Legislación

Universidad de Sevilla

Departamento de Lenguajes y Sistemas Informáticos

Objetivos


Constitución
Jerarquía
Información
Nacional
Protección
Lopd
Personales
Derechos
Seguridad
Autoridad
Datos
Normativa
Usuarios
Persona
Rgpd
Ámbito
Europeo
Tratamiento
Consentimiento
Introducción

Contenidos

Contenidos

Introducción

La falta de regulación llevó a muchas empresas a hacer negocio con los datos de sus usuarios, cediendo su uso a terceros sin el consentimiento consciente de estos.

Introducción

Empresa	Motivo del abuso / infracción	Sanción / consecuencias
Google & Shein	CNIL de Francia los sancionó por usar cookies publicitarias sin consentimiento adecuado y por no informar transparentemente al usuario. (The Wall Street Journal, Reuters)	€475 millones en total: €325 millones a Google y €150 millones a Shein.
TikTok	Transferencia indebida de datos de usuarios europeos a China y políticas de privacidad insuficientes en cuanto a esa transferencia.	Multa de €530 millones impuesta por la autoridad irlandesa.
Cadena de gimnasios Supera (España)	Uso de reconocimiento facial como único método de acceso, sin consentimiento explícito de los usuarios. Tratamiento de datos biométricos sin base legal. (Cadena SER)	Multa de €96.000 por la AEPD.
British Airways	Fallos de seguridad que permitieron un ataque ("web-skimming") que afectó datos personales de clientes. (Wikipedia)	Inicialmente una multa grande, reducida luego a £20 millones por el ICO en Reino Unido.
Marriott International	No proteger adecuadamente los datos de sus clientes, lo que derivó en una violación de información masiva. (Wikipedia)	Multa de £18.4 millones por el ICO.
Meta Platforms	Transferencias de datos de la UE a EEUU sin garantías legales suficientes. (Wikipedia	Reciente sanción de €1.2 mil millones.

Introducción

Empresa / entidad	Qué hicieron mal	Qué norma se vulneró / tipo de datos implicados	Cuánto se les sancionó
Supera (cadena de gimnasios)	Usó reconocimiento facial como único medio de acceso al gimnasio, sin ofrecer alternativa ni consentimiento expreso libre de los usuarios. Datos biométricos tratados sin legitimación adecuada. Cadena ser	RGPD, art. 9: datos de categoría especial (biométricos); autorización explícita requerida; consentimiento no libre al imponerse como único método.	**96.000 €** tras reducción por reconocimiento de responsabilidad.
LaLiga	Recogida de datos biométricos de espectadores en los accesos a los estadios. El País	RGPD: tratamiento de datos sensibles/biométricos sin legitimación adecuada; uso automático de datos para identificación.	**1.000.000 €** (la multa inicial era mucho mayor, se redujo).
Holiday Fit Tres Cantos (gimnasio)	Grabaciones con móvil durante clases, sin garantizar que los alumnos voluntariamente consintieran salir en vídeos, sin cláusulas contractuales claras, ni consentimientos expresos para uso comercial de imágenes. Huffington Post	RGPD: principio de consentimiento libre; derechos de imagen / uso de grabaciones; transparencia e información.	**21.600 €** (se redujo desde 36.000 € por pronto pago/reconocimiento de responsabilidad).
Hotel & Spa Beverly Park (Girona)	Exigía a huéspedes escanear el DNI como requisito de check-in, lo que implicaba recopilar datos no estrictamente necesarios / almacenamiento de más información de la necesaria. Diario AS	RGPD: principio de minimización de datos; recogida de datos innecesarios; falta de proporcionalidad.	**5.400 €** tras reducción.
Ibermutua	Infringió obligaciones de seguridad de los datos personales: violación del artículo 6 del RGPD (tratamiento lícito) y del art. 5.1.f (seguridad de los datos); no implementó suficientes medidas de protección técnica y organizativa. Software CRM	RGPD: requisitos de licitud y seguridad de los datos; medidas adecuadas de seguridad; responsabilidad proactiva.	**1.000.000 €** (rebajada a **600.000 €** por reconocimiento de responsabilidad).

Introducción: La importancia de los datos

La empresa de análisis de datos Cambridge Analytica -que no tiene ninguna relación con la conocida universidad británica- es conocida por el papel que jugó en durante la **campaña para la elección de Donald Trump** como presidente de EE.UU., durante la cual aportó información compleja sobre el pensamiento de los votantes estadounidenses.

