGÁNICA DE PROTECCIÓN DE DATOS (**NO VIGENTE**):

A título enunciativo, no limitativo:

- ✓ Centros educativos y Universidades
- ✓ Prestadores de servicios de comunicaciones
- ✓ Establecimientos de crédito
- ✓ Aseguradoras
- ✓ Empresas de energía y gas natural
- ✓ Actividades publicidad y de investigación
- ✓ Centros sanitarios, etc.

DELEGADO/A DE PROTECCIÓN DE DATOS (DPD = DPO)

FUNCIONES: “Controlar cumplimiento interno de protección de datos”

- **Informar y asesorar** de las obligaciones.
- Supervisar el **cumplimiento** legal. En concreto:
 - la asignación de responsabilidades internas
 - la concienciación y formación del personal
 - las auditorías correspondientes
- En **evaluaciones de impacto**: asesorar y supervisar su aplicación.
- **Con las Agencias** de Protección de Datos: cooperar y actuar como contacto.

DELEGADO/A DE PROTECCIÓN DE DATOS (DPD = DPO)

REQUISITOS : CUALIFICACIÓN Y POSICIÓN

- ✓ **Conocimientos especializados** del derecho y de la práctica de la protección de datos.
- ✓ **Independiente** funcional y jerárquicamente en el organigrama de la empresa.
No puede recibir instrucciones sobre sus funciones, ni ser destituido ni sancionado por el desempeño de su trabajo.
- ✓ **Reporta al más alto nivel jerárquico.**
- ✓ Sus **datos de contacto serán publicados y notificados** a la Agencia.
- ✓ **Interno** o un servicio **externo.**
- ✓ **No** debe existir **conflicto de intereses.**

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

¿QUÉ ES? Documentar los diferentes tratamientos de datos.

CONTENIDO: Por cada tratamiento:

- Identificación y datos de contacto del Responsable y del DPD
- Fines
- Categorías de interesados
- Tipos de datos
- Destinatarios existentes o previsto (incluidas transferencias internacionales)
- Base de legitimación del tratamiento
- Si es posible, las medidas de seguridad y los plazos de conservación

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

¿QUIÉN? Responsable
Encargado

¿CUÁNDO? En organizaciones en alguno de los siguientes supuestos:

- ✓ Más de 250 personas trabajadoras.
- ✓ Tratamientos de datos con riesgos para los interesados y no sea ocasional.
- ✓ Datos de categorías especiales o relativos a condenas e infracciones penales.

¿DÓNDE? A disposición de las Agencias de Protección de Datos, si lo solicitan.

