

Privacidad: Aspectos Legales

David Rodríguez González

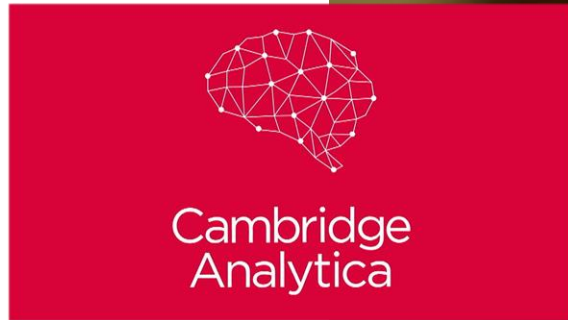
Grupo de Computación Avanzada y e-Ciencia



La protección de las personas físicas en relación con el tratamiento de los datos de carácter personal es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) disponen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Newsreels



Project Nightingale

Nikkei 23319.87 -0.85% ▼ Hang Seng 26517.10 -2.03% ▼ U.S. 10 Yr -0/32 Yield 1.918% ▼ Crude Oil 56.56 -0.42% ▼ Yen 109.06 0.04% ▲ DJIA 27691.49 0.00% ▼

THE WALL STREET JOURNAL.

English Edition ▼ November 13, 2019 | Print Edition | Video

Subscribe | Sign In

Search 🔍


SHARE

WSJ NEWS EXCLUSIVE | TECH

Google's 'Project Nightingale' Triggers Federal Inquiry

Deal with Ascension health system aimed at improving patient care provides Google with health-data gold mine

208



Why Big Tech Wants Access to Your Medical Records

Tech giants like Amazon and Apple are expanding their businesses to include electronic health records -- which contain data on diagnoses, prescriptions and other medical information. That's creating both opportunities and spurring privacy concerns. Here's what to know. Photo Composite: Heather Seidel/ The Wall Street Journal (Originally published Jan. 9, 2019)

Por [Rob Copeland](#) and [Sarah E. Needleman](#)
Actualizado miércoles, 13 de noviembre de 2019 5:13 EDT

Google's project with the country's second-largest health system to collect detailed health information on 50 million American patients sparked a federal inquiry and criticism from patients and lawmakers.

MOST POPULAR VIDEOS

1. Three Things Not Known About the Public Impeachment Hearings
2. Impeachment Hearings: What's Been Said Behind Closed Doors
3. Why Big Tech Wants Access to Your Medical Records
4. Hong Kong Officer Shoots at Protesters
5. Why Your Connecting Gate May Be a Mile Walk

MOST POPULAR ARTICLES

1. Google Amasses Medical Records of Millions of People
2. Once-Hot Bet on Housing for Seniors Is Cooling Off

- Datos cedidos por Ascension Health
 - Opera en 21 estados de EEUU y en DC
 - 10 millones de personas
 - Objetivo 50 en marzo
 - Sin notificar a los pacientes o médicos
 - **No anonimizados**
- Al menos 150 empleados de Google han tenido acceso
- Pero no sólo Google está interesado en los datos médicos:
 - Apple
 - Intel
 - Microsoft
 - Amazon

Reconocimiento facial a partir de Resonancias Magnéticas

Nikkei 23319.87 -0.85% ▼ Hang Seng 26515.70 -2.03% ▼ U.S. 10 Yr -1/32 Yield 1.924% ▼ Crude Oil 56.54 -0.46% ▼ Yen 109.06 0.04% ▲ DJIA 27691.49 0.00% ▼

THE WALL STREET JOURNAL.
English Edition | November 13, 2019 | Print Edition | Video

Subscribe | Sign In

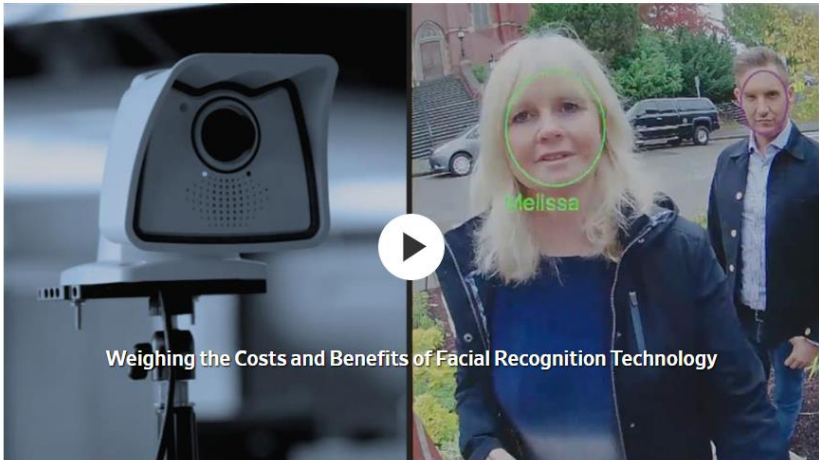
Search 🔍

HEALTH

SHARE
AA
TEXT

Facial-Recognition Software Was Able to Identify Patients From MRI Scans

Study calls attention to a privacy threat that is set to grow as technology improves and medical-imaging data increases



Weighing the Costs and Benefits of Facial Recognition Technology

Facial recognition is going mainstream. The technology is increasingly used by law-enforcement agencies and in schools, casinos and retail stores, spurring privacy concerns. In this episode of Moving Upstream, WSJ's Jason Bellini tests out the technology at an elementary school in Seattle and visits a company that claims its algorithm can identify potential terrorists by their facial features alone.

Por [Melanie Evans](#)
miércoles, 23 de octubre de 2019 23:02 EDT

Facial-recognition software correctly matched photos of research volunteers to unidentified medical scans of their heads, in a new study of images that are commonly used in brain research.

MOST POPULAR VIDEOS

1. Three Things Not Known About the Public Impeachment Hearings
2. Impeachment Hearings: What's Been Said Behind Closed Doors
3. Why Big Tech Wants Access to Your Medical Records
4. Hong Kong Officer Shoots at Protesters
5. Why Your Connecting Gate May Be a Mile Walk