Cómo un test de personalidad de Facebook le sirvió a Cambridge Analytica para recolectar información privada de millones de usuarios sin que lo supieran

Redacción
BBC Mundo

Introducción: Beneficios

CORONAVIRUS >

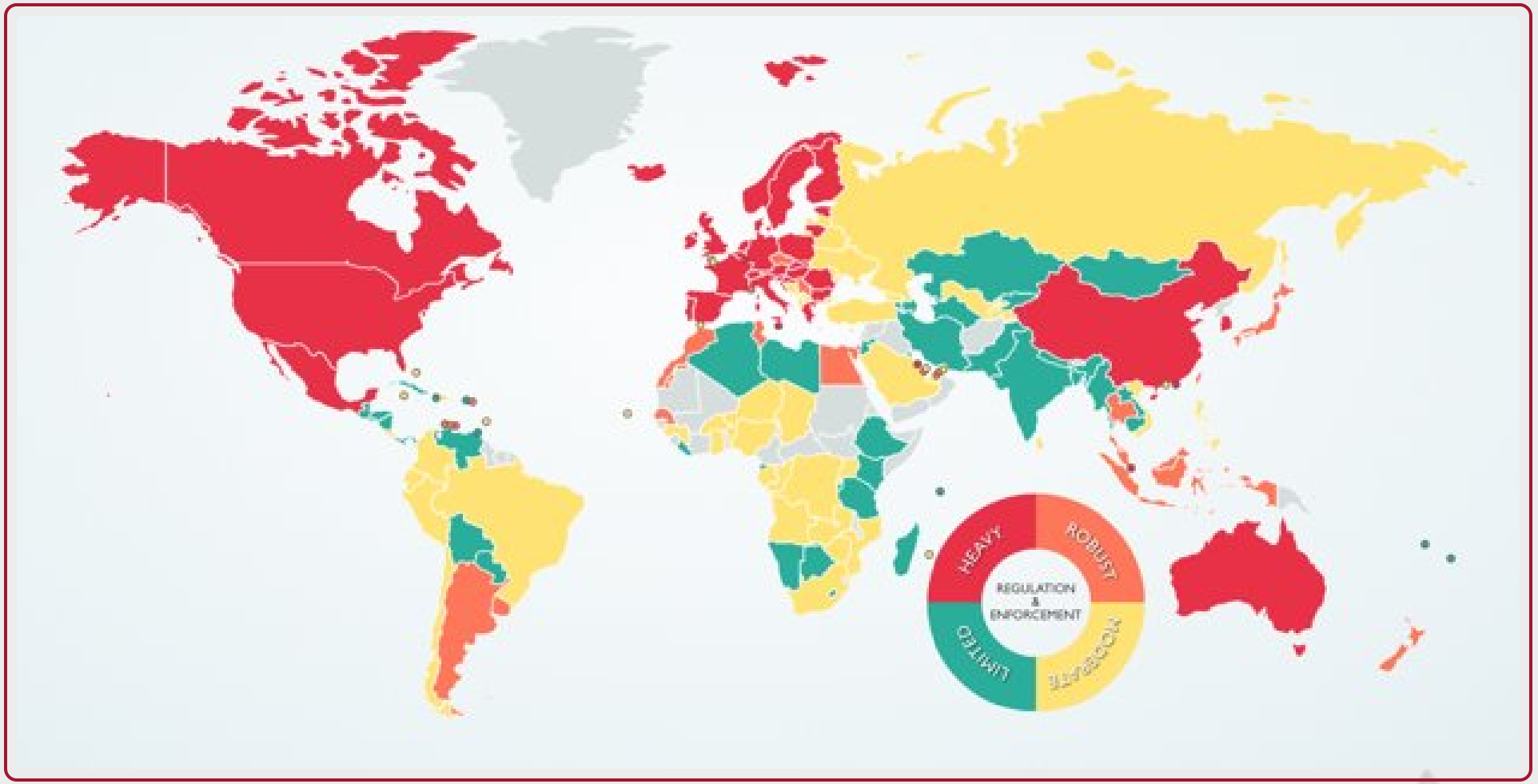
Corea, el ejemplo para controlar la epidemia que España no siguió

El país asiático consigue una drástica reducción del número de casos sin necesidad de cerrar grandes ciudades

