Datuak Babesteko Euskal Bulegoa
Agencia Vasca de **Protección de Datos**

#RGPD y #LOPD
Principios y Conceptos
"Responsabilidad Proactiva"

Pedro Alberto González
Delegado de Protección de Datos
paGonzalez@avpd.eus

CONCEPTOS:

INTIMIDAD...
PRIVACIDAD...
PROTECCIÓN DE DATOS

La intimidad

- "*Derecho a que me dejen en paz*"
  - Warren & Brandeis, Harvard, 1890
- Delimitación de la intimidad:
  - Espacial (mis cuatro paredes)
  - Subjetivo (persona / personaje)
  - Objetivo (vida privada / pública)
- Regulación legal de la Intimidad:
  - Ley Orgánica 1/1982, de protección civil del derecho:
    - al honor,
    - a la intimidad personal y familiar
    - y a la propia imagen


HARVARD
LAW REVIEW.
THE RIGHT TO PRIVACY

La Privacidad

- *La **Intimidad:***
  - *"protege la esfera en que se desarrollan las facetas más **singularmente reservadas** de la vida de la persona*
    - *el domicilio donde realiza su vida cotidiana,*
    - *las comunicaciones en las que expresa sus sentimientos, … "*
- *La **Privacidad.***
  - *"constituye un conjunto, más amplio, más global, de **facetas de su personalidad***
    - *que, aisladamente consideradas, pueden carecer de significación*
    - *pero que, **coherentemente enlazadas** entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado."*

Exposición de motivos de la antigua LORTAD (1982)

Protección de Datos

Un Derecho de 4ªGeneración:

1. Derechos Civiles y Políticos
   - Vida, Libertad, dignidad, …
2. Derechos socioeconómicos y culturales
   - Educación, Salud, Trabajo, prot. Social, …
3. Derechos de solidaridad
   - Medio ambiente, consumo, …

4. "Ciberderechos"

La Protección de Datos: un *Derecho Fundamental*

- Art. 18.4 de la Constitución (1978):
  - *"La Ley limitará **el uso de la informática** para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio en su derecho"*
- Art. 1 de la Ley Orgánica 15/1999:
  - *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los **derechos fundamentales** de las personas físicas, y especialmente de su honor e intimidad personal y familiar"*

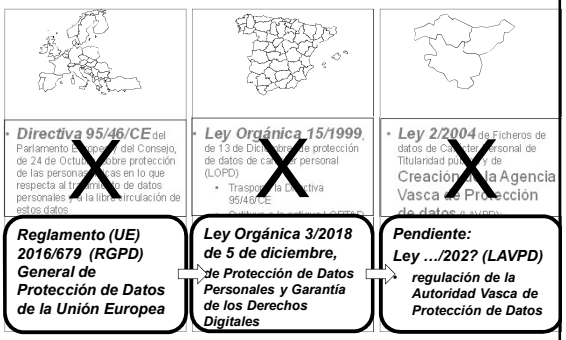
Protección de Datos: Derecho Fundamental *Europeo*

- Carta de los Derechos Fundamentales de la Unión Europea (2000)
  - Artículo 1: Dignidad humana
  - Artículo 2: Derecho a la vida
  - Artículo 3: Derecho a la integridad de la persona
  - Artículo 4: Prohibición de la tortura y de las penas o los tratos inhumanos o degradantes
  - Artículo 5: Prohibición de la esclavitud y del trabajo forzado
  - Artículo 6: Derecho a la libertad y a la seguridad
  - Artículo 7: Respeto de la vida privada y familiar
  - ***Artículo 8: Protección de datos de carácter personal***

Carta de los Derechos Fundamentales de la Unión Europea

- Artículo 8 - Protección de datos de carácter personal
  1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
  2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.
     Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
  3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Marco Legal de la P.D.



El #RGPD: Principios subyacentes

- Reglamento vs Directiva
- "Protección de las ***personas***"
  - Binomio derecho / deber
- "***Libre circulación*** de datos"
  - Intra-UE ("Tratamientos transfronterizos")
  - Extra-UE ("Transferencias internacionales")
- "Responsabilidad proactiva"
  - "Accountability"

#RGPD, Artículo 1

1.- (…)

*2.- El presente Reglamento protege los **derechos y libertades fundamentales de las personas** físicas y, en particular su derecho a la protección de los datos personales.*

#RGPD, Artículo 1

2.- (…)

*3..- La **libre circulación** de los datos personales en la Unión **no podrá ser restringida ni prohibida** por motivos relacionados con la protección (…) de datos personales.*

#RGPD: Ámbito de aplicación (Art. 2)

- Datos Personales de Personas Físicas…
  - No de personas jurídicas
  - No de personas fallecidas
  - No de personas anónimas
- Tratados por Personas Jurídicas
  - No por Personas Físicas (Tto. Doméstico)
    - Correspondencia personal,
    - Repertorio de direcciones,
    - Actividad en RRSS
  - …Salvo que exista oferta de bienes o servicios

Definiciones #RGPD (art. 4)

- ***Datos Personales***:
  - "toda información sobre …«el interesado»;
- ***Interesado*** *("data subject")*
  - "*Persona física identificada o identificable … cuyos datos personales (DP) se tratan*"
- ***Persona Identificable***:
  - 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 o
  - uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Definiciones #RGPD

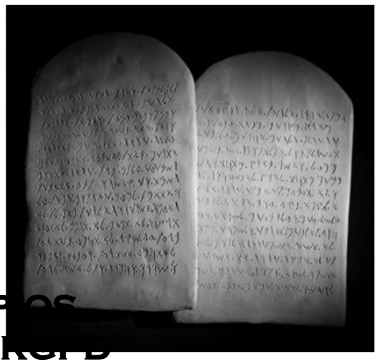
- ***Tratamiento*** *("processing"")*
  - *"Cualquier operación (o conjunto de operaciones) que se hace sobre DP como:*
    - Recogida, Registro, … Conservación
    - Modificación, Consulta, … Utilización
    - ***Comunicación*** ("*Disclosure*"), … ***Difusión***
    - Supresión, … Destrucción

Definiciones #RGPD

- Elaboración de perfiles:
  - *"Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales*
  - *para evaluar determinados aspectos personales de una persona física en particular para analizar o predecir aspectos relativos al*
    - *rendimiento profesional,*
    - *situación económica,*
    - *salud,*
    - *preferencias personales, intereses,*
    - *fiabilidad, comportamiento,*
    - *ubicación o movimientos*
  - *de dicha persona física"*

Definiciones #RGPD

- Seudonimización
  - "El tratamiento de datos personales de manera tal que
    - ya no puedan atribuirse a un interesado sin utilizar información adicional,
  - siempre que dicha información adicional
    - figure por separado y
    - esté sujeta a medidas técnicas y organizativas que eviten la reidentificación"
- Siguen siendo Datos Personales
  - Sirve para reducir riesgos
  - No para excluir la aplicación del RGPD



PRINCIPIOS EN EL #RGPD

Evolución de los Principios de la PD

- Directiva 95/46/CE
  - Los principios se mantienen (+/-)
- LOPD: Cambia la formulación
  - Corresponden con la "Calidad de los datos"
- Cambio más significativo:
  - Consentimiento
    - de "principio" a "supuesto legitimador"

principios #RGPD relativos al tratamiento

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad

Corolario: Responsabilidad proactiva

Art. 5 #RGPD

Art. 5.1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

Art. 6 - Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) …

A.- PRINCIPIO DE ... ...LICITUD....

...Licitud (o Legitimidad)...

Art. 6 #RGPD

- El tratamiento ***solo será lícito*** si se cumple al menos una de las siguientes condiciones:
  a) consentimiento
  b) contrato
  c) obligación legal;
  d) intereses vitales;
  e) interés público / ejercicio de poderes públicos
  f) interés legítimo (excepto Autoridades Públicas)

Supuestos de Legitimidad en base al interés del Interesado

Art. 6 #RGPD

- ***B) contrato***
  - *"el tratamiento es necesario para la ejecución de un contrato en el que el **interesado** es parte o para la aplicación a petición de este de medidas precontractuales";*

….

