Comunicando el RGPD ".con Sentido”
RGPD: un pequeño paso para el hombre... un gran paso para la privacidad

EU-GDPR: New data privacy regulation in the European Union - Impact on EU citizens and organizations (EUpriv8)
611826-EPP-1-2019-1-ES-EPPJMO-PROJECT

https://eupriv8.eu

Co-funded by the Erasmus+ Programme of the European Union

PRIV8

ÍNDICE

- 1. Introducción
- 2. Marco normativo
- 3. Marco General: RGPD
- 4. Ejemplos

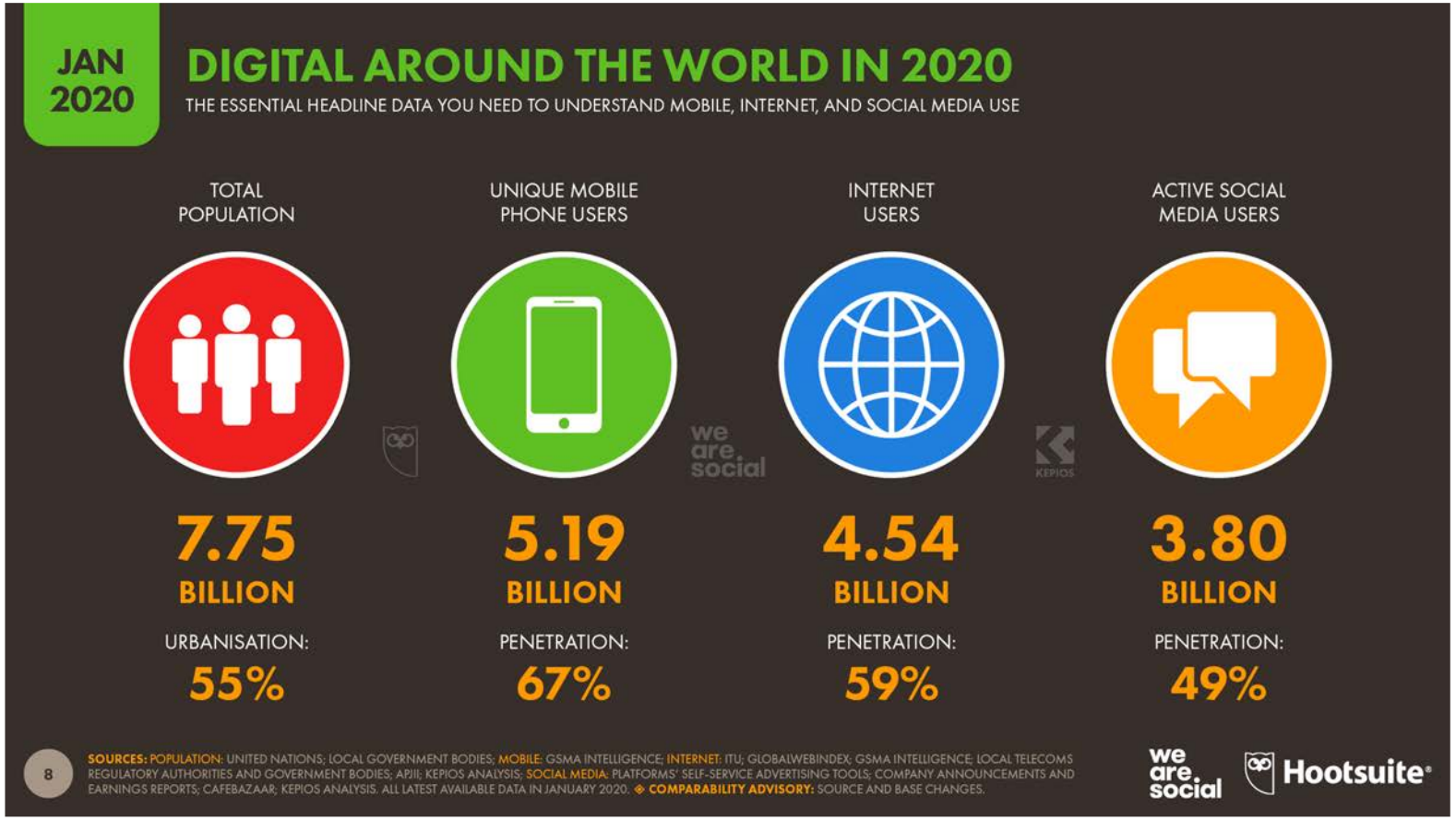
#SNOLAwebinars

Co-funded by the
Erasmus+ Programme
of the European Union

1. Introducción

Co-funded by the
Erasmus+ Programme
of the European Union

1. Introducción - ¿Por qué existe un RGPD?



Co-funded by the Erasmus+ Programme of the European Union

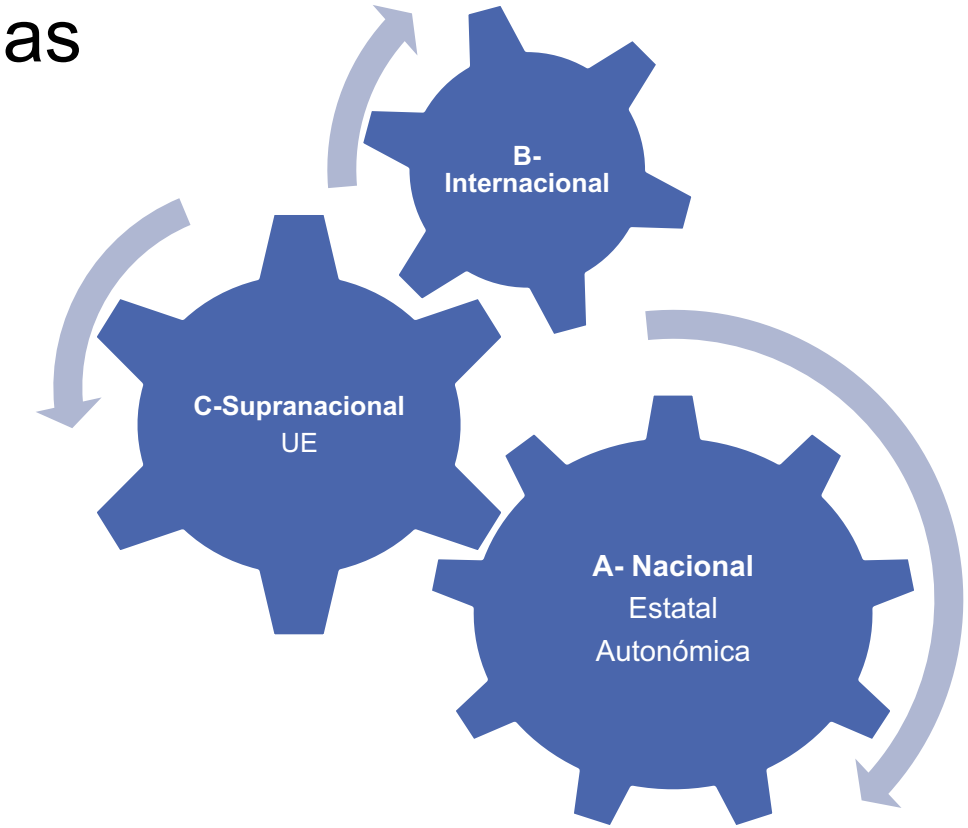
PRIV8

2. Marco normativo

Co-funded by the
Erasmus+ Programme
of the European Union

2. Marco normativo

- Origen
  - Primera Ley de protección de datos en Hesse 1970
- Las realidades normativas conectadas
  - Internacional
  - Supranacional
  - Nacional



Co-funded by the
Erasmus+ Programme
of the European Union

2. Marco normativo nacional

- Marco normativo básico:

Art 18.4 Constitución Española (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 de sus derechos"

Co-funded by the
Erasmus+ Programme
of the European Union

2. Marco normativo nacional

- Marco normativo básico:

  - Ley Orgánica 5/1992. **LORTAD – Libertad Informática**
    - *Regulación del tratamiento automatizado de los datos de carácter persona*
  - Ley Orgánica 15/1999. **LOPD – Derechos ARCO**
    - *Protección de Datos de Carácter Personal*
  - **Ley Orgánica 3/2018. LOPDgdd – Ampliación de derechos (ACTUAL)**
    - *Protección de Datos Personales y garantía de derechos digitales*

  - **Jurisprudencia del Tribunal Constitucional**
    - **254/1993; 144/1999; 292/2000; 58/2018** (Reconocimiento del derecho al olvido)

Co-funded by the Erasmus+ Programme of the European Union

2. Marco normativo nacional

- Otras normas a considerar:

- Reglamento de desarrollo de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y 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 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones;
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica;
- Real Decreto 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones;
- Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera;
- Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo;
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Código electrónico BOE ”Protección de datos de Carácter Personal”

Co-funded by the Erasmus+ Programme of the European Union

3. Marco general del RGPD

Co-funded by the
Erasmus+ Programme
of the European Union

3. Marco general: RGPD

- El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al **tratamiento** de los datos personales y las normas relativas a la libre circulación de tales datos.