MOST POPULAR ARTICLES

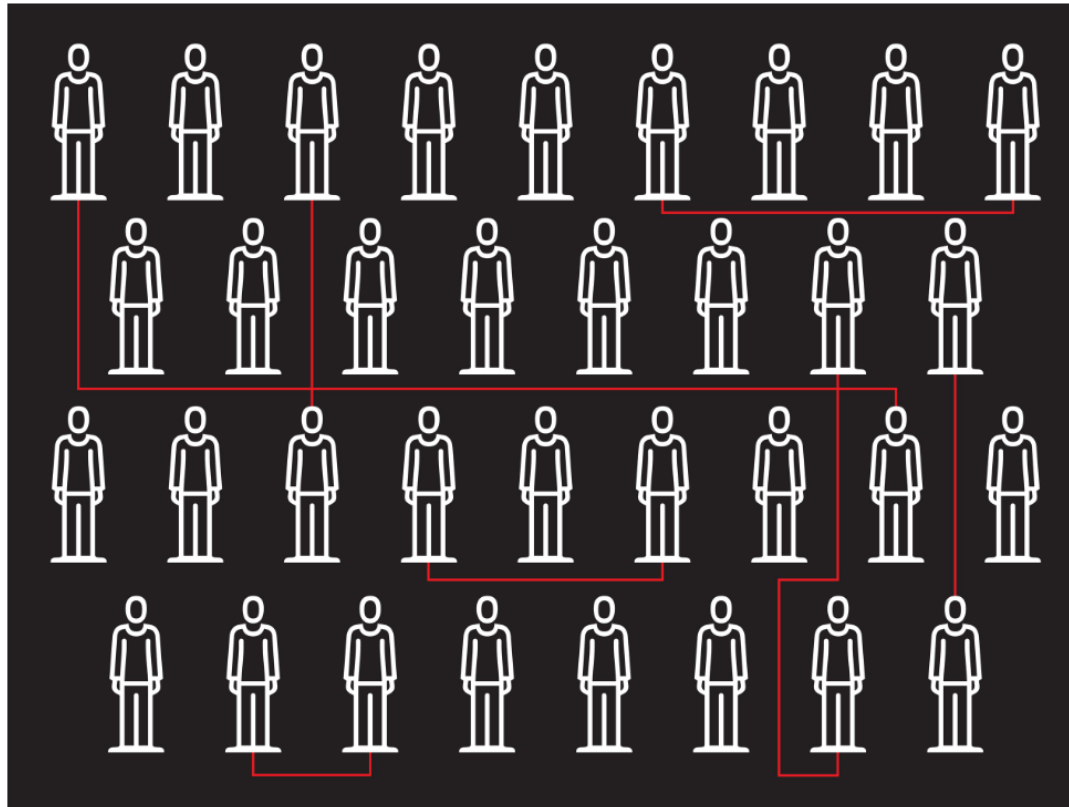
1. Google Amasses Medical Records of Millions of People
2. Once-Hot Bet on Housing for Seniors Is Cooling Off

- [October 24, 2019](#)
N Engl J Med 2019; 381:1684-1686
DOI: 10.1056/NEJMc1908881
- Clínica Mayo
- 83% precisión
- Microsoft Azure
- 84 volunteers participated in the study

Identificación ADN

Genome Hackers Show No One's DNA Is Anonymous Anymore

Consumer genomics is making it easier than ever to identify individuals from anonymous DNA databases. Even if you've never spit in a tube.

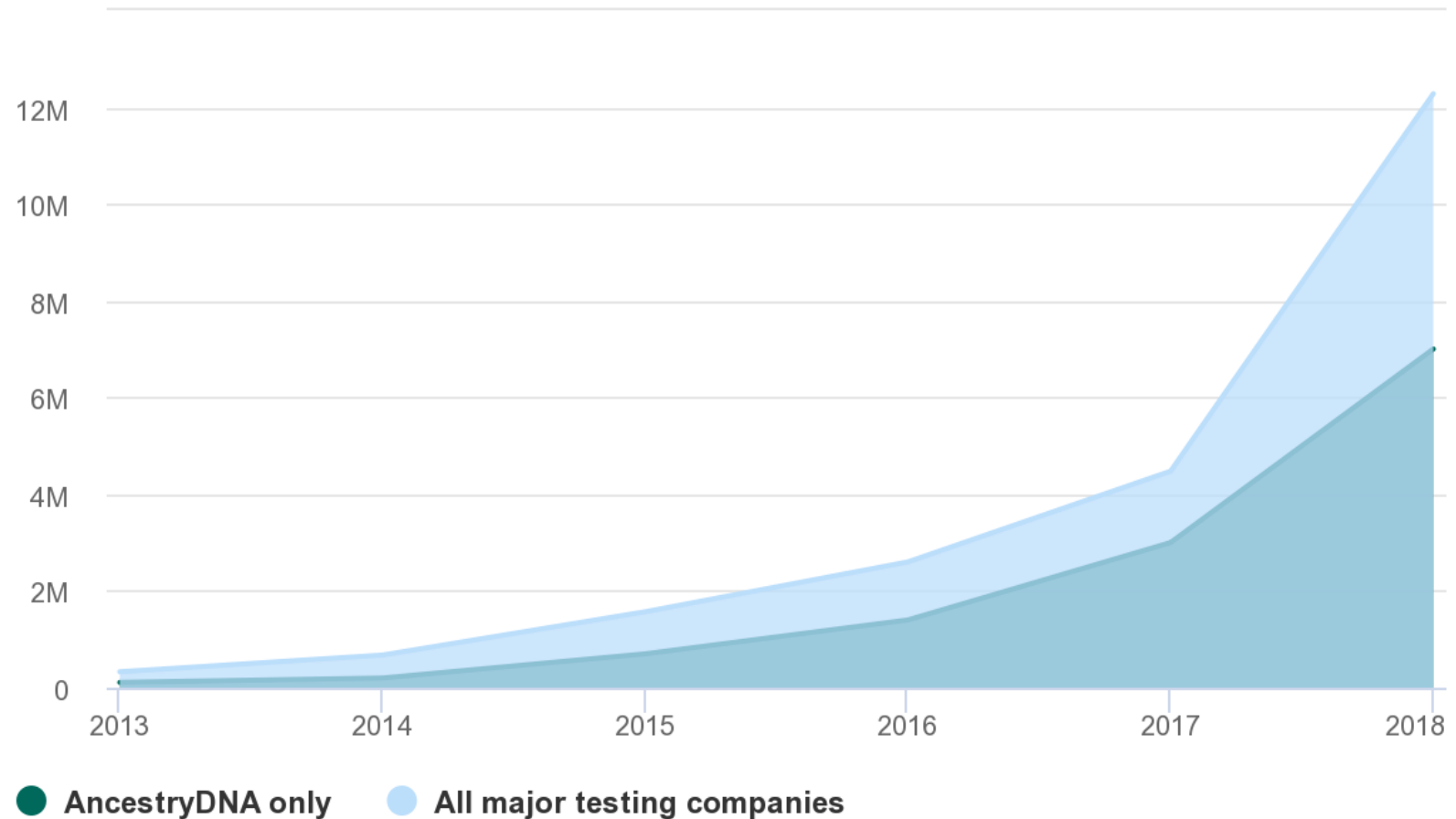


HOTLITTLEPOTATO

Genómica de consumo

Up, up, and away

Total number of people tested by consumer genetics companies, in millions.