- ***D) intereses vitales;***
  - *"el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
  - *Fines humanitarios, emergencias, epidemias,…*
  - *Legitimación residual*

Supuestos de Legitimidad en base al interés del Responsable

Art. 6 #RGPD

- ***C) Obligación Legal***
  - *"el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento";*

….

- ***E) interés público / poderes públicos***
  - *"el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

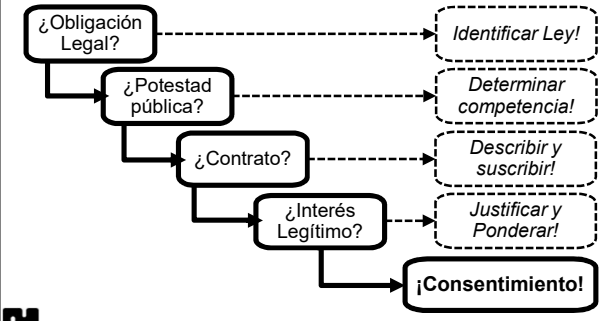
Legitimidad en base al interés legítimo del Responsable

Art. 6 #RGPD

….

- ***F) interés legítimo***
  - *"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 intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales,*
    - *en particular cuando el interesado sea un niño.*
- *Lo dispuesto anteriormente no será de aplicación al tratamiento realizado*
  - *por las autoridades públicas*
  - *en el ejercicio de sus funciones.*

El consentimiento, base de legitimación residual



Legitimidad en base al Consentimiento

Art. 6 #RGPD

- ***A) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;***
- ***DEF: «consentimiento del interesado»: …***
  - toda manifestación de voluntad
    - libre, específica, informada e inequívoca
  - por la que el interesado acepta,
    - ya sea mediante una declaración
    - o una clara acción afirmativa,
  - el tratamiento de datos personales que le conciernen

Condiciones para el Consentimiento

- Libre…
  - Puede denegarse sin perjuicio
  - No vinculado a otras prestaciones
  - Sin desequilibrio interesado / Responsable
- Específica…
  - Diferenciando operaciones de tratamiento
- Informada…
  - Identidad responsable y finalidad del tratamiento
- Inequívoca…
  - Responsable, ser capaz demostrarlo

Condiciones para el consentimiento

Art. 7 #RGPD

1. El responsable deberá ser capaz de demostrarlo
2. Consentimiento claramente distinguido de otros asuntos
   - Presentada de forma inteligible y accesible, con lenguaje claro y sencillo.
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento.
   - Su retirada no afecta a la licitud del tratamiento previo.
   - Antes de dar su consentimiento, el interesado será informado de ello.
   - Será tan fácil retirar el consentimiento como darlo.

Condiciones para el consentimiento

Art. 7 #RGPD

(…)

4. Al evaluar si se ha dado libremente, se tendrá en cuenta
   - si la ejecución de un contrato, o la prestación de un servicio, se supedita al consentimiento …
   - al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

El Consentimiento y su "Clara Acción Afirmativa"

- Declaración…
  - Por escrito, por medios electrónicos, incluso verbalmente
- Podría incluir…
  - marcar una casilla de un sitio web en internet,
  - escoger parámetros técnicos para la utilización de servicios
  - cualquier otra conducta que indique claramente que el interesado acepta el tratamiento de sus datos.
- Por tanto,…
  - el silencio,
  - las casillas ya marcadas
  - o la inacción

no deben constituir consentimiento.

El Consentimiento de los menores

- Oferta de Servicios realizada a niños:
  - El consentimiento es lícito si tiene 16 años.
  - Los Estados pueden establecer por ley una edad inferior a 16 años…
  - …siempre que esta no sea inferior a 13 años.
- ***El Proyecto de LOPD establece 13 años***
  - La actual LOPD contempla 14 años
  - Para menores de 13, requiere el del ***titular de la patria potestad o tutela***

Categorías especiales de datos

Art. 9 #RGPD

- Queda prohibido el tratamiento de los siguientes datos:
  - Origen étnico o racial
  - Opiniones políticas
  - Convicciones religiosas o filosóficas
  - Afiliación sindical
  - Datos de Salud
  - Vida sexual u orientaciones sexuales

  y además:
  - Datos genéticos
  - Datos biométricos
- salvo cuando concurran una serie de circunstancias

Otros datos protegidos

- Datos relativos a la condenas e infracciones penales
  - Sólo podrán ser tratados por las Autoridades Públicas
    - O cuando lo prevea el Derecho de la Unión o de los Estados Miembros
- No incluye las infracciones administrativas como datos con protección especial

Tratamiento de las Categorías Especiales de Datos

- Circunstancias que legitiman el tratamiento de las Categorías Especiales de datos:

(…)

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad

Corolario: Responsabilidad proactiva

Art. 5.1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

A.- PRINCIPIO … … DE LEALTAD… Y TRANSPARENCIA

Principio de "Lealtad"

- Principio "ético"
  - *"No defraudar las expectativas del interesado"*
- Debe quedar totalmente claro:
  - que se están recogiendo, utilizando, consultando, … sus datos personales,
  - así como la medida en que dichos datos son o serán tratados
- No puede informarse vaga o confusamente
  - Finalidad o finalidades ocultas
  - Consecuencias o comunicaciones posteriores

Principio de transparencia

- Obligación de informar: el principio de transparencia exige que
  - toda información y comunicación relativa al tratamiento de los datos sea fácilmente accesible y fácil de entender,
  - y que se utilice un lenguaje sencillo y claro."
- La obligación de informar
  - opera sin requerimiento previo y
  - su cumplimiento debe poder acreditarse

¿Qué cambia el RGPD sobre el deber de informar?

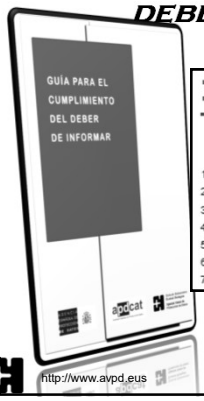
Antes (LOPD)

- La existencia del fichero, su finalidad y destinatarios.
- El carácter obligatorio o no de la respuesta, así como de sus consecuencias.
- La posibilidad de ejercitar los derechos ARCO.
- La identidad y datos de contacto del responsable del fichero/tratamiento.

Después (RGPD)

- Los datos de contacto DPD,
- La base jurídica del tratamiento,
- El Plazo de conservación,
- Decisiones automatizadas o elaboración de perfiles,
- Transferencias fuera UE
- El derecho a presentar una reclamación ante las APDs

Guía (directrices) sobre el *deber de informar*



Indice

¿Cómo y Dónde informar?

- Con un lenguaje ***claro*** y ***sencillo***,
- De forma ***concisa, transparente, inteligible y de fácil acceso***.
- Consecuencia: Condiciones del medio
  - En el ***mismo momento*** de la recogida
    - Formularios en papel, -- Entrevista telefónica
    - Formularios Web, -- Aplicaciones móviles
    - Sensores de actividad -- Sensores de entorno
  - En algún ***momento posterior***:
    - Correo postal
    - Mensajería electrónica e instantánea
    - Notificaciones emergentes en servicios y aplicaciones

La respuesta: Información por capas

- Información ***multinivel*** consistente en:
  - presentar ***información básica*** en un 1er nivel,
    - de forma ***resumida***,
    - en el mismo momento y
    - en el mismo medio de recogida,
  - remitir a ***información adicional*** en un 2º nivel,
    - de forma ***detallada***,
    - en un medio más adecuado para su presentación, comprensión y archivo.