El cruce a gran escala de datos privados y de geolocalización permitió a China y Corea del Sur controlar los movimientos de sus ciudadanos y contener la expansión de la epidemia de coronavirus. Este modelo de gestión ha llevado a la Comisión Europea a solicitar a los principales operadores de telecomunicaciones datos de sus clientes para hacer un seguimiento de la Covid-19 en los Estados miembros y poder anticipar el ritmo de evolución de los contagios. Paralelamente, el Gobierno español ha puesto en marcha el programa DataCovid-19 para rastrear los desplazamientos de la población y evaluar así las capacidades sanitarias en cada provincia.

Introducción: El presente

Protección datos en el mundo (Enlace)



Conclusión: Normativa

- No hay que prohibir el uso por parte de las empresas de los datos personales, pero sí regular este uso para que se haga con ciertos límites, y con **plenas garantías** para los derechos de los usuarios.
  - Fines legítimos
  - Información clara
  - Almacenamiento seguro
- Especialmente hay que vigilar las **cesiones y ventas** de datos a organizaciones, tanto del mismo país como de otros países
- La normativa que afecta a las aplicaciones cuya explotación se produce en España existe a nivel:
  - Europeo
  - Nacional

Contenidos

Jerarquía normativa

Las leyes se definen como **documentos legales jurídicos escritos que prevalecen frente a cualquier fuente normativa**.

Dentro de las leyes existe una jerarquía, que dependiendo del rango u órgano de dónde emanen tendrán un lugar en la misma. **Toda norma que contradiga a la de rango superior carece de validez**.

Una vez están aprobadas las leyes, pasan a formar parte del **ordenamiento jurídico**.

Ordenamiento jurídico español

Tipos de normativa - autoridad

Contenidos

Reglamento General de Protección de Datos (RGPD)

Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

- Entrada en vigor: 25 de Mayo de 2018
- Principios clave: licitud, transparencia, minimización, limitación de finalidad y seguridad.
- Derechos del usuario: acceso, rectificación, supresión, oposición, portabilidad y limitación.
- Obligaciones de las empresas: consentimiento expreso, medidas de seguridad, registro y notificación de brechas, privacidad desde el diseño.
- Delegado de Protección de Datos: obligatorio en ciertos sectores o tratamientos masivos.
- Sanciones: hasta 20 M € o el 4 % de la facturación global anual.

https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Datos personales

(Art. 4 RGPD)

Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Tratamiento

(Art. 4 RGPD)

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;

Elaboración de perfiles

(Art. 4 RGPD)

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;

Seudonimización

(Art. 4 RGPD)

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;

Seudonimizar

> se pueden volver a identificar usando la clave.

Anonimizar

> los datos ya no pueden vincularse a una persona.

Autoridad de control

La autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

(Art. 4 RGPD)

Agencia Española de Protección de Datos (AEPD):

- Operativa desde 1994
- Ejerce las funciones de control respecto de los ficheros de datos de carácter personal creados o gestionados por las comunidades autónomas y por la Administración local de su ámbito territorial

Ámbito de aplicación

EL RGPD se aplica a:

- Todos los datos mencionados anteriormente, que hagan referencia a una persona identificable
  - Es posible seudonimizar los datos para ciertos tratamientos
- Se aplica especialmente a:
  i. Datos personales especialmente sensibles, que revelen el origen racial o étnico
  ii. Datos personales de menores
- No se aplica a:
  i. La información anónima, es decir información que no guarda relación con una persona física identificada o identificable
  ii. Los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.
  iii. Los datos personales de personas fallecidas (cada estado miembro debe legislar al respecto)
  iv. Datos de personas jurídicas y empresas

Obligaciones

- Tratamiento leal, legal y transparente de los datos
  - Usar los datos con fin legítimo, solo para ese fin e informando a los usuarios
- Limitación del fin, datos y almacenamiento
  - Almacenar solo los datos necesarios, solo durante el tiempo necesario
- Establecer medidas de protección suficientes
  - Cifrado de datos, comunicaciones seguras…
- Registros de violación de seguridad de los datos
  - Notificar las violaciones de seguridad a la autoridad de control (AEPD)
- Privacidad en diseño
  - Diseñar el producto con la protección de datos en mente, no adaptarlo a posteriori
- Transferencias a terceros con garantías
- Delegado de protección de datos
- Derechos ARCO-POL
- Obtener el consentimiento expreso de los usuarios