Identificación de sujetos en bases de datos anónimas de ADN

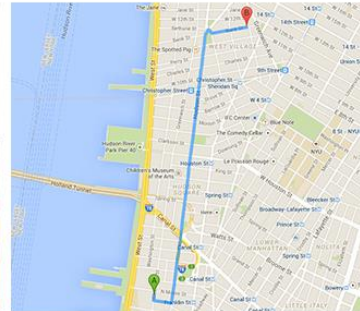
- 2013 Yaniv Erlich: Identificación de sujetos a partir de bases de datos de ADN anónimas por medio de inferencia de apellidos.
 - Identifying Personal Genomes by Surname Inference (Science 18 Jan 2013)
 - DOI: 10.1126/science.1229566
 - Restricción del acceso a datos genéticos.
 - NIH: “The chances of this happening for most people are small, but they’re not zero”
- Genética de consumo (23andMe and Ancestry) más de 12 millones de perfiles genéticos a finales de 2017 (MIT Technology Review feb. 2018)
 - Principalmente en EEUU
- Se estima que la cantidad de datos genéticos disponibles permiten ahora a más de la mitad de la población de EEUU (Science nov. 2018)
 - Más del 60% de los americanos de origen europeo,
 - independientemente de si se han hecho el test.
 - Uso de webs para compartir datos genéticos GED Match.

Ejemplo: Datos abiertos de Nueva York

- Nueva York publicó los trayectos de taxi1 (lugar y hora de recogida, número de taxi, lugar y fecha de destino, etc.) como un dataset abierto
- Ataque 1: Anonimizado a través de MD5 en principio, fue posible desanonimizarlo.
- Ataque 2: Cruzando este dataset con fotos geolocalizadas (obtenidas a través de Google) de famosos subiendo en taxi se pudo sacar los trayectos que hacen.



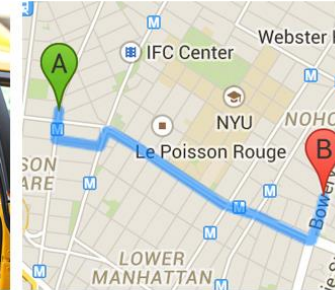
BRADLEY COOPER



JULY 8, 2013 • 7:34 PM - 7:44 PM
376 GREENWICH ST. TO 13 BANK ST.
\$9.00 FARE • CASH; UNKNOWN TIP • ©SPLASH



OLIVIA MUNN

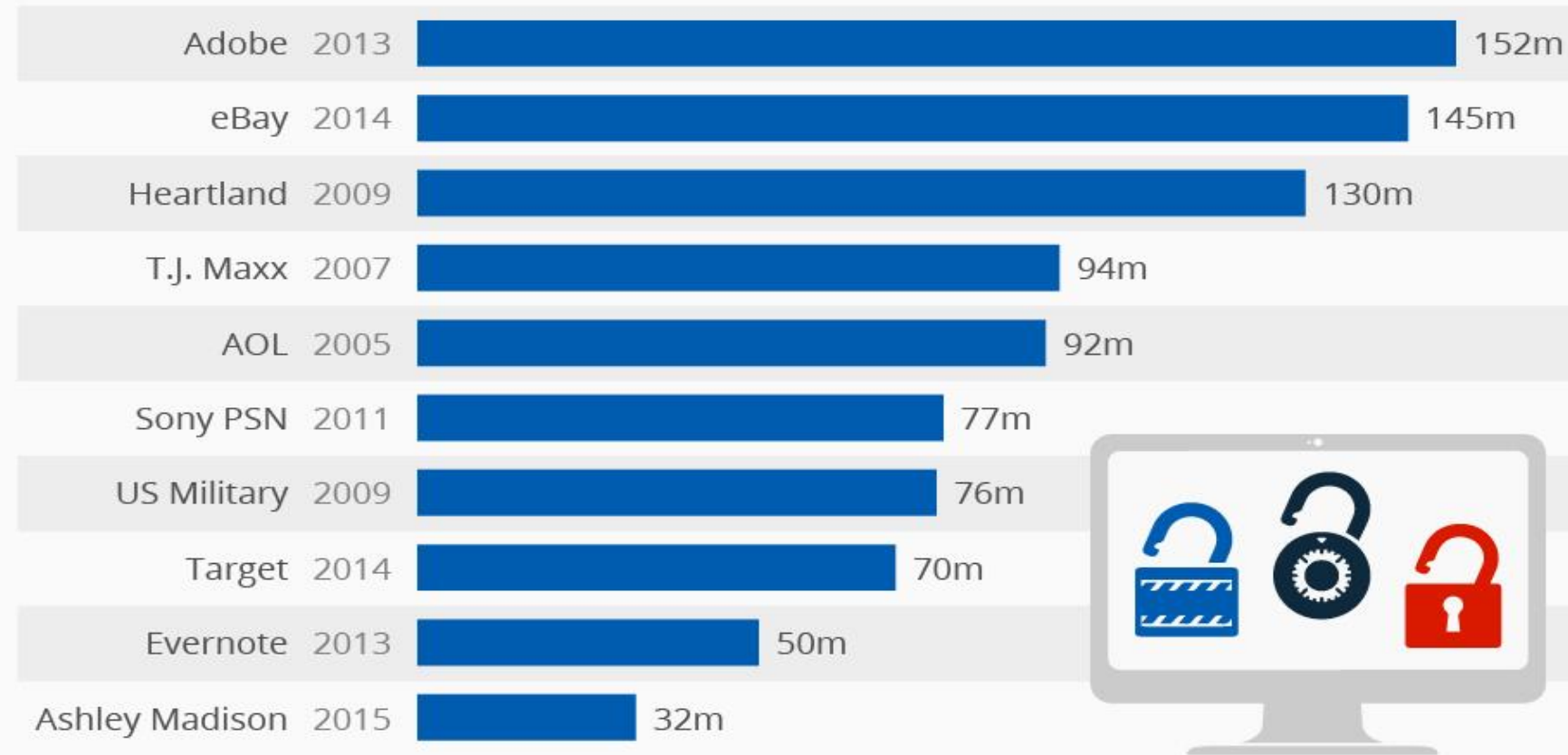


JULY 8, 2013 • 11:20 AM - 11:26 AM
225 VARICK ST. TO 325 BOWERY
\$6.00 FARE • CASH; UNKNOWN TIP • ©SPLASH

<https://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546>

Large-Scale Data Breaches Affect Millions of Users

Number of compromised data records in recent large-scale data breaches



@StatistaCharts Source: Media Reports

statista

Introducción

Legislación actual y precedentes

Reglamento General de Protección de Datos

- Legislación actual en la Unión Europea
- Aprobado el 27 de abril de 2016
- Entró en vigor el 25 de mayo de 2018
- Deroga la Directiva 95/46/CE de 24 de octubre de 1995
 - Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Supone una profunda modificación del régimen vigente:
 - Derechos y deberes
 - Supervisión por parte de las autoridades

Implementación en España

- Inicialmente:
 - Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
 - Deroga el Real-decreto mencionado
 - Y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal

Objetivos RGPD

- Superar los obstáculos que impidieron la finalidad armonizadora de la Directiva
 - La transposición de la directiva generó un mosaico normativo irregular
 - Provoca diferencias en la protección de los derechos de los ciudadanos
- Adaptarse a nuevas circunstancias:
 - Aumento de los flujos de datos transfronterizos (mercado interior)
 - Evolución tecnológica y globalización
 - Los datos personales son el recurso fundamental de la sociedad de la información
- Reforzar la seguridad jurídica y la transparencia