Información agrupada en 5 +1 Epígrafes

1. ***"Responsable"*** (del tratamiento)
2. ***"Finalidad"*** (del tratamiento)
3. ***"Legitimación"*** (del tratamiento)
4. ***"Destinatarios"***(de cesiones o transferenc.)
5. ***"Derechos"***(de las personas interesadas)

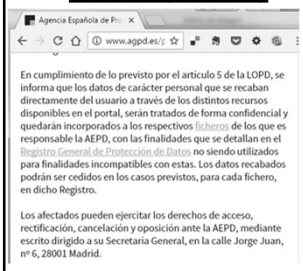
+1"Procedencia"(de los datos)

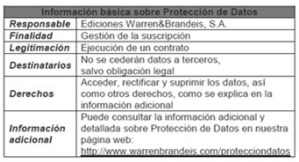
Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable"	Identidad del Responsable del Tratamiento	Datos de contacto del **Responsable**
		Identidad y datos de contacto del **representante**
		Datos de contacto del **Delegado** de Protección de Datos
"Finalidad"	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción **ampliada de los fines** del tratamiento
		Plazos o **criterios de conservación** de los datos
		Decisiones **automatizadas, perfiles** y lógica aplicada
"Legitimación"	Base jurídica del tratamiento	Detalle de la **base jurídica**, en casos de **obligación legal, interés público o interés legítimo**.
		Obligación o no de facilitar datos y **consecuencias** de no hacerlo

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Destinatarios"	Previsión o no de Cesiones	Destinatarios o **categorías** de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de **adecuación**, **garantías**, **normas corporativas vinculantes** o situaciones específicas aplicables
"Derechos")	Referencia al ejercicio de derechos.	Cómo ejercer los **derechos** de acceso, rectificación, supresión y **portabilidad** de sus datos, y la **limitación u oposición** a su tratamiento
		Derecho a **retirar el consentimiento**
		Derecho a **reclamar ante la Autoridad** de Control
"Procedencia"	Fuente de los datos (cuando no proceden del interesado)	Información detallada del **origen de los datos**, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

¿Qué cambia el RGPD sobre el deber de informar?

Antes (LOPD) **Después (RGPD)**


Agencia Española de Pro
www.agpd.es/p
En cumplimiento de lo previsto por el artículo 5 de la LOPD, se informa que los datos de carácter personal que se recaban directamente del usuario a través de los distintos recursos disponibles en el portal, serán tratados de forma confidencial y quedarán incorporados a los respectivos ficheros de los que es responsable la AEPD, con las finalidades que se detallan en el Registro General de Protección de Datos no siendo utilizados para finalidades incompatibles con estas. Los datos recabados podrán ser cedidos en los casos previstos, para cada fichero, en dicho Registro.
Los afectados pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición ante la AEPD, mediante escrito dirigido a su Secretaría General, en la calle Jorge Juan, nº 6, 28001 Madrid.



Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A.
Finalidad	Gestión de la suscripción
Legitimación	Ejecución de un contrato
Destinatarios	No se cederán datos a terceros, salvo obligación legal
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos

¿Qué medios son adecuados para la información adicional?

- **En papel:**
  - En el mismo formulario cumplimentado (por ejemplo, en el reverso)
  - Como un anexo que se entregue al interesado y que pueda conservar
  - Como información expuesta, en carteles, paneles, trípticos, etc, de los cuales se pueda solicitar una copia manejable para conservar.
- **Inf. electrónica**
  - En una página web específica, accesible desde un hipervínculo
  - Como un documento disponible para su descarga desde una URL
  - Como información adjunta a un mensaje electrónico
- **Inf. telefónica:**
  - Como una locución, ofertada como complemento o alternativa a una oferta de disponibilidad de información adicional accesible electrónicamente o remitida, por correo postal o electrónico.

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad
Corolario: Responsabilidad proactiva

Art. 5.1. Los datos personales serán:
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (…) («limitación de la finalidad»);

B.- PRINCIPIO DE LIMITACIÓN DE LA FINALIDAD

Principio de Limitación de la finalidad

- Los datos personales serán recogidos con fines
  - ***determinados,*** [concretos]
  - ***explícitos y*** [finalidad]
  - ***legítimos,*** [lícitos]
- y no serán tratados ulteriormente de manera ***incompatible*** con dichos fines;
  - el tratamiento ulterior de los datos personales con
    - fines de archivo en interés público,
    - fines de investigación científica e histórica o
    - fines estadísticos
  - no se considerará incompatible con los fines iniciales

La Finalidad ha de ser determinada y explícita

- *"¡Una linterna para tu dispositivo!*
  - *"Una aplicación de linterna increíblemente simple y, a su vez, muy útil."*
  - *Podrás utilizar el flash de la cámara de tu dispositivo a modo de linterna"*
- *"Sus datos serán tratados para mejorar su experiencia de usuario"*

El "Test de Compatibilidad"

Art. 6.- Licitud del tratamiento

(…) 4.- Cuando el tratamiento para otro fin distinto (…) no esté basado

- en el consentimiento del interesado o
- en el Derecho de la Unión (…),

el responsable del tratamiento, (…), tendrá en cuenta, entre otras:

a) la relación entre los fines [inicial y ulterior];
b) el contexto y (…) la relación entre los interesados y el responsable;
c) la naturaleza de los datos, en concreto cuando se traten
  - categorías especiales, o
  - datos relativos a condenas e infracciones penales;

d) las consecuencias para los interesados del tratamiento ulterior;
e) la existencia de garantías, como cifrado o seudonimización.

Reutilización de datos

- No se prohíben:
  - Tratamientos adicionales (misma finalidad)
  - Otras finalidades no-Incompatibles
- Necesidad de información al interesado:
  - *"Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente"*

Garantías y excepciones aplicables a determinados "tratamientos Compatibles"

- Artículo 89.- Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos
  - 1. El tratamiento con
    - fines de archivo en interés público,
    - fines de investigación científica o histórica o
    - fines estadísticos
  - estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados.
  - Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales.
  - Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines.
  - Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

Garantías y excepciones aplicables a determinados "tratamientos Compatibles"

- (…)
- 2 .- Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos
  - 15 (Acceso)
  - 16 (Rectificación)
  - 18 (Limitación de tratamiento)
  - 19 (notificación de rectificación, …)
  - 20 (Portabilidad)
  - y 21 (Oposición)
- sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines (…) y cuanto esas excepciones sean necesarias para alcanzar esos fines.

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad
Corolario: Responsabilidad proactiva

Art. 5.1. Los datos personales serán:

c)adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

C.- PRINCIPIO DE PERTINENCIA Y MINIMIZACIÓN DE DATOS

"MINIMIZACIÓN DE DATOS"

- *Los datos personales serán:*
  - adecuados,
  - pertinentes y
  - limitados a lo necesario en relación con los fines
- Cambio respecto de la Directiva:
  - Directiva: "no excesivos"
  - RGPD: "limitados a lo necesario"
  - Matiz que refuerza el contenido del principio.
  - Frecuente fuente de infracciones en lo sanitario
- Recomendable aplicar "desde el diseño"

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad
Corolario: Responsabilidad proactiva

Art. 5.1. Los datos personales serán:

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan

D.- PRINCIPIO DE EXACTITUD Y VIGENCIA

Exactitud y vigencia

- Origen de derechos del interesado
  - Exactitud ➔ Derecho de rectificación
  - Vigencia ➔ Derecho de supresión
- Obligación de diligencia del responsable
  - Afecta a decisiones, derechos e intereses
    - (HC, perfiles, registros administrativos,…)

Previsión en el Proyecto de LOPD

- Art.4 pLOPD:
- *No será imputable al responsable la inexactitud en los casos:*
  - Datos facilitados por el interesado
  - Facilitados por un "intermediario sectorial"
  - Consecuencia del "derecho a la portabilidad"

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad
Corolario: Responsabilidad proactiva

Art. 5.1. Los datos personales serán:

e)mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; (…)

E.- PRINCIPIO DE LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

"MINIMIZACIÓN TEMPORAL"

- "Mantenidos de forma que
  - se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales;
  - los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con
    - fines de archivo en interés público,
    - fines de investigación científica o histórica
    - o fines estadísticos,
  - sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas a fin de proteger los derechos y libertades del interesado

EXCEPCIONES A LA SUPRESIÓN

- Art. 17.3 [La supresión] no se aplicarán cuando el tratamiento sea necesario:
  - a) para ejercer el derecho a la libertad de expresión e información;
  - b) para el cumplimiento de
    - una obligación legal (…) que se aplique al responsable del tratamiento, o
    - una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
  - c) por razones de interés público en el ámbito de la salud pública (…);
  - d) con fines de
    - archivo en interés público,
    - investigación científica o histórica o
    - fines estadísticos,
  - en la medida en que [la supresión] pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento,
  - e) para la formulación, el ejercicio o la defensa de reclamaciones.