Delegado de protección de datos

- Necesarios siempre que:
  - El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
  - Datos a gran escala (LOPDGDD, Art 34)
- Funciones
  - Informar y asesorar al responsable o al encargado del tratamiento y a los empleados
  - Supervisar el cumplimiento del RGPD
  - Ofrecer el asesoramiento
  - Cooperar con la autoridad de control (AEPD)
  - Actuar como punto de contacto
- Designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho
- Podrá formar parte de la plantilla o no.
- Contacto público y registrado por autoridad de control (AEPD)
- Participar en todas las cuestiones relativas a la protección de datos personales
- Facilitar los recursos necesarios
- No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones
- Mantener la confidencialidad
- Podrá desempeñar otras funciones que no den lugar a conflicto de intereses

Derechos ARCO-POL

Derecho de Acceso

Obtener confirmación de si se están tratando datos personales. De ser así, se deberán proporcionar los datos junto a (i) finalidades, (ii) plazo, (iii) categorías, (iv) destinatarios.

Derecho de Portabilidad

Posibilita a los interesados solicitar sus datos personales para que les sean entregados a ellos mismos o bien directamente a otro proveedor de servicios/productos: datos entregados por el interesado (p. e. contacto) y generados por su actividad (p. e. transferencias), excluyéndose los datos inferidos (p. e. perfil de consumo).

Derecho de Rectificación

Obtención de la rectificación de datos inexactos o agregación de datos incompletos.

Derecho de Limitación

Estado intermedio mientras se toma una decisión respecto a una solicitud del interesado. Durante la vigencia de la estimación no se pueden borrar ni tratar los datos.

Derecho de Cancelación

Junto con los principios de minimización de datos y de limitación del plazo de conservación, derivan en la obligación de borrado de datos.

Derecho de Supresión

Eliminación de los datos en alguno de los siguientes supuestos: (i) los datos ya no son necesarios; (ii) los datos han sido tratados ilícitamente; (iii) el interesado se opone al tratamiento / retira el consentimiento.

Derecho de Oposición

Oponerse a los tratamientos de los datos personales que le conciernen.

Derecho de Oponerse a decisiones automatizadas

Posibilidad de oponerse a ser sometido a decisiones 100% automatizadas sin ninguna intervención humana siempre que el tratamiento tenga efectos jurídicos o afecte significativamente al interesado.

Supuestos para evitar pedir el consentimiento

Según el RGPD, hay ciertos supuestos en los que no sería necesario obtener el consentimiento expreso del usuario:

1. Cuando el tratamiento sea necesario para ejecutar un contrato en el que el usuario sea parte.
2. Por aplicación de alguna ley (por ejemplo, la Ley de blanqueo de capitales).
3. Para proteger intereses vitales del interesado o de otra persona o para cumplir con alguna tarea de interés público.
4. Cuando el tratamiento sea necesario para satisfacer intereses legítimos, siempre que sobre este interés no prevalezcan los intereses o derechos y libertades del interesado.

Sin embargo, para prevenir problemas, es mejor obtener el consentimiento

Sanciones del RGPD

Multas de hasta 10M € o 2% del volumen de negocio global del último año:

- Por vulnerar las obligaciones

Multas de hasta 20M € o 4% del volumen de negocio global del último año:

- Por vulnerar los principios básicos de tratamiento
- Por vulnerar los derechos de los interesados
- Por transferir datos a países ajenos a la UE que no tengan un nivel de garantía adecuado
- Incumplimiento de una resolución

Contenidos

Constitución

Artículo 18

> 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 de sus derechos.

Sentencia del TC 94/1998:

> Derecho a la protección de datos de forma que el ciudadano pueda oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

Sentencia del TC 292/2000:

> Protección de Datos como un Derecho Fundamental autónomo e independiente: faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Contenidos

- Tipos de normativa
- Ámbito Europeo
- RGPD
- Directiva 58/2002/CE
- Ámbito Nacional
- Constitución
- **Nueva LOPD (LOPDGDD)**