ANALISIS DE RIESGOS

VALORACIÓN DE RIESGOS
DE TODOS LOS TRATAMIENTOS

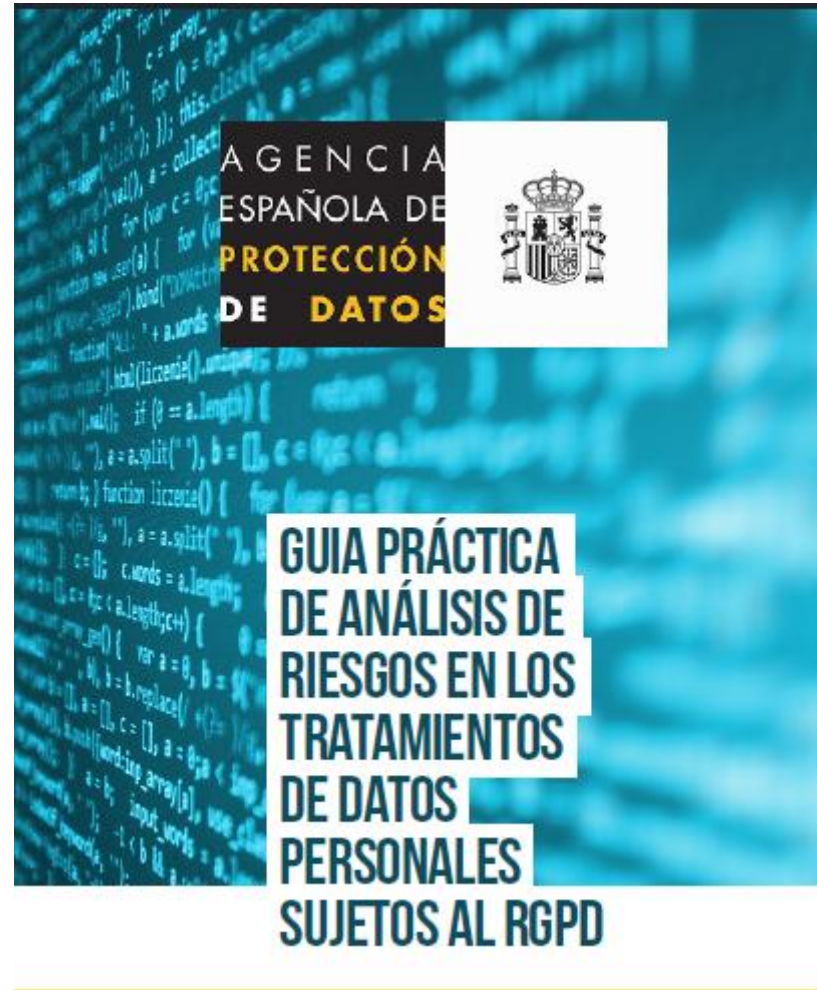


MEDIDAS DE SEGURIDAD

TENIENDO EN CUENTA:

- ✓ el estado de la **técnica**
- ✓ el **coste** de la aplicación de las medidas
- ✓ la naturaleza, ámbito, contexto y fines del **tratamiento**
- ✓ los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los **derechos y libertades de las personas físicas**.

ANALISIS DE RIESGOS



Novedades Reglamento Europeo

MEDIDAS DE SEGURIDAD: ejemplos

- ✓ Contraseñas no compartidas y seguras
- ✓ Perfiles de acceso diferenciados
- ✓ Copias de seguridad
- ✓ Recoger lo imprimido y eliminar lo escaneado
- ✓ Protector de pantalla
- ✓ ¿Almacenamiento en pendrives? ¿Fotos en móviles o cámaras?
- ✓ Utilizar CCO, al enviar *emails*, cuando sea necesario
- ✓ Datos en papel: destructoras, archivo, no sobre la mesa, impresora...

PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

¿QUÉ ES? Pensar en la protección de datos desde el diseño de un tratamiento.

¿QUÉ SUPONE?

- Medidas técnicas y organizativas adecuadas para aplicar los principios de protección de datos en los tratamientos.
- Medidas que garanticen que sólo se tratan los datos necesarios:
cantidad, periodo de conservación, personas con acceso

PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

¿QUIÉN? Responsable
Trasladable al Encargado

¿CUÁNDO? Antes de iniciar el tratamiento.
En el propio tratamiento.

EVALUACIONES DE IMPACTO DE PROTECCIÓN DE DATOS

¿CUÁNDO? Antes de puesta en marcha del tratamiento.

¿QUIÉN? Responsables. Trasladable a Encargados.

¿EN QUÉ CASOS? Cuando tratamiento entrañe un “**alto riesgo** para los derechos y libertades de las personas físicas, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines.”

Supuestos concretos:

- Perfiles como base para tomar decisiones.
- **Datos especialmente protegidos** o de condenas /infracciones, a gran escala.
- Otros que puedan establecer las Agencias.

Novedades Reglamento Europeo

EVALUACIONES DE IMPACTO

¿CONTENIDO?

- Operaciones de **tratamiento** previstas y de los **fin**es del tratamiento.
- Evaluación de la **necesidad** y la **proporcionalidad** de las operaciones de tratamiento con respecto a su finalidad.
- Evaluación de los **riesgos** para los derechos y libertades de los interesados.
- **Medidas** previstas
- **Asesoramiento** del Delegado de Protección de Datos.
- Cuando proceda, opinión de los interesados o sus representantes.

EVALUACIONES DE IMPACTO

Si concluye que el tratamiento entraña **alto riesgo**,
que **no se puede minimizar** con las medidas adecuadas (tecnología + coste):



CONSULTAR a AGENCIA de PROTECCIÓN DE DATOS antes de iniciarlo.