PREVISIÓN EN EL PROYECTO DE LOPD (BLOQUEO)

- Art.32 pLOPD – Bloqueo de los datos:
  - 1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.
  - 2. Los datos bloqueados quedarán a disposición exclusiva de
    - los jueces y tribunales,
    - el Ministerio Fiscal o
    - las Administraciones Públicas competentes,
    - en particular de las autoridades de protección de datos,
  - para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.
  - 3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
  - (…)

¿CUÁL ES EL PLAZO DE CONSERVACIÓN CORRECTO?

- Buena pregunta…
  - Caso por caso, según su regulación sectorial
    - Ley Autonomía del Paciente
    - Leyes 39-40/2015
    - …
  - Responsabilidad derivada del tratamiento
    - Prescripción/Caducidad de las acciones
    - Obligaciones derivadas de contratos
  - Excelente compilación de Alfonso Pacheco en http://www.privacidadlogica.es/ Privacidad Lógica

A. LICITUD, LEALTAD Y TRANSPARENCIA
B. LIMITACIÓN DE LA FINALIDAD
C. PERTINENCIA Y MINIMIZACIÓN DE DATOS
D. EXACTITUD Y VIGENCIA
E. LIMITACIÓN DEL PLAZO DE CONSERVACIÓN
F. INTEGRIDAD Y CONFIDENCIALIDAD
COROLARIO: RESPONSABILIDAD PROACTIVA

Art. 5.1. Los datos personales serán:

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, (…)

F.- PRINCIPIO DE INTEGRIDAD Y CONFIDENCIALIDAD

INTEGRIDAD Y CONFIDENCIALIDAD

- *Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales,*
  - *incluida la protección contra el tratamiento no autorizado o ilícito*
  - *y contra su pérdida, destrucción o daño accidental,*
- *mediante la aplicación de medidas técnicas u organizativas apropiadas*

Se concreta en las Medidas de Seguridad

Art. 32 – Seguridad del Tratamiento

1. Teniendo en cuenta (…) aplicarán ***medidas*** (…) ***seguridad adecuada al riesgo***, que incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar

- confidencialidad,
- integridad,
- disponibilidad y
- resiliencia

permanentes de los sistemas y servicios de tratamiento;

c) (…)

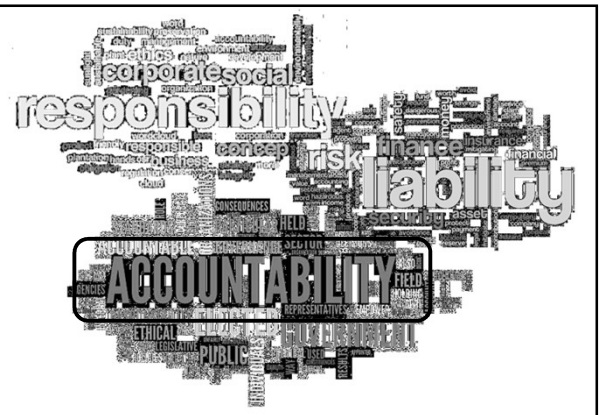
principios #RGPD s al tratamiento

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad

Art. 5 #RGPD

Corolario:

Responsabilidad Proactiva



"Responsabilidad proActiva" = "Rendición de Cuentas"

"Responsabilidad proActiva"

"Art. 5.2- *El responsable del tratamiento será…*

–***Responsable de Cumplir***

–***y Capaz de demostrar***

que trata los datos de acuerdo con los principios de:

A. Licitud, lealtad y transparencia
B. Limitación de la finalidad
C. Pertinencia y Minimización de datos
D. Exactitud y vigencia
E. Limitación del plazo de conservación
F. Integridad y confidencialidad

Art. 5 #RGPD

Cambio de "esquema mental"

"Cumplimiento pasivo"

- Declarar los ficheros en el Registro…
- Incluir una "clausula LOPD"…
- Copiar un "documento de seguridad"…
- ¿Problemas?
  - (…salir del paso…)
  - Reaccionar a posteriori

"Responsabilidad proActiva"

- Aplicar la Privacidad desde el diseño (y por defecto)
- Llevar un registro interno de actividades de tratamientos
- Seguridad basada en Gestión de Riesgos
- Efectuar Evaluaciones de Impacto sobre la privacidad
- Adoptar Códigos de Conducta y Certificaciones
- Disponer de un Delegado de Protección de Datos

"*Quién-es-quién*" en la Responsabilidad proActiva

- Responsable ("*controller*")
  - del tratamiento (RT)
- Encargado ("*processor*")
  - (o subencargado) del tto. (ET)
- Delegado/a
  - de protección de datos (DPD) ("officer")
- (+ Autoridades de Control)

Responsables de tratamientos

«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"

«Responsable del tratamiento»:

- Establecido en varios estados miembros
  - (con un "Establecimiento Principal")
- Establecidos fuera de la UE
  - (con designación de Representante)
- Posibilidad de "Co-Responsables"
- Ya no se habla de "Ficheros",
  - sino de "Tratamientos"

Obligaciones del Responsable

Art. 24.1 #RGPD

- "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, …

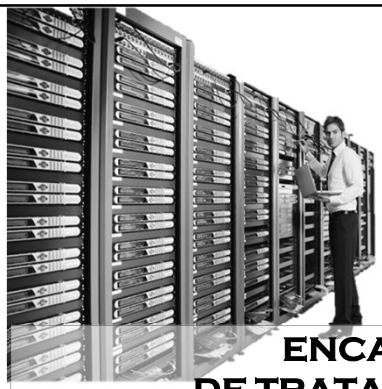
Obligaciones del Responsable

Art. 24.1 #RGPD

- …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."



ENCARGADOS DE TRATAMIENTOS

«ENCARGADO DEL TRATAMIENTO» O «ENCARGADO»

- "Persona …
  - física o jurídica,
  - autoridad pública,
  - servicio u otro organismo,
- que trate datos personales
- …por cuenta del responsable "

«ENCARGADO DEL TRATAMIENTO» O «ENCARGADO»

- La mayor parte de las obligaciones son para ambos,
  - Responsable
  - Encargado
- Exigencia de garantías
  - técnicas
  - organizativas
- Permitidos los sub-Encargos,
  - con autorización del Responsable

RESPONSABILIDAD RESPECTO DEL ENCARGADO DEL TRATAMIENTO

- Se exige **deber de diligencia** por parte del Responsable en su elección
- El Encargado del tratamiento debe ofrecer **garantías** suficientes
  - respecto a la implantación y el mantenimiento
  - de las **medidas técnicas y organizativas** apropiadas,
  - de acuerdo con lo establecido en el RGPD.

GARANTÍAS DEL ENCARGADO DEL TRATAMIENTO

- Para **demostrar** que el encargado ofrece garantías suficientes, el RGPD prevé
  - la adhesión a **códigos de conducta** o
  - la posesión de un **certificado** de protección de datos

pueden servir como mecanismos de prueba.