Nueva LOPD

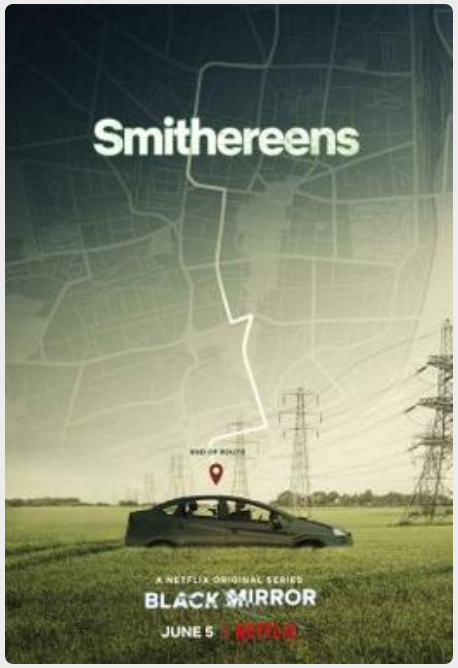
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

- **Deroga** a la antigua Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales (LOPD)
- Su objetivo es **adaptar** el ordenamiento jurídico español al RGPD

Enlace BOE

Datos de personas fallecidas

Los familiares y herederos pueden solicitar el acceso a los datos de la persona fallecida, excepto si ésta lo hubiera prohibido expresamente o así lo establezca una ley



Entidades obligadas a tener delegado PD

1. Colegios profesionales y sus consejos generales.
2. Centros docentes, incluyendo Universidades públicas y privadas.
3. Centros sanitarios. No se incluyen profesionales de la salud que ejerzan a título individual, aunque sí están obligados a guardar el historial clínico de los pacientes.
4. Empresas que exploten redes y presten servicios de comunicaciones electrónicas, cuando traten datos personales a gran escala de forma sistemática.
5. Prestadores de servicios de la información que elaboren perfiles de usuarios a gran escala.
6. Entidades de ordenación, supervisión y solvencia de entidades de crédito.
7. Establecimientos financieros de crédito.
8. Aseguradoras y reaseguradoras.
9. Empresas que ofrecen servicios de inversión, reguladas por la legislación del Mercado de Valores.
10. Distribuidores y comercializadores de energía eléctrica y gas natural.
11. Entidades responsables de ficheros relacionados con la solvencia patrimonial, prevención del fraude, blanqueo de capitales o financiación del terrorismo.
12. Compañías que desarrollen actividades de publicidad y prospección comercial, cuando realicen evaluaciones de perfiles de usuarios y lleven a cabo tratamientos basados en las preferencias de los mismos.
13. Entidades que emitan informes comerciales sobre personas físicas.
14. Operadores de juegos y apuestas que desarrollen su actividad a través de canales electrónicos, informáticos, telemáticos e interactivos.
15. Empresas de seguridad privada.
16. Federaciones deportivas que traten datos personales de menores

Conclusiones

La **protección de datos** no busca prohibir el uso de información personal, sino fijar **límites**, **garantías** y **responsabilidades**.

El marco legal se aplica en dos niveles: **europeo** (RGPD) y **nacional** (Constitución y LOPDGDD).

En la **jerarquía normativa**, toda norma inferior que contradiga una superior **carece de validez**.

En sistemas de información, cumplir la normativa es un requisito **jurídico**, **técnico** y **organizativo**.

Conclusiones

El RGPD define conceptos clave: **dato personal**, **tratamiento**, **elaboración de perfiles** y **seudonimización**.

Deben aplicarse principios de **licitud**, **transparencia**, **minimización**, **limitación de finalidad** y **seguridad**.

La organización debe garantizar **consentimiento expreso** (salvo base legitimadora alternativa), **privacidad desde el diseño** y **notificación de brechas**.

Los interesados ejercen derechos **ARCO-POL**: **acceso**, **rectificación**, **supresión**, **oposición**, **portabilidad** y **limitación**.

Conclusiones

La LOPDGDD **adapta** el RGPD al ordenamiento español y añade aspectos como datos de **personas fallecidas** y **derechos digitales**.

Muchas entidades están obligadas a designar **Delegado de Protección de Datos (DPD)** y a cooperar con la **AEPD**.

El incumplimiento puede implicar sanciones de hasta **10 M EUR / 2%** o **20 M EUR / 4%** del volumen global.

La protección de datos debe incorporarse desde el análisis de requisitos hasta la operación del sistema: **cumplimiento continuo**.

Gracias

Universidad de Sevilla

Departamento de Lenguajes y Sistemas Informáticos