Precedentes

- En 1890 en EEUU dos abogados, Warren and Brandeis, publican el artículo The Right to Privacy: “the right to be left alone”.
- Declaración Universal de los Derechos Humanos (1948): el derecho a la privacidad es el número 12
 - “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”
- 1967 entra en vigor la Freedom of Information Act (FOIA) en EEUU
- En 1980 la OCDE publica una guía sobre protección de datos

Precedentes en Europa

- Artículo 8 de la Convención Europea de Derechos Humanos
 - Consejo de Europa en Roma, 4 de noviembre de 1950; en vigor 3 de septiembre de 1953
 - Ahora Carta de los Derechos Fundamentales de la Unión Europea
- Trabajos desarrollados en el Consejo de Europa desde finales de la década de 1960
- En 1981 el Consejo adopta la Convención de Protección de datos (Tratado 108), el derecho la privacidad se convierte en un imperativo legal
- Directiva 95/46/CE de 24 de octubre de 1995

Precedentes en Europa

- Artículo 286 Tratado Constitutivo de la Comunidad Europea (vigente hasta el 1 de diciembre de 2009)
- Ahora Artículo 16 del Tratado de Funcionamiento de la Unión Europea
 - “Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan”
 - “El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.”
- El artículo 39 del Tratado de la Unión Europea fija las competencias
 - “el Consejo adoptará una decisión que fije las normas”

Precedentes en España

- Constitución española
 - Artículo 18.4
 - “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”
- LORTAD, Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales
- Remplazada por la antes mencionada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, que transponía la directiva europea 95/46/CE

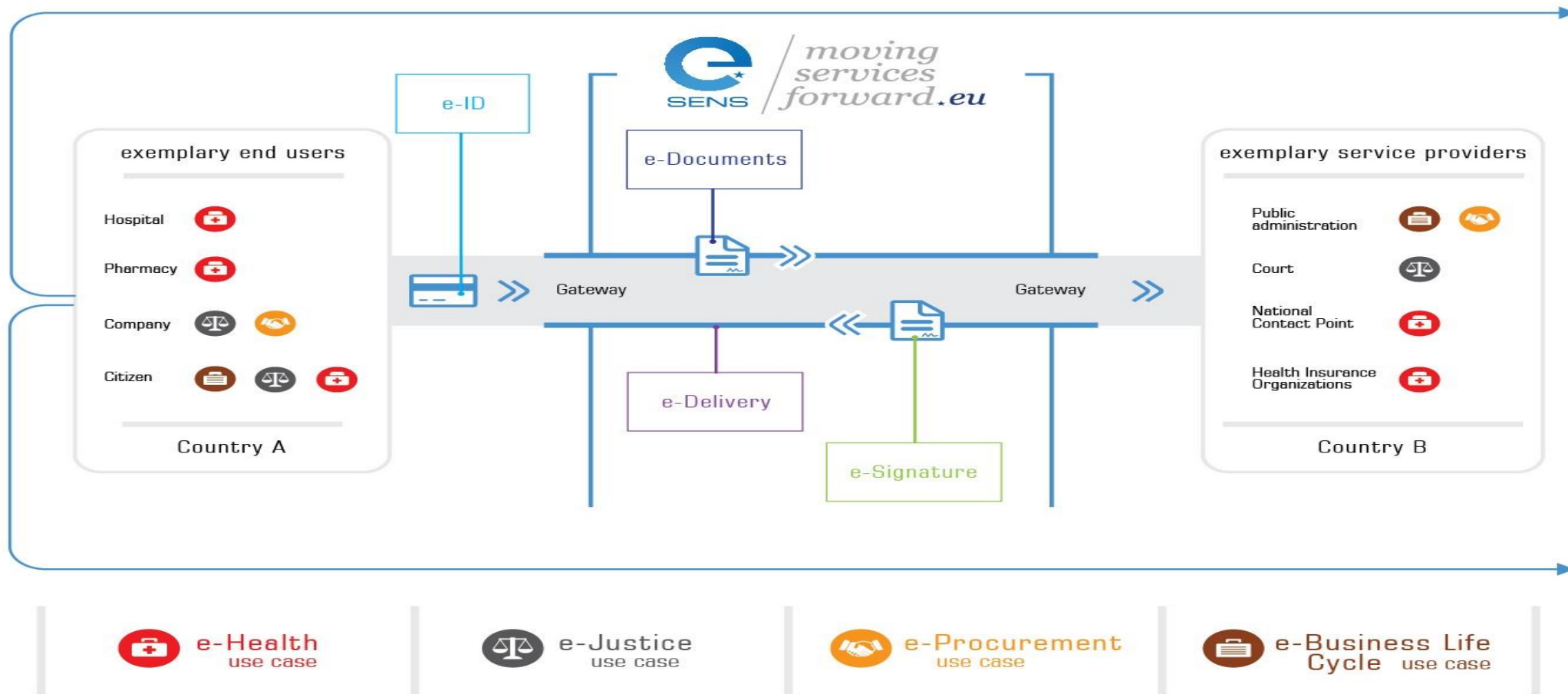
Reglamento General de Protección de Datos

Legislación Europea

Reglamento General de Protección de Datos

- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**
 - Aprobado el 27 de abril de 2016; de aplicación el 25 de mayo de 2018
- Norma a nivel de la Unión Europea que rige la protección de datos de personas físicas y la libre circulación de los mismos
- Aplicable a todo tratamiento de datos personales por entidades radicadas en la Unión Europea, aunque los tratamiento de los datos se lleve a cabo fuera de la misma

Mercado Único Digital de la Unión Europea



http://www.noraonline.nl/wiki/NORA_licentie http://www.noraonline.nl/wiki/Bestand:E-SENS_architecture.jpg (<https://www.esens.eu/>)

- Pasa de un modelo basado en el control del cumplimiento
- ... a uno basado en el principio de responsabilidad activa
 - Valoración previa del riesgo que puede conllevar el tratamiento de los datos personales
 - Adoptar las medidas que procedan.
- Delegados de protección de datos
 - El RGPD y la ley orgánica regulan de forma detallada sus funciones
 - Figura obligatoria en algunos casos especificados en el RGPD
 - El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
 - Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
 - Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

RGPD: resumen novedades

- Más control y derechos para los sujetos.
- Más obligaciones para los controladores de datos.
- Más poder para el regulador.

Responsabilidades

- Dos tipos de responsabilidad: corporativa e individual
- Corporativa (en el caso de la Universidad el rector, jefes de servicios, etc.):
 - Asegurar el cumplimiento
 - Desarrollar y fomentar buenas prácticas de gestión de información dentro de sus áreas de responsabilidad.
 - Se puede delegar la gestión, pero no la responsabilidad.
- Responsabilidad individual: todo el personal
 - Responsabilidad de cumplir con el reglamento.