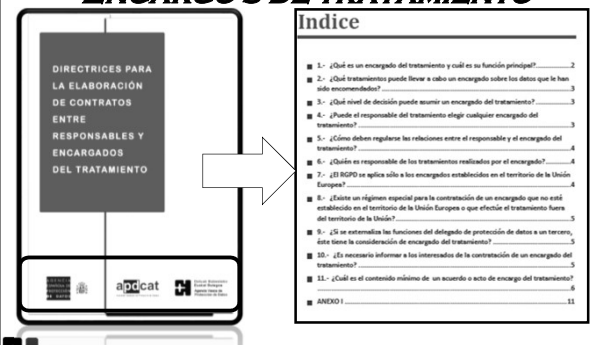
EXIGENCIA DE CONTRATO O "ACTO JURÍDICO" VINCULANTE

- Constancia por escrito / electrónico
- Tratamiento bajo instrucciones documentadas del Responsable
- Garantía y compromiso de confidencialidad
- Especificación de medidas de seguridad
- Condiciones de subEncargo
- Devolución o Destrucción de datos
- Realización de auditorías e inspecciones

Directrices de las APDs (AEPD + APDCAT + AVPD)

- Las tres Agencias de Protección de Datos han elaborado una "guía" con directrices sobre el Contrato de Encargo de Tratamientos.
- Disponible en:
  - http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/

Guía (directrices) sobre los *Encargos de tratamiento*



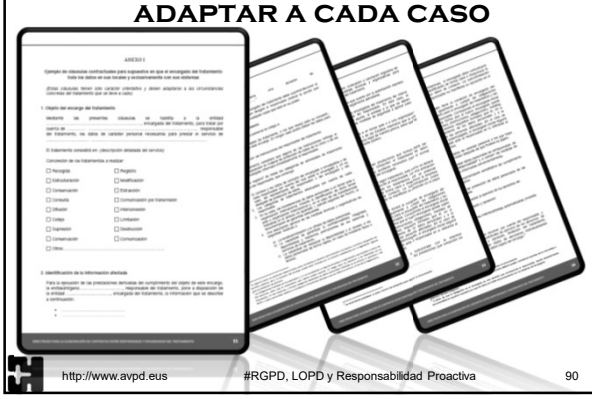
¿Cuál es el contenido mínimo de un encargo de tratamiento?

- Como mínimo debe establecerse:
  - el **objeto** y la **duración**,
  - la **naturaleza** y la **finalidad** del tratamiento,
  - el **tipo de datos** personales y categorías de **interesados**, y
  - las obligaciones y derechos del **Responsable**
  - las obligaciones y derechos del **Encargado**

¿Qué obligaciones del Encargado deben quedar recogidas

- A.- Las **instrucciones** del responsable del tratamiento
- B.- El deber de **confidencialidad**
- C.- Las medidas de **seguridad**
- D.- El régimen de la **subcontratación**
- E.- Los **derechos** de los **interesados**
- F.- La **colaboración** en el cumplimiento de las obligaciones del responsable
- G.- El **destino** de los datos al **finalizar** la prestación
- H.- La colaboración con el responsable para **demostrar** el cumplimiento

Modelos con opciones para adaptar a cada caso



¿Puede contratarse con encargados no establecidos en la UE?

- Tiene base legal en el propio contrato
- Si no está establecido en la UE, es una Transferencia Internacional, sujeta a :
  - Decisiones de **adecuación**,
  - Existencia de **garantías adecuadas**, en particular:
    - Normas **corporativas vinculantes**
    - **Clausulas tipo** de PD
    - Códigos de Conducta
    - Mecanismos de certificación

Los Delegados de Protección de Datos

- Necesario siempre que los Tratamientos:
  - Se lleven a cabo por Autoridades u Organismos Públicos
  - Requieran una observación habitual y sistemática de interesados a gran escala
  - Traten a gran escala de datos personales de categorías especiales o relativos a condenas e infracciones penales
- Puede ser único para:
  - Grupos Empresariales
  - Autoridades u Organismos Públicos
  - Asociaciones u Organismos representativos

Algunos "Conceptos (mas o menos) indeterminados"

- **"Gran Escala"**
- **"Ocasional" / "Regular" / "Sistemático"**
- **"Alto Riesgo" / "Riesgo improbable"**

  – **Reciente documento del art29WP aclarando el papel del DPO (dic-2016 – rev. Abr-2017)**
  - **"Guidelines on Data Protection Officers"**
  - **http://ec.europa.eu/newsroom/document.cfm?doc_id=44100**

"Gran Escala"

Art29WP-wp243

- El número de interesados involucrados,
  – bien como cifra concreta o
  – como proporción de la población
- El volumen de datos
  – o el abanico de diferentes conceptos de datos que se procesan
- La duración, o permanencia, de la actividad de tratamiento de datos
- El alcance geográfico de la actividad de tratamiento

"Regular y Sistemático"

Art29WP-wp243

- Continuado, recurrente o periódico
- Que se produce de acuerdo con un sistema
- Preestablecido, organizado o metódico
- Que tiene lugar como parte de un plan general de recogida de datos
- Llevado a cabo como parte de una estrategia

Funciones del DPD

Art.39 #RGPD

- a) informar y asesorar al responsable o encargado;
- b) supervisar el cumplimiento legal y de las políticas del responsable o del encargado, incluidas:
  – la asignación de responsabilidades,
  – la concienciación y formación del personal
  – las auditorías correspondientes;
- c) ofrecer el asesoramiento acerca de las evaluaciones de impacto y supervisar su aplicación;
- d) cooperar con la autoridad de control;
- e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

Cualificación y Posición

Art.38 #RGPD

- Conocimientos especializados del derecho y la Práctica de la PD
- Puede ser empleado o servicio externo
- Independiente. Inviolable. No exclusivo
- Reporta al más alto nivel jerárquico
- Datos de contacto publicados y notificados a ACPD

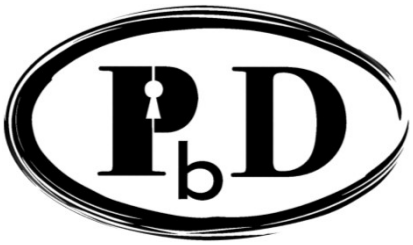
¿Puede designarse un DPD voluntariamente?

- Sí.
- Si se designa DPD es con todas sus consecuencias (derechos y obligaciones)
- Puede contarse con otro "personal encargado de Protección de datos"
  - Pero entonces NO puede denominarse DPD

Volviendo a la "Responsabilidad ProActiva"...

Elementos que forman la "Responsabilidad proActiva"

1. Privacidad desde el diseño y por defecto
   - (PbD)
2. Registro de actividades de tratamiento
   - (interno)
3. Seguridad basada en Gestión de Riesgos
   - (RA / RM)
4. Evaluación de Impacto sobre la Privacidad
   - (EIPD / PIA)
5. Códigos de Conducta, certificaciones y sellos
   - (CdC)



PRIVACIDAD DESDE EL DISEÑO (Y POR DEFECTO)

Protección de datos desde el diseño ...

Art.25.1 #RGPD9

"Art. 25.1.- El responsable del tratamiento aplicará,

- tanto en el momento de determinar los medios de tratamiento
- como en el momento del propio tratamiento,

medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección de datos, como

- la seudonimización,
- la minimización de datos,

e integrar las garantías necesarias en el tratamiento.