- 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.

- La libre **circulación** de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Co-funded by the Erasmus+ Programme of the European Union

3. RGPD ¿Qué se entiende por datos personales?

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***

Co-funded by the Erasmus+ Programme of the European Union

3. RGPD ¿Qué se entiende por datos personales?

- Anónimos y pseudónimos

Los principios de protección que despliega esta normativa **NO se aplican a los datos** que se convierten en **ANÓNIMOS,** ya que el interesado no está identificado ni es identificable.

Rocher, L., Hendrickx, J.M. & de Montjoye, Y. **Estimating the success of re-identifications in incomplete datasets using generative models**.*Nat Commun* **10,** 3069 (2019).

Co-funded by the Erasmus+ Programme of the European Union

3. RGPD ¿Qué se entiende por “tratamiento”?

Operación o conjunto de operaciones con datos personales:

- Recogida
- Registro
- Organización
- Estructuración
- Conservación
- Adaptación
- Extracción
- Consulta
- Utilización
- Difusión
- Cotejo
- Supresión
- Destrucción….

Automatizado
y/o
Manual

Co-funded by the
Erasmus+ Programme
of the European Union

3. RGPD: Ámbito de aplicación material

El Reglamento **se aplica:**

al tratamiento **total o parcialmente automatizado** de datos personales,

al tratamiento **no automatizado** de datos personales contenidos o destinados a ser incluidos en un fichero.

El Reglamento **NO se aplica** al tratamiento de datos personales:

- en el ejercicio de una ***actividad no comprendida en*** **el ámbito de** ***aplicación del Derecho de la Unión****;*
- por parte de los Estados miembros cuando lleven a cabo ***actividades comprendidas en el ámbito de*** aplicación de disposiciones específicas sobre ***la política exterior y de seguridad común;***
- efectuado por una persona física en el ejercicio de ***actividades exclusivamente personales o domésticas;***
- por parte de las autoridades competentes con fines ***de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales***, incluida la de protección frente a amenazas a la seguridad pública y su prevención

Co-funded by the Erasmus+ Programme of the European Union

3. RGPD: Ámbito de aplicación del RGPD

Sujetos afectados

- **Interesado:** persona física a la que se refiere la información
- **Responsable del tratamiento:** quien determina los fines del tratamiento de datos
- **Encargado del tratamiento:** quien "trata" los datos personales por cuenta del responsable. Esto es, quien lleva a cabo las funciones diarias de almacenamiento y procesamiento de datos
- **Destinatario:** a quien se comunican los datos personales
- **Tercero:** quienes no siendo los anteriores "tratan datos personales" bajo la autoridad directa del responsable o del encargado

Co-funded by the
Erasmus+ Programme
of the European Union

3. RGPD – Sistema jurídico de protección

Principios relativos al tratamiento

- Lealtad, licitud y transparencia
- Limitación respecto a la finalidad
- Minimización de los datos
- Exactitud y actualización de los datos
- Integridad y confidencialidad
- Responsabilidad

Co-funded by the
Erasmus+ Programme
of the European Union

3. RGPD – Sistema jurídico de protección

Bases jurídicas para el tratamiento de datos personales

- **Datos “sensibles” - art. 9 RGPD**
  - Afiliación sindical
  - Convicciones religiosas
  - Convicciones filosóficas
  - Origen racial o étnico
  - Datos relativos a la salud
  - Vida sexual
  - Dato genético
  - Dato biométrico
  - Orientación sexual

Co-funded by the Erasmus+ Programme of the European Union

3. RGPD – Sistema jurídico de protección

Bases jurídicas para el tratamiento de datos personales

- **Datos "sensibles" - art. 9 RGPD:**

Prohibición de tratamiento de datos sensibles.