Terminología

- Datos personales
- Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre los datos personales
- Seudonimización: tratamiento de datos personales para que ya no puedan atribuirse a un interesado sin utilizar información adicional
- Consentimiento del interesado

Actores

- El interesado (persona sobre quien versan los datos personales)
- Responsable/corresponsables del tratamiento
- Encargados del tratamiento
- Destinatario
- Delegado de protección de datos
- Regulador

¿Qué son datos personales?

- Cualquier información sobre una persona a través de la cual dicha persona pueda ser directa o indirectamente identificada
 - Información estructurada
 - Sobre un individuo vivo
 - Identificable directa o indirectamente
 - Incluye identificadores en línea
 - Los datos deben ser almacenados
 - Tratamiento automatizado de datos personales
 - Y también sistemas de archivo manuales

¿Qué hace a los datos identificables?

- Año de nacimiento

¿Qué hace a los datos identificables?

- Sexo

¿Qué hace a los datos identificables?

- Código postal
- En España hay 11 752 códigos postales

¿Qué hace a los datos identificables?

- Lugar de nacimiento

¿Qué hace a los datos identificables?

- Año de nacimiento
- Sexo
- Código postal
- Lugar de nacimiento

¿Qué hace a los datos identificables?

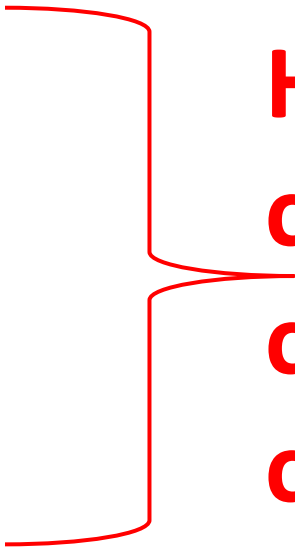
- Código postal
- En España hay 11 752 códigos postales
- CP 39580

¿Qué hace a los datos identificables?

- Código postal
 - En España hay 11 752 códigos postales
 - Pero no todos son iguales a la hora de identificar a una persona.
- Por ejemplo: 39580
 - Bejes: 69
 - Caldas (Peñarrubia): 20
 - Cicera: 69
 - La Hermida: 94
 - Linares: 76
 - Navedo: 49
 - Piñeres: 53
 - Roza (Peñarrubia): 19

¿Qué son datos personales?

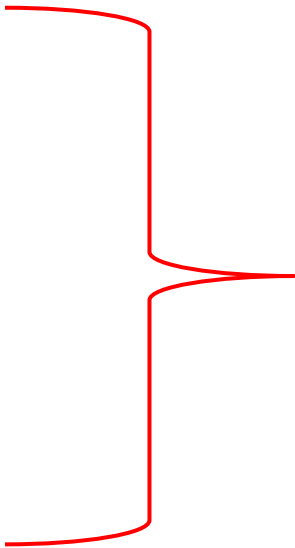
- Cualquier información sobre una persona a través de la cual dicha persona pueda ser directa o indirectamente identificada
 - Información estructurada
 - Sobre un individuo vivo
 - Identificable directa o indirectamente
 - Incluye identificadores en línea
 - Los datos deben ser almacenados
 - Tratamiento automatizado de datos personales
 - Y también sistemas de archivo manuales



Hay que tener en cuenta el contenido y el contexto.

¿Qué son datos personales?

- Cualquier información sobre una persona a través de la cual dicha persona pueda ser directa o indirectamente identificada
 - Información estructurada
 - Sobre un individuo vivo
 - Identificable directa o indirectamente
 - Incluye identificadores en línea
 - Los datos deben ser almacenados
 - Tratamiento automatizado de datos personales
 - Y también sistemas de archivo manuales



Test: “intruso motivado”. ¿Qué es razonable?

Intruso motivado

- Aquel que sin partir de conocimientos previos acerca de un individuo desea identificarlo a partir de una base de datos anonimizada.
- Se trata de una persona con competencias técnicas,
 - Pero no posee necesariamente habilidades (hacking) o equipos especiales.
- Puede acceder a toda la información pública disponible
 - Internet
 - Bibliotecas
 - Documentos públicos
- Hará uso de técnicas de investigación para encontrar información adicional
 - Esto incluye el preguntar a gente que pueda poseer conocimientos adicionales
 - Pero no el recurrir a procedimientos delictivos, como allanamientos de morada.

¿Qué dice el RGPD?

- Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable.
- **Los datos personales seudonimizados**, que cabría atribuir a una persona física mediante la utilización de información adicional, **deben considerarse** información **sobre una persona física identificable**.
- Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que **razonablemente** pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.

¿Qué dice el RGPD?

- Para determinar si existe una **probabilidad razonable** de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.
- Por lo tanto **los principios de protección de datos no deben aplicarse a la información anónima**, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.
- En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

¿Qué dice el RGPD?

- Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable.
- Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable.
- Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.
- Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.
- Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Taller: ¿son datos personales?

15 minutos para discutir los casos en grupos de 3 personas.

Luego discutimos las respuestas entre toda la clase.

Categorías especiales de datos

- Corresponden a lo que se denominaba datos personales sensibles en la antigua directiva, pero con añadidos
- Orígenes étnicos o raciales
- Opiniones políticas
- Creencias religiosas
- Pertenencia a organizaciones sindicales
- Datos sobre salud física o mental
- Orientación y vida sexual
- Datos genéticos
- Datos biométricos

Tratamiento de datos personales relativos a condenas e infracciones penales

- Se trata específicamente en el artículo 10 del RGPD
- Sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el derecho de la UE o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados
- Sólo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas



Taller: ¿son datos personales de categoría especial?

10 minutos para discutir los casos en grupos de 3 personas.
Luego discutimos las respuestas entre toda la clase.

Principios (Capítulo II)

- Artículo 5. Principios relativos al tratamiento
- Artículo 6. Licitud del tratamiento
- Artículo 7. Condiciones para el consentimiento
- Artículo 8. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información
- Artículo 9. Tratamiento de categorías especiales de datos personales
- Artículo 10. Tratamiento de datos personales relativos a condenas e infracciones penales
- Artículo 11. Tratamiento que no requiere identificación

Principios relativos al tratamiento

- Los datos personales se tratarán de forma lícita, leal y transparente
- Limitación de propósito
- Minimización de datos
- Exactitud y actualización
- Limitación del tiempo de almacenamiento
- Integridad y confidencialidad
- Responsabilidad proactiva

Licitud del tratamiento (bases legales)

- Consentimiento
- Necesario para ejecución de contrato
- Cumplimiento de una obligación legal
- Protección de intereses vitales del interesado o de otra persona física
- Interés público o en el ejercicio de poderes públicos
- Intereses legítimos del responsable o u tercero (balance con los del interesado)