...y por defecto

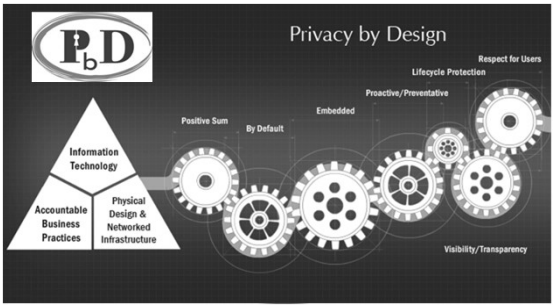
Art.25.2 #RGPD

(…)

Art. 25.2.- El responsable del tratamiento implementará mecanismos con miras a garantizar que,

- por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento
- y, especialmente, que no se recojan ni conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación.
- En concreto, estos mecanismos garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas.

La privacidad, desde el diseño (y por defecto)



7 Principios fundamentales de la "Privacy by Design"

1. Diseño Proactivo, no Reactivo;
   - Preventivo, no Correctivo
2. Privacidad como configuración por defecto
3. Privacidad incrustada en el diseño
4. Funcionalidad total:
   - "Suma-Positiva", no "Suma-Zero"
5. Seguridad en todo el ciclo de vida ("end-to-end")
6. Visibilidad y transparencia – "Keep it Open"
7. Respeto a la privacidad personal ("User-centric")

Directrices ENISA Protección por Diseño y defecto

- Estrategias:
  - #Minimizar
  - #Ocultar
  - #Separar
  - #Agregar
  - #Informar
  - #Autocontrol
  - #Cumplir
  - #Demostrar

- Técnicas:
  - Autenticación
  - Credenciales
  - Comunicac. Seguras
  - Anonim./Pseudonim.
  - Base de Datos
  - Estadísticas/reident.
  - Minería de datos
  - Recuperación
  - Almacenamiento
  - Computación
  - Transparencia
  - Intervención

Estrategias de diseño orientadas a DATOS

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
Estrategias orientadas a datos	Minimizar	Limitar al máximo posible el tratamiento de datos personales. TÁCTICAS: **seleccionar, excluir, podar** y **eliminar**	Anonimización Seudonimización Bloqueo de correlación en sistemas de gestión de identidad federada
	Ocultar	Evitar que los datos personales se hagan públicos o sean conocidos. TÁCTICAS: **restringir, ofuscar, disociar** y **agregar**)	Cifrado Redes de mezcla Atributos basados en credenciales
	Separar	Mantener separados los conjuntos de datos personales. TÁCTICAS: **aislar** y **distribuir**	Listas negras anónimas Cifrado homomórfico Separación física y lógica
	Abstraer	Limitar al máximo el nivel de detalle utilizado en los tratamientos de datos personales. TÁCTICAS: **sumarizar, agrupar** y **perturbar**	Agregación en el tiempo K-anonimidad Ofuscación de medidas mediante agregación de ruido Granularidad dinámica de ubicación Privacidad diferencial

Estrategias de diseño orientadas a PROCESOS

ESTRATEGIA DE DISEÑO DE LA PRIVACIDAD		DESCRIPCIÓN Y TÁCTICAS	CONTROLES Y PATRONES DE DISEÑO
Estrategias orientadas a procesos	Informar	Mantener informados a los sujetos de datos de la naturaleza y condiciones del tratamiento. TÁCTICAS: **facilitar, explicar** y **notificar**	Notificación de brechas de privacidad Visualización dinámica de la política de privacidad Iconos de privacidad Alertas de tratamiento
	Controlar	Proporcionar a los sujetos de datos un control efectivo sobre sus datos personales. TÁCTICAS: **consentir, alertar, elegir, actualizar, retirar**	Paneles de preferencias de privacidad Transmisión activa de presencia Selección de credenciales Consentimiento informado
	Cumplir	Respetar e impulsar el cumplimiento de las obligaciones impuestas en la normativa vigente y en la propia política de protección de datos. TÁCTICAS: **definir, mantener, defender**	Evaluación de impacto de privacidad en soluciones de gestión de identidad federada Control de acceso Gestión de obligaciones Políticas adheridas
	Demostrar	Poder demostrar que los tratamientos se realizan de una forma respetuosa con la privacidad. TÁCTICAS: **registrar, auditar** e **informar**	Auditoría Registro

REGISTRO (INTERNO) DE TRATAMIENTOS

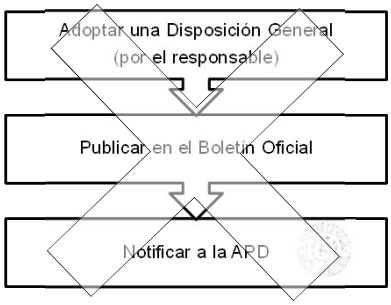
Registro (interno) de Tratamientos

el anterior Registro de Ficheros... ¡¡¡ Desaparece !!!

Hasta ahora, ¿qué eran los Registros de Ficheros?

- Órgano previsto en la LOPD para garantizar la publicidad de la existencia de ficheros (art. 39)
- Registro de ficheros de la ***AEPD***:
  - Ficheros de titularidad privada
  - Ficheros de titularidad pública de
    - Órganos Constitucionales
    - AGE (Administración General del Estado)
    - EELL y CCAA sin APD
- Registro de ficheros de la ***AVPD***:
  - Ficheros de titularidad pública de Euskadi

Regulación en el ámbito público



El (nuevo) registro (interno) de Actividades de tratamientos

- Se mantiene la necesidad de llevanza de un registro (interno) de las actividades de tratamiento
  - Por el Responsable
  - Por el Encargado
- Para las organizaciones:
  - Que empleen más de 250 personas, o bien:
  - Que el tratamiento entrañe riesgos para los interesados,
  - no sea ocasional
  - o incluya categorías especiales o relativos a condenas e infracciones penales.
- Dicho Registro interno estará a disposición de las Autoridades de Control

SEGURIDAD BASADA EN GESTIÓN DE RIESGOS

HASTA AHORA: RD-1720/2007


BOE
LEGISLACIÓN CONSOLIDADA

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.

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Referencia: BOE-A-2008-979

TEXTO CONSOLIDADO
Última modificación: 8 de marzo de 2012

ESTRUCTURA DEL RD 1720/2007

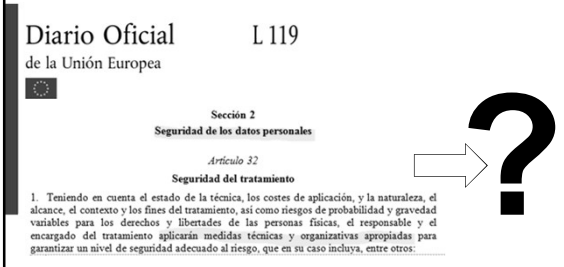
- Clasificación de la Información
  - Criterios de exigencia de los niveles de seguridad
- Requisitos de documentación
  - Estructura y contenido del "Documento de Seguridad"
- Relación de "Puntos de control"
  - Medidas de seguridad, diferenciadas para cada uno de los niveles exigibles

NIVELES DE SEGURIDAD

10 PUNTOS DE CONTROL EN MEDIDAS DE SEGURIDAD

1. ORGANIZACIÓN DE LA SEGURIDAD
2. DOCUMENTACIÓN DE SEGURIDAD
3. FUNCIONES Y OBLIGACIONES DEL PERSONAL
4. IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS
5. CONTROLES Y REGISTROS DE ACCESOS
6. ACCESOS A TRAVÉS DE REDES / INTERNET
7. SOPORTES Y DOCUMENTOS CON INFORMACIÓN
8. COPIAS DE RESPALDO Y RECUPERACIÓN
9. GESTIONAR INCIDENCIAS DE SEGURIDAD
10. EFECTUAR AUDITORÍAS Y CONTROLES

MARCO #RGPD SEGURIDAD DEL TRATAMIENTO:


Diario Oficial L 119
de la Unión Europea

Sección 2
Seguridad de los datos personales

Artículo 32

Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

Enfoque completamente distinto del RD-1720/2007

Marco #RGPD
Seguridad del Tratamiento

- Art. 32 #RGPD:
  "1.- Teniendo en cuenta:
  - el estado de la técnica,
  - los costes de aplicación, y
  - la naturaleza, el alcance, el contexto y los fines del tratamiento, así como
  - riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas,

  "el responsable y el encargado del tratamiento aplicarán:
  - medidas técnicas y organizativas apropiadas
  - para garantizar un nivel de seguridad
  - adecuado al riesgo"
- Orientación hacia "evaluación y gestión de riesgos"

Marco #RGPD
Seguridad del Tratamiento

1. (…) el responsable y el encargado (…) aplicarán ***medidas*** de ***seguridad adecuada al riesgo***, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia (…);

c)la capacidad de restaurar la disponibilidad de los datos de forma rápida en caso de incidente;

d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas.