Excepciones a la prohibición

- Consentimiento explícito
- Datos manifiestamente públicos
- Necesario para:
  - el cumplimiento de las obligaciones o el ejercicio de derechos: ámbito laboral, de la seguridad y protección social;
  - proteger intereses vitales del interesado;
  - el ejercicio de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial
  - fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social o gestión de los sistemas y servicios de asistencia sanitaria y social;
- Interés público:
  - Interés público esencial
  - En el ámbito de la salud pública
  - Fines de archivo, investigación científica, histórica o estadística
- Fundación, asociación u otro organismo sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical

Co-funded by the Erasmus+ Programme of the European Union

3. RGPD: Técnicas para el adecuado cumplimiento

Derechos de los interesados

- Transparencia
- Información
- Acceso
- Rectificación
- Cancelación/Supresión/Olvido
- Oposición
- Limitación del tratamiento
- Portabilidad

Guía AEPD para el Ciudadano:

Co-funded by the Erasmus+ Programme of the European Union

3. RGPD: Técnicas para el adecuado cumplimiento

Obligaciones de los responsables y agentes

- Registro de actividades de tratamiento
- Legitimación del tratamiento
- Información y consentimiento
- Análisis de riesgos y evaluación de impactos
- Privacidad en el diseño y por defecto
- Control de proveedores
- Seguridad
- Delegado de protección de datos

Co-funded by the
Erasmus+ Programme
of the European Union

3. RGPD: Técnicas para el adecuado cumplimiento

c) Las autoridades de control:

- Supervisor Europeo de protección de datos
- Comité Europeo de protección de datos
- La Agencia Española de Protección de Datos
- Autoridades autonómicas

Co-funded by the
Erasmus+ Programme
of the European Union

3. RGPD: Régimen de infracciones y sanciones

- **Infracciones**
  - Muy Graves
    - Graves
      - Leves

¿Quiénes pueden ser sancionados?

- Responsable del tratamiento
- Encargado del tratamiento
- Representante del responsable/ encargado no establecidos en la UE
- Entidades de certificación
- Entidades acreditadas de supervisar códigos de conducta

Co-funded by the
Erasmus+ Programme
of the European Union

3. RGPD: Régimen de infracciones y sanciones

- **Sanciones**

Multas:

Primer Nivel:

2% del volumen de ingreso anual de la empresa, o 10 millones de euros, el que sea mayor. Esto se aplicará, por ejemplo, en situaciones en las que la empresa no pueda demostrar una seguridad adecuada, no haya designado un delegado de protección de datos o no haya establecido un acuerdo sobre el procesador de datos.

Segundo Nivel:

4% del volumen de ingreso anual de la empresa, o 20 millones de euros, el que sea mayor. Esta multa se aplica si se han infringido los derechos de los sujetos de datos, como la situación en la que se procesaron sus datos sin una base jurídica.

Otras:

Advertencia, apercibimiento, requerimiento de atención, ordenar que las operaciones de tratamiento se ajusten a las previsiones exigidas, obligación de comunicar al interesado las violaciones de seguridad de los datos personales, limitación temporal o definitiva del tratamiento de datos, ordenar la rectificación o supresión, retirar la certificación, ordenar la suspensión de los flujos de datos hacia un destinatario...