EVALUACIONES DE IMPACTO



Novedades Reglamento Europeo

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

¿QUIÉN? El **Responsable**. Trasladable al Encargado

¿A QUIÉN? **A la Agencia** de Protección de Datos

¿CUÁNDO? Si se produce una **brecha de seguridad**

EXCEPCIÓN: Improbable que la incidencia suponga riesgo para derechos y libertades de las personas físicas.

¿EN CUÁNTO TIEMPO? Sin demora.
Como máximo, en 72 horas

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

¿QUIÉN? El **Responsable**. Trasladable al Encargado.

¿A QUIÉN? A los **interesados**

¿CUÁNDO? Si **brecha de seguridad supone un alto riesgo** para derechos y libertades de las personas físicas.

EXCEPCIÓN: medidas que minimicen el riesgo o suponga esfuerzo desproporcionado

¿EN CUÁNTO TIEMPO? En el menor tiempo posible.

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

¿QUIÉN? El Encargado

¿A QUIÉN? Al Responsable

¿CUÁNDO? Se produce brecha de seguridad. En todo caso, sin excepción.

¿EN CUÁNTO TIEMPO? Sin demora. (posible pactar tiempo y forma)

CODIGOS DE CONDUCTA Y CERTIFICACIONES

¿PARA QUÉ? Demostrar el cumplimiento de protección de datos y medidas de seguridad.

¿QUIÉN? Responsables
Encargados

¿OBLIGATORIO? NO
Salvo para Encargado, si acepta por contrato.

¿Qué pasa si no cumplimos?: Con LOPD

Nivel	Descripción de la infracción	Sanción
LEVE	1. No remitir a AEPD las notificaciones previstas en LOPD. 2. No solicitar inscripción de fichero en el RGPD 3. No informar, si datos proceden del interesado. 4. No tener contrato con encargado de tratamiento.	900 € – 40.000 €
GRAVE	1. Ficheros públicos, sin publicación en Boletín Oficial. 2. Recoger datos sin consentimiento expreso de los interesados, si es necesario. 3. Tratar datos personales incumpliendo el principio de calidad. 4. Vulnerar el deber de secreto. 5. Impedir ejercicio de derechos de acceso, rectificación, cancelación y oposición. 6. No informar, cuando datos no se recogen del interesado. 7. Otros deberes de notificación o requerimiento al interesado. 8. No cumplir las debidas medidas de seguridad. 9. No atender requerimientos o apercibimientos o peticiones de AEPD. 10. Obstruir la función inspectora. 11. Cesión de datos sin legitimación (puede llegar a ser muy grave)	40.001 € – 300.000 €
MUY GRAVE	1. Recoger datos de forma engañosa o fraudulenta. 2. Tratar datos de nivel alto sin las garantías añadidas sobre el consentimiento. 3. No cesar en tratamiento ilícito, tras requerimiento previo de AEPD. 4. Transferencias internacionales de datos incumpliendo la normativa.	300.001€ – 600.000 €

¿Qué pasa si no cumplimos?

REGIMEN SANCIONADOR

Se flexibiliza

Criterios de modulación para las multas:

- ✓ Intencionalidad
- ✓ Negligencia
- ✓ Medidas implementadas para paliar los posibles daños
- ✓ Cooperación
- ✓ Tipología de datos afectados

¿Qué pasa si no cumplimos?

REGIMEN SANCIONADOR

No límite inferior para las sanciones.

Límites máximos: obligatorio la de mayor cuantía:

- ✓ **10 Millones € o 2%** del volumen de negocio.
- ✓ **20 Millones € o 4%** del volumen de negocio.

AUTORIDADES DE PROTECCIÓN DE DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.aepd.es / Menores: www.tudecideseninternet.es

AGENCIA VASCA DE PROTECCIÓN DE DATOS

- Desde 2004

www.avpd.euskadi.eus / Menores: www.kontuzdatos.info

OTRAS AGENCIAS AUTONÓMICAS

- Agencia Catalana: año 2002 (www.apdcat.net)
- ~~Agencia de la Comunidad de Madrid: 2001 - 2012~~

Eskerrik asko etortzeagatik

Naiara Souto