Tratamiento de categorías especiales de datos personales

- El interesado dio su consentimiento explícito
 - Excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición no puede ser levantada por el interesado
 - Ese es el caso en España
- Necesario para cumplimiento de obligaciones y derechos laborales, de seguridad y protección social
- Proteger intereses vitales del interesado o de otra persona física
- El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos
- Formulación, ejercicio o defensa de reclamaciones o cuando los tribunales actúen en el ejercicio de su función judicial

Tratamiento de categorías especiales de datos personales

- Por una fundación, asociación u otro organismo sin ánimo de lucro
 - Cuya finalidad sea política, filosófica, religiosa o sindical
 - Exclusivamente miembros actuales o antiguos del organismo
 - O personas que mantengan contactos regulares en relación con sus fines
- Interés público esencial
- Medicina preventiva o laboral, diagnóstico médico, prestación de asistencia o tratamiento sanitario o social, o gestión de sistemas de salud y sociales
- Salud pública
 - Secreto profesional
- Archivo en interés público, fines de investigación científica o histórica, o fines estadísticos

Compartir datos internamente

- El RGPD no es una barrera que impida que se compartan datos personales internamente en una organización
- Siempre que se cumpla (y se señale) una de las bases legales para el tratamiento de datos personales
- Y se sigan los principios

Consentimiento

Condiciones y validez

Consentimiento

- «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;
- Los requisitos han aumentado
- La carga de la prueba recae en el responsable, debe demostrar que ha obtenido un consentimiento valido

Condiciones para el consentimiento

- Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo
- El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada.
 - Antes de dar su consentimiento, el interesado será informado de ello.
 - Será tan fácil retirar el consentimiento como darlo.
- Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Consentimiento Válido

- Libre
- Granular
- Activo
 - El silencio, las casillas ya marcadas o la inacción no son validos
 - LOPDGDD hace mención a lo recogido en el RGPD: se excluye el "consentimiento tácito"
- El interesado debe conocer como mínimo la identidad del responsable del tratamiento
- Verificable
- Fácil de retirar
- Renovado periódicamente

Consentimiento tratamiento datos de menores

- Oferta directa de servicios de la sociedad de la información
- El reglamento establece 16 años como edad de consentimiento
 - Por debajo los tutores legales deben dar el consentimiento
 - Pero deja a los estados la posibilidad de establecer una edad inferior por ley, siempre que no sea inferior a 13 años
- En España la Ley Orgánica establece los 14 años como edad para el consentimiento del tratamiento de datos personales
- Por ejemplo, en Escocia se ha establecido una edad de 12 años en general para ejercer los derechos sobre los datos y el consentimiento
 - Pero 13 para servicios en línea (servicios de la sociedad de la información)

Taller: consentimiento informado

¿Cuáles son los problemas en cada ejemplo, si es que los hay?

10 minutos para discutir los casos en grupos de 3 personas.

Luego discutimos las respuestas entre toda la clase.

Privacidad: aspectos legales

Política de protección de datos: responsables y encargados

Bases legales

Derechos

EIPD

Sanciones

Ley Orgánica de Protección de datos

Política de protección de datos

Responsables y encargados

Política de Protección de Datos

- Ver sección artículo 13
- Debe identificar:
 - Al responsable y al DPD
 - Propósito y base legal para el tratamiento
 - Cualquier interés legítimo cuando se base en el artículo 6 (1,f)
 - Destinatarios o categorías de destinatarios de los datos
 - Información sobre posible transferencia a terceros países
 - Periodo de retención o criterios para determinarlo
 - Origen de los datos si no se obtuvieron directamente del interesado

Política de Protección de Datos

- También debe incluirse información sobre:
 - Los derechos de los interesados, y el derecho a reclamar ante la autoridad competente
 - En España la AEPD o las autonómicas correspondientes
 - Las consecuencias de no proporcionar los datos en caso de que sea un requisito legal o contractual
 - La existencia de decisiones automatizadas, incluida elaboración de perfiles
 - Lógica aplicada
 - Importancia y consecuencias para el interesado

Política de Protección de Datos

- La información debe ser clara y concisa
- Es decir:
 - No usar términos ambiguos como podría, en ocasiones,...
 - Lenguaje adecuado a la audiencia esperada
 - No citar la ley y usar construcciones simples
 - Usar encabezamientos claros y guiones
 - Organización en capas



“We firmly believe that privacy is both inconsequential and unimportant to you. If it were not, you probably would not have a Facebook, Twitter, or LinkedIn account: and you certainly wouldn't ever use a search engine like Google. If you're one of those tin-foil-hat wearing crazies that actually cares about privacy: stop using our services and get a life.”

Fuente: “The World's Worst Privacy Policy”, Andy Greenberg, Forbes, 2012

<https://www.forbes.com/sites/andygreenberg/2012/01/25/the-worlds-worst-privacy-policy>

Algunos ejemplos

- UC
 - <https://web.unican.es/consejo-direccion/gerencia/rgpd/politica-general-de-proteccion-de-datos-en-la-universidad-de-cantabria>
 - Normativa propia <https://web.unican.es/consejo-direccion/secretaria-general/Documents/NormativapropiaLOPDCG171219.pdf>
 - DPD
 - Gema Bilbao Prieto
 - dpd@unican.es
- CSIC
 - <https://www.csic.es/es/aviso-legal>
 - <https://www.csic.es/es/el-csic/proteccion-de-datos>
 - DPD
 - José López Calvo
 - delegadoprotecciondatos@csic.es
- UIMP
 - http://www.uimp.es/images/institucional/Politica_de_privacidad_UIMP_Octubre.pdf
 - Ahora accesible desde la página web principal.
 - DPD: la propia organización, no identifican a la persona física responsable, pero dan una dirección de correo electrónico
 - dpd@uimp.es
 - En el año 2018 organizaron encuentros sobre el RGPD
 - Con un convenio de colaboración con la AEPD como se puede ver en el BOE
 - <https://www.boe.es/boe/dias/2018/06/29/pdfs/BOE-A-2018-9003.pdf>

Responsable del Tratamiento (Controlador)

- La persona física o jurídica, autoridad pública, agencia, u otra organización que, en solitario o junto con otros, determina los propósitos y los medios usados en el tratamiento de los datos personales
- Responsabilidades:
 - Aplicar medidas técnicas y organizativas adecuadas para garantizar, y poder demostrar, que el tratamiento cumple el RGPD
 - Protección de los datos
 - Adhesión a códigos de conducta

Protección de datos desde el diseño y por defecto

- El responsable aplicará medidas técnicas y organizativas adecuadas
 - Tanto en el momento de determinar los medios de tratamiento
 - Como en el momento del propio tratamiento
 - Ejemplos:
 - Seudonimización
 - Minimización de datos
- Garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines
 - Cantidad de datos recogidos
 - Plazo de conservación
 - Accesibilidad

Encargado del tratamiento (Procesador)