Seguridad del Tratamiento (cont.)

2. (…) se tendrán en cuenta los ***riesgos***, en particular como consecuencia de
- la ***destrucción, pérdida o alteración*** accidental o ilícita de datos personales,
- o la comunicación o ***acceso no autorizados*** .

3. (…).

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona
- que actúe bajo la autoridad del responsable o del encargado
- y tenga acceso a datos personales
- solo pueda tratar dichos datos siguiendo instrucciones del responsable,
- salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Seguridad del Tratamiento (cont.)

2. (…).

3. La adhesión a un código de conducta (…) o a un mecanismo de certificación (…) podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el (…) presente artículo.

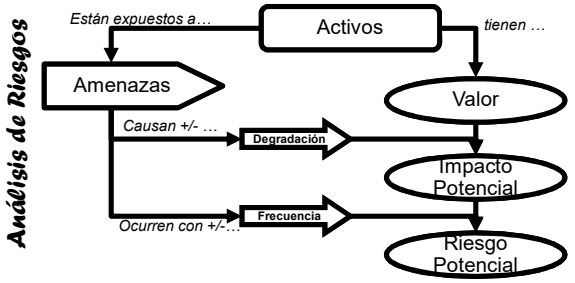
4. (…).

APROXIMACIÓN INTUITIVA A LA GESTIÓN DE RIESGOS

Algunas Definiciones

- **Activo ("Fuente de riesgo"):**
  - "*Cualquier cosa que tenga algún valor para alguien*"
  - "*Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección*"
  - Los activos pueden presentar **Vulnerabilidades**
- **Amenaza ("Suceso"):**
  - "*Evento que puede desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales (degradación) en sus activos*"
  - Las amenazas ocurren con una cierta **probabilidad**

Marco de Referencia para análisis de Riesgos

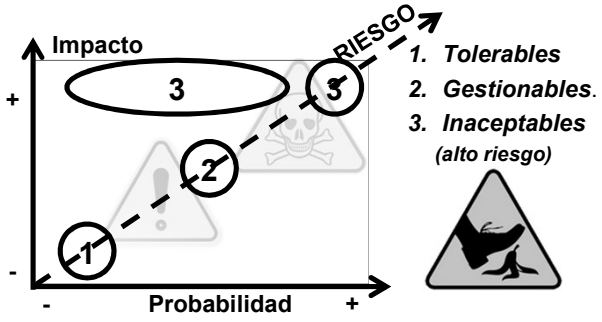


Más Definiciones

- **Impacto** (potencial)
  - "*Consecuencia que sobre un activo tiene la materialización de una amenaza*"
- **Riesgo** (potencial, inherente, intrínseco)
  - "*Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización*"

Riesgo = Impacto X Probabilidad

Valoración de los riesgos

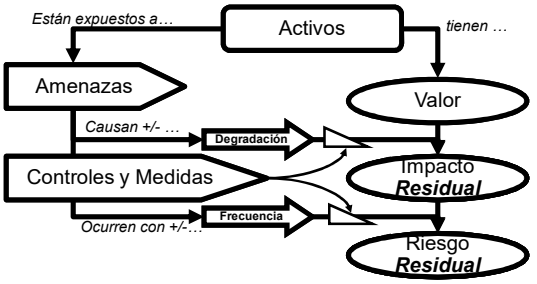


1. ***Tolerables***
2. ***Gestionables***.
3. ***Inaceptables***
   (alto riesgo)

Más Definiciones

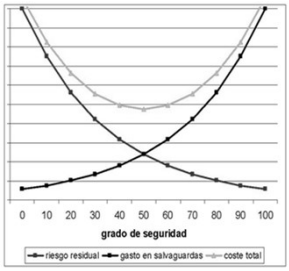
- **Controles y medidas** *(Salvaguardas)*
  - "*Procedimiento o mecanismo tecnológico que reduce el riesgo.*"
- **Riesgo Residual**
  - "*Riesgo remanente tras la aplicación de las salvaguardas (controles y medidas) previstas*"

Marco de Referencia para tratamiento de Riesgos



Tratamiento de los riesgos

- ***Modificar el riesgo***,
  - ya sea mitigando el impacto
  - o evitando la oportunidad de la amenaza.
- ***Transferir el riesgo***
  - no la responsabilidad.
- ***Aceptar el riesgo***,
  - riesgos aceptables, o por debajo del umbral de riesgo asumible.
- ***Evitar el riesgo***,
  - riesgos inaceptables,
  - renunciando a algunas actividades o tratamientos.



Activos más comunes

- Instalaciones
  - Edificios, locales, canalizaciones, redes de comunicaciones,…
- Equipamientos
  - Mobiliario, maquinaria, ordenadores personales, …
- Sistemas de Información
  - Servidores, sistemas de almacenamiento,…
  - Aplicaciones y programas de ordenador
  - Información, datos de negocio, datos personales

Activos más comunes

- Intangibles
  - Licencias, derechos,..
  - Reputación, imagen, …
  - Personas de la Organización
- Servicios prestados
  - Continuidad del negocio

Activos en Protección de Datos

- Datos de Carácter Personal
- y, como consecuencia,
  - Instalaciones donde se ubican,
  - Equipos donde se tratan
  - Redes por donde “viajan”
  - Programas que los tratan
  - Soportes que los contienen
  - Personas que los gestionan

Amenazas más comunes

- Desastres naturales
  - Fuego, agua, … terremotos, …
- Desastres industriales
  - Explosiones, derrumbes, fallo de equipos,
- Interrupciones de servicios
  - Luz, agua, teléfono, internet, …
- Errores humanos no intencionados
  - De usuarios, de administradores, de operadores,
- Ataques intencionados
  - Contra personas, equipos, programas,
  - Posibles empleados desleales

Dimensiones de la seguridad de la Información

- Confidencialidad
  - Acceso o revelación indebidos
- Integridad
  - Modificación de los datos
- Disponibilidad
  - Sabotaje
- + Resiliencia
  - Capacidad de recuperación
- (Autenticidad)
  - Suplantación de Identidad

Medidas previstas en el #RGPD:

a) la seudonimización y el cifrado;

b) la confidencialidad, integridad y disponibilidad

c) la resiliencia y restauración de la disponibilidad;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia.

¿Resiliencia?

- **Seres vivos:**
  - *Capacidad de **adaptación** frente a un agente perturbador o un estado o situación adversos*
- **Materiales, mecanismos o sistemas:**
  - *Capacidad para **recuperar** su estado inicial, cuando ha cesado la perturbación a la que había estado sometido*

Nuevos conceptos

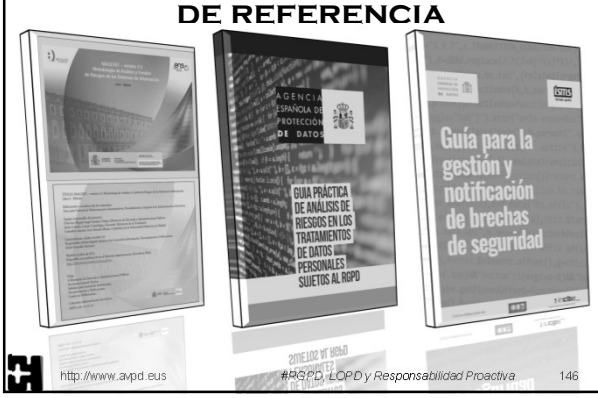
- Resiliencia ("*continuidad de negocio*")
  - "capacidad de adaptación y recuperación ante desastres"
- Seudonimización ("*disociación reversible*")
  - el tratamiento de datos personales de manera tal que:
    - ya no puedan atribuirse a un interesado sin utilizar información adicional,
    - siempre que dicha información adicional figure por separado
  - y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

Notificación de violaciones de seguridad

Notificación de violaciones de seguridad

- Notificación a la Autoridad de Control
  - Salvo que haya un riesgo improbable
- Comunicación a los interesados
  - Siempre que haya un alto riesgo
  - salvo que se hayan aplicado medidas que minimicen el riesgo
  - O suponga un esfuerzo desproporcionado

Materiales & Guías de referencia



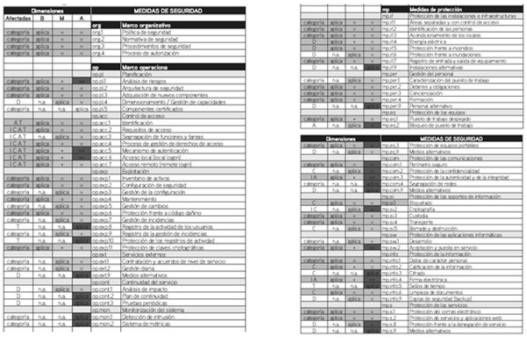
Cómo gestionar la seguridad desde mayo de 2018?

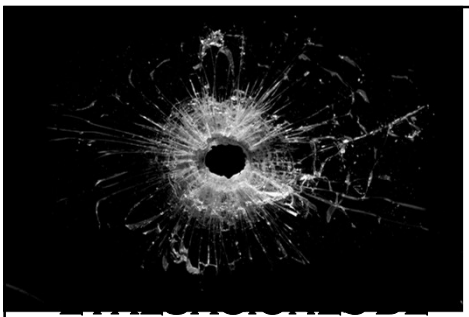
- El RD-1720/2007 ya no es el referente
- Ámbito de tratamientos privados:
  - Códigos de conducta y esquemas de certificación existentes y comúnmente aceptados: ISO-27000, ISO-29000, ISO-31000
  - Nuevos CC&Cert que puedan adoptarse
- Tratamientos de AAPP :
  - ENS (Esquema Nacional de seguridad) (Disp. Adic. Primera de la LOPDGDD-2018)

Puntos de Control ISO-27001

Medidas de Seguridad en el ENS

Puntos de Control en el ENS





IMPACTO SOBRE LA PROTECCIÓN DE DATOS

Las evaluaciones de impacto ("ex-Ante", "Impact assessent")

- Necesarias 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, (…)

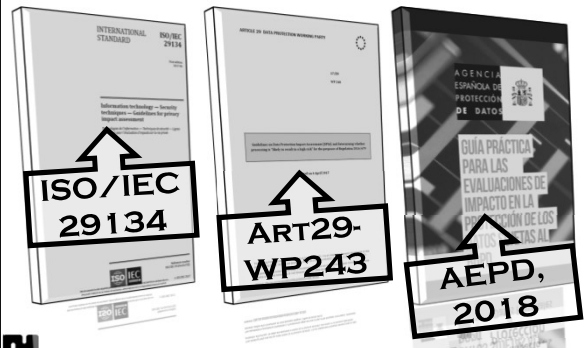
Las evaluaciones de impacto ("ex-Ante", "Impact assessent")

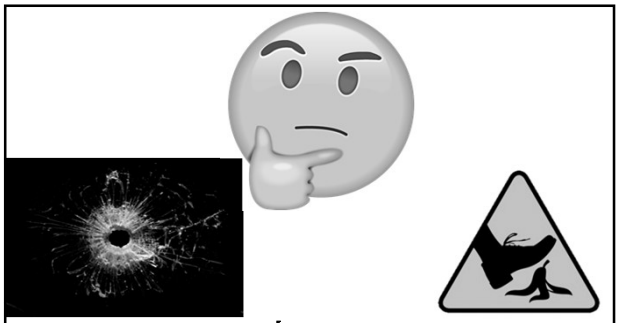
- (…) en particular en caso de:
  - evaluación sistemática y exhaustiva de aspectos personales, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos;
  - tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales, o
  - observación sistemática a gran escala de una zona de acceso público.

Contenido de la evaluación de impacto

- a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento;
- b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- c) una evaluación de los riesgos para los derechos y libertades de los interesados, y
- d) las medidas previstas para afrontar los riesgos.

¿Cómo hacer Evaluaciones de impacto?





Evaluación de impacto .vs. análisis de riesgos

Seguridad / Gestión de Riesgos

Evaluaciones de Impacto

Criterios para determinar el "Alto Riesgo" (Art29WP)

1. Elaboración de perfiles o puntuación de comportamientos
2. Decisiones automatizadas con consecuencias legales o similares
3. Observación sistemática de una zona de acceso público
4. Tratamiento de categorías especiales de datos

Criterios para determinar el "Alto Riesgo" (Art29WP)

5. Tratamiento de datos a gran escala
6. Combinación cruzada de datos procedentes de tratamientos diferentes
7. Tratamiento de datos de colectivos vulnerables
8. Uso innovador de tecnologías o soluciones organizativas
9. Transferencias de datos fuera de las fronteras de la Unión Europea

Criterios para determinar el "Alto Riesgo" (Art29WP)

- solo 1 criterio (de los 9)
  - → No Alto Riesgo
  - → No EIPD
- 2 o más criterios
  - → Alto Riesgo
  - → EIPD necesaria

CÓDIGOS DE CONDUCTA, CERTIFICACIONES Y SELLOS

Códigos de Conducta

- Finalidad:
  - "***contribuir a la correcta aplicación del Reglamento***", teniendo en cuenta:
    - las características de los sectores de tratamiento
    - las necesidades de las (…) pequeñas (…) empresas

Códigos de Conducta

- Definición en el #RGPD:
  - No hay definición en el #RGPD
- Definición de la OIE (Organización Internacional de Empleadores, 1999)
  - *"Declaración expresa de la política, los valores o los principios en que se inspira el comportamiento de una empresa en lo que atañe a:*
    - *el desarrollo de sus recursos humanos,*
    - *su gestión medioambiental*
    - *su interacción con los consumidores, los clientes, los gobiernos y las comunidades en las que desarrolla su actividad*

Códigos de Conducta

- Definición en las Directivas 2005/29/CE y 2008/122/CE
  - *«**código de conducta**»:*
    - *un acuerdo o conjunto de normas no impuestas por disposiciones legales, reglamentarias o administrativas de un Estado miembro,*
    - *en el que se define el comportamiento de aquellos comerciantes que se comprometen a cumplir el código*
    - *en relación con una o más prácticas comerciales o sectores económicos concretos;*
  - *«**responsable del código**»:*
    - *cualquier entidad, incluido un comerciante o un grupo de comerciantes, que sea responsable de la elaboración y revisión de un código de conducta o de supervisar su cumplimiento por quienes se hayan comprometido a respetarlo.*

Los Códigos de Conducta y Certificación

- Mecanismos para la ***acreditación del cumplimiento*** de obligaciones
  - (art.24.3, 28.5, 32.3, 46.2.e)
- Promocionados por:
  - Estados miembros, Autoridades de control,
  - "el Comité", "la Comisión "
- Supervisados por
  - Organismos acreditados
  - Autoridades de Control (sin perjuicio de…)
- Cuando afectan a más de un estado miembro, aplica el "***mecanismo de coherencia***"

Códigos de Conducta