- Persona física o jurídica, autoridad pública, agencia u otro organismo que realiza el tratamiento de los datos personales por cuenta del responsable/controlador.
 - No se refiere a un empleado del responsable
- Se debe elegir un encargado que ofrezca garantías suficientes para aplicar medidas apropiadas
- El encargado no puede recurrir a otro encargado sin autorización previa por escrito del responsable

Encargado del tratamiento (Procesador)

- La relación responsable-encargado se registrará por un contrato
 - Objeto
 - Duración
 - Naturaleza
 - Finalidad
 - Tipo de datos personales
 - Categorías de los interesados
 - Obligaciones y derechos del responsable

Encargado del tratamiento (Procesador)

- Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable
- El personal debe comprometerse a respetar la confidencialidad
- Medidas de seguridad en el tratamiento
- Asistirá al responsable con su obligación a responder a las solicitudes de ejercicio de los derechos de los interesados
- Ayudará al responsable con las obligaciones en los artículos 32 a 36
- Suprimirá o devolverá todos los datos personales (elección responsable)
- Pondrá a disposición del responsable la información necesaria sobre el cumplimiento de las obligaciones

Taller: responsables y encargados

Identificar a los responsables y encargados en los casos presentados

20 minutos para discutir los casos en grupos de 3 personas.

Luego discutimos las respuestas entre toda la clase.

Bases legales

Tratamiento lícito de datos personales

Tratamiento lícito de datos personales

- Consentimiento
- Necesario para ejecución de contrato
- Necesario para cumplir una obligación legal
- Necesario para proteger intereses vitales
- Necesario para llevar a cabo una tarea de interés público o en el ejercicio de autoridad oficial
- Necesario para propósitos de intereses legítimos
 - No, en general, para entidades públicas

Interés legítimo y autoridades públicas

- Las autoridades públicas sólo pueden basarse en el interés legítimo si el tratamiento es para una razón legítima distinta de sus tareas como autoridad pública
- Es decir, cuando se realicen funciones distintas de las que se realicen como entidad pública
 - Por ejemplo marketing.

¿Es el interés legítimo un “todo vale”?

- Test en tres etapas:
 - ¿Se trata realmente de un interés legítimo del responsable o de una tercera parte?
 - ¿Es necesario el tratamiento?
 - Balance de los derechos y libertades reconocidas al interesado contra el interés legítimo del responsable o la tercera parte

Taller: bases legales

¿Cuál debe usarse en cada caso?

20 minutos para discutir los casos en grupos de 3 personas.

Luego discutimos las respuestas entre toda la clase.

Derechos

Derechos del interesados y condiciones

Derechos del interesado en el RGPD

- Acceso
- Portabilidad
- Rectificación
- Derecho de supresión (“el derecho al olvido”)
- Limitación del tratamiento
- Derecho de oposición
- Decisiones individuales automatizadas

Reglas similares para todos los derechos

- Respuesta sin dilación indebida y en menos de un mes
 - Puede extenderse otros dos meses
- Gratis
 - A no ser que la petición sea manifiestamente infundada o excesiva
- Respuesta concisa, transparente, inteligible y en un formato accesible
 - Utilizar lenguaje sencillo y claro

Derecho de acceso del interesado

- Derecho a saber si están tratando o no datos personales que le conciernen. Y si es así a saber:
 - Fines del tratamiento
 - Categorías de datos personales
 - Destinatarios o categorías de destinatarios
 - De ser posible, el plazo de conservación,
 - si no, criterios usados para determinar ese plazo
 - Derecho a solicitar del responsable la rectificación, supresión o limitación
 - Derecho a presentar una reclamación
 - La fuente, si no se obtuvieron del interesado
 - La existencia de decisiones automatizadas, incluida la elaboración de perfiles

Derecho de acceso del interesado - Copia

- Se puede solicitar una copia de los datos
 - Se puede pedir un canon por copias repetidas
- Hay excepciones, en particular si se pueden perjudicar los derechos o libertades de terceras personas
 - Datos personales de terceras personas
 - Información sujeta a secreto profesional, etc.

Derecho a la portabilidad de los datos

- Obliga al responsable a proporcionar al interesado sus datos en un formato estructurado, de uso común y lectura mecánica
- El interesado puede transferirlos a otro responsable
 - Directamente de responsable a responsable cuando sea técnicamente posible
- Condiciones:
 - Datos facilitados por el interesado
 - Tratamiento basado en el consentimiento o contrato
 - Tratamiento por medios automatizados

Derecho de Rectificación

- Artículo 16:
 - El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional
- Inexactos o incompletos
- Se suele usar en general para objetar a opiniones
 - No se requiere el cambio de opiniones subjetivas, pero se debe anotar la opinión contraria

Derecho al olvido

- Sólo aplicable a ciertos tipos de información personal y exclusivamente cuando:
 - Los datos ya no son necesarios para el propósito
 - Se ha retirado el consentimiento
 - El interesado objeto y no hay un interés legítimo mayor para continuar con el tratamiento de los datos
 - Los datos se han procesado ilícitamente
 - Los datos deben ser borrados por una obligación legal
 - Datos de redes sociales de un menor

Derecho al olvido

- No aplicable cuando el tratamiento sea de datos relativos a:
 - Razones periodísticas o de libertad de expresión
 - Para cumplir con obligaciones legales o tareas de interés público
 - Salud pública
 - Propósitos de archivo, de investigación científica o histórica
 - Formulación, ejercicio o la defensa de reclamaciones

Limitación del tratamiento

- Exactitud de los datos puesta en duda por el interesado
- El tratamiento es ilícito, pero el interesado no quiere que sean borrados
- El responsable no los necesita más, pero el interesado los quiere para la formulación, ejercicio o defensa de reclamaciones legales
- Se ha objetado al tratamiento, mientras se verifica si los intereses legítimos del responsable prevalecen sobre los del interesado

Evaluación de Impacto

Sección 3 RGPD: Evaluación de impacto relativa a la protección de datos y consulta previa

Evaluación de Impacto (EIPD)

- ¿Qué es?
- Un ejercicio de evaluación de riesgos llevado a cabo por una organización, auditando sus propios procesos, para comprobar como dichos procesos pueden afectar o comprometer la privacidad de los interesados cuyos datos se poseen, adquieren o tratan
- ¿Cuándo hacerla?
 - Nuevo proyecto que recoge datos personales
 - Nuevo sistema informático para almacenar y acceder a información personal
 - Participación en una nueva iniciativa de compartición de datos con otras organizaciones
 - Uso de datos existente para nuevos propósitos, no previsto o más intrusivos

Ejemplos

- Instalación de sistema de circuito cerrado de cámaras
- Compartir datos de empleados con terceros
- Instalación de nuevo software para tratar datos de una categoría especial
- Monitorización de asistencia de estudiantes a clase por nuevos métodos

¿Cómo llevarla a cabo?

- Responder a una serie de preguntas para identificar los riesgos
- Identificar a las partes interesadas
- Consulta con las partes interesadas (internas)
- Consulta con las partes interesadas (externas)
- Análisis de riesgos
- Aprobación

Notificaciones

Requisito de informar

Notificación de violaciones de seguridad

- Requisito de informar ciertas violaciones de la seguridad de los datos personales
 - A la autoridad de control (AEPD o autonómica en su caso) si es probable que se pueda producir un daño a los derechos y libertades de los interesados
 - A los interesados directamente si el riesgo es muy grande
- Dentro de las 72 horas siguientes al descubrimiento
- Obligación de mantener un registro de todas las violaciones de seguridad independientemente de si se han notificado o no

¿Qué constituye una violación de la seguridad de los datos personales?

- Más allá de las pérdidas de datos
- Una violación de la seguridad que conlleve la destrucción, pérdida, alteración, revelación, o acceso no autorizado a datos personales transmitidos, almacenados o tratados de cualquier otra manera
 - Bien sea accidental o malintencionado (ilícito)

Riesgo: probabilidad y severidad

- Probabilidad:
 - Encriptación
 - Copias de seguridad
 - Ataques dirigidos
 - Pérdida de control
- Severidad
 - Datos de categorías especiales
 - Datos financieros
 - Discriminación
 - Pérdida de reputación

Multas

Recursos, responsabilidad y sanciones

Recursos, responsabilidad y sanciones

- Todo interesado tiene derecho a presentar una reclamación ante una autoridad de control
 - Si considera que el tratamiento de datos personales infringe el RGPD
 - Sin perjuicio de cualquier otro recurso administrativo o judicial
- Derecho a la indemnización:
 - Toda persona que sufra daños y perjuicios materiales por una infracción del RGPD
 - Indemnización del responsable o encargado
 - El encargado sólo cuando
 - no haya cumplido con las obligaciones marcadas para ellos en el RGPD
 - O haya actuado al margen o en contra de las instrucciones legales del responsable

Recursos, responsabilidad y sanciones

- Multas administrativas impuestas por la autoridad de control
 - Deben ser efectivas, proporcionadas y disuasorias. Máximo la mayor de
 - 10 millones de euros
 - el 2% del volumen de negocio total anual global (ejercicio anterior)
- Se tendrá en cuenta:
 - Naturaleza, gravedad y duración de la infracción
 - Intencionalidad o negligencia
 - Medidas tomadas para paliar los daños
 - Grado de responsabilidad
 - Toda infracción anterior
 - Grado de cooperación
 - Categorías de datos
 - Notificación (o no)
 - Medidas anteriores aplicadas o no
 - Adhesión a código de conducta

Online pharmacy fined for selling customer data

Online drug seller Pharmacy2U has been fined £130,000 for selling information about customers to marketing companies.

<https://www.bbc.com/news/technology-34570720>





Multas pre-RGPD en RU

- The International Fund for Animal Welfare - £18,000
- Cancer Support UK - £16,000
- Cancer Research UK - £16,000
- Guide Dogs for the Blind Association - £15,000
- Macmillan Cancer Support - £14,000
- The Royal British Legion - £12,000
- The NSPCC - £12,000
- Great Ormond Street Hospital Children's Charity - £11,000
- WWF-UK - £9,000
- Battersea Dogs and Cats Home - £9,000
- Oxfam - £6,000

Multas en la era del RGPD

- Han pasado 2 años y medio desde la entrada en vigor
 - Después de un periodo de ajuste se están empezando a ver más sanciones
- Informe de la firma legal DLS Piper: el pasado año £142.7 millones
 - <https://blogs.dlapiper.com/privacymatters/dla-piper-gdpr-fines-and-data-breach-survey-january-2021/>
 - Un incremento de un 40% con respecto a los 20 meses anteriores. Total £245 millones en la era RGPD.
- Se han notificado 331 violaciones por día.
 - Con grandes diferencias geográficas: Alemania 77747, Italia 3460.
- Ejemplos:
 - Google: 50 millones de euros por el regulador francés.
 - Falta de transparencia
 - British Airways: £20 millones
 - por el robo de datos personales de sus clientes por hackers
 - reducida de £183.4 millones.
 - Marriot £18.4 millones. Misma razón, también reducida.
 - En España, por ejemplo, multa a Caixabank de 6 millones de euros.
 - Más en el portal GDPR enforcement tracker: <https://www.enforcementtracker.com/>

Otras medidas

- Los reguladores pueden decidir suspender completamente las transferencias de datos si se consideran ilegítimas
 - Para algunas compañías esto es todavía más preocupante que las multas
- El año pasado la Corte Europea de Justicia invalidó “privacy shield”
 - Permitía la transferencia de datos personales de ciudadanos de la UE a EEUU
 - Se considera que las leyes de vigilancia gubernamentales presentes en EEUU impiden a las organizaciones proteger los datos personales de una manera compatible con el RGPD

Notificaciones

Requisito de informar

Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

- BOE: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>
 - En vigor desde el 7 de diciembre de 2018
 - Remplaza a la Ley Orgánica 15/1999, de 13 de diciembre
 - Propósitos: adaptar el derecho español al RGPD y garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución
- Estatuto jurídico de la Agencia Española de Protección de Datos como autoridad estatal de control
 - Y las de las CCAA
- Reconoce y garantiza una serie de derechos "digitales" tales como
 - la neutralidad de la Red y su acceso universal,
 - el derecho a la seguridad y a la educación digital,
 - el derecho al olvido,
 - el derecho a la portabilidad de los datos digitales y el testamento digital;
 - siendo igualmente regulado el derecho a la desconexión digital en el marco de las relaciones laborales

Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

- Datos personas fallecidas (acceso, rectificación y supresión)
- Cautelas tratamiento datos de “listas de morosos”
- A fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico
- DPD obligatorio (lista no exhaustiva):
 - Los colegios profesionales
 - Los centros docentes
 - Las entidades que exploten redes y presten servicios de comunicaciones
 - Los prestadores de servicios de la sociedad de la información
 - Establecimientos financieros de crédito, inversión y aseguradoras
 - Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural
 - Los centros sanitarios. Se exceptúan los profesionales de la salud que ejerzan su actividad a título individual
 - Las empresas de seguridad privada.
 - Las federaciones deportivas cuando traten datos de menores de edad.

Sentencia del Tribunal Constitucional

- La disposición final tercera de la Ley añade un nuevo artículo (cincuenta y ocho bis) a la Ley Orgánica del Régimen Electoral General
- permite a los partidos políticos, por considerarlo «amparado por el interés público», recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales siempre y cuando dichas actividades se realicen con «garantías adecuadas».
- Posiblemente amparado por el RGPD
- Agencia Española de Protección de Datos: la Ley no permite la creación de bases de datos ideológicas ni el envío de información personalizada basada en perfiles ideológicos o políticos
- Pero inconstitucional: recurso presentado por el Defensor del Pueblo, sentencia unánime TC del 29 de mayo de 2019

Guías AEPD

- Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción.
- El uso de las tecnologías en la lucha contra el COVID19. Un análisis de costes y beneficios.