Cuadro sanciones RGPD

Co-funded by the Erasmus+ Programme of the European Union

4. Ejemplos

Co-funded by the
Erasmus+ Programme
of the European Union

RGPD Privacidad desde el Diseño

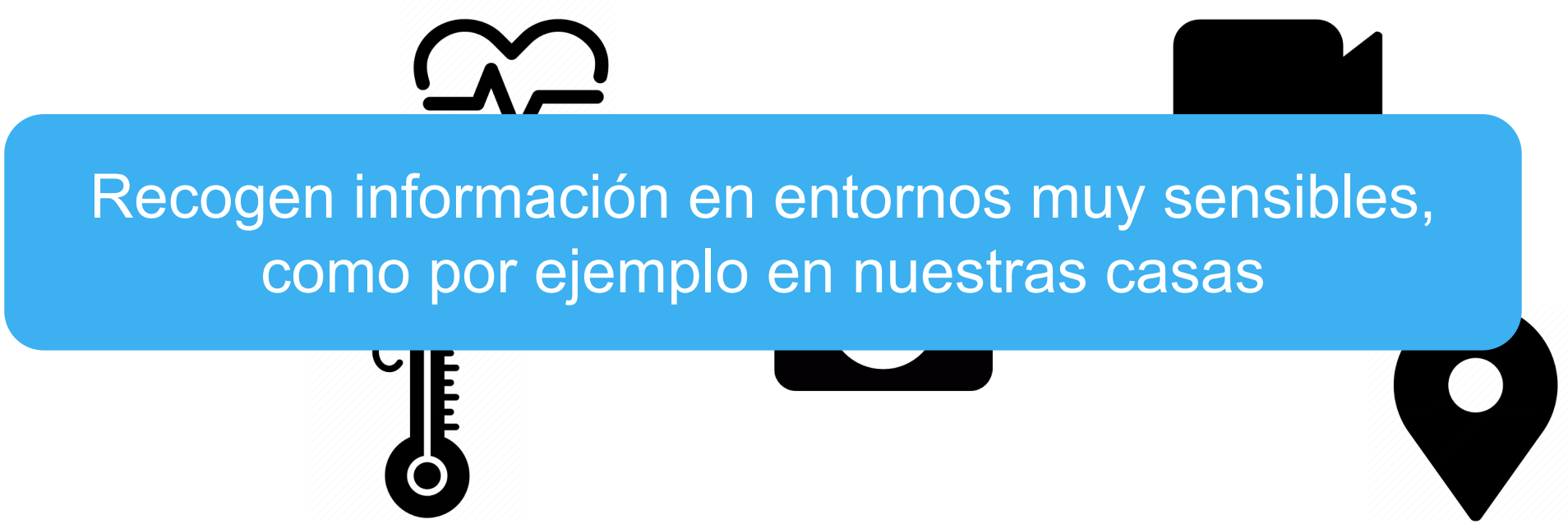
Implica un enfoque en el desarrollo software orientado a la gestión de riesgos y la rendición de cuentas (*Accountability*)

Conlleva establecer estrategias que incorporen la protección de la privacidad a lo largo del ciclo de vida de un objeto (ya sea un sistema, un producto de hardware o software, un servicio o un proceso).

Co-funded by the
Erasmus+ Programme
of the European Union

RGPD en IoT

Sensores recolectando información del entorno 24/7



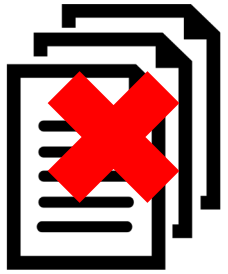
Recogen información en entornos muy sensibles, como por ejemplo en nuestras casas

Co-funded by the Erasmus+ Programme of the European Union

RGPD en IoT

El problema del consentimiento

Términos y Condiciones



¿El sujeto sabe que se recolectan sus datos?

Todavía es un reto a día de hoy solicitar el consentimiento, ya que el RGPD obliga a contar con él

Co-funded by the Erasmus+ Programme of the European Union

RGPD en IoT

Uso mínimo de datos

Sólo se pueden recabar aquellos datos que tengan un propósito determinado

¿Qué ocurre con los datos que se recaban de forma continua?

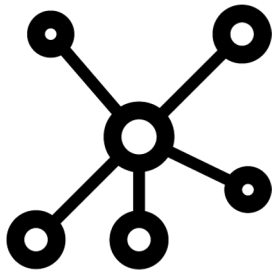
Co-funded by the
Erasmus+ Programme
of the European Union

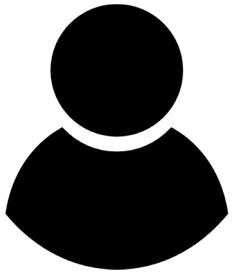
RGPD en IoT

Ejecutar los derechos de los sujetos

Las redes de dispositivos conectados en IoT es muy compleja y los datos se comparten

Quiero ejercer mis derechos





Debemos ser capaces de realizar un seguimiento de los datos para ofrecer transparencia y ser capaces de modificarlos, recopilarlos, borrarlos, etc.

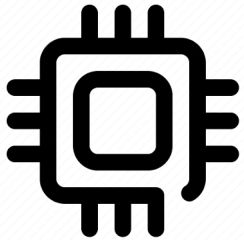
Co-funded by the Erasmus+ Programme of the European Union

RGPD en IoT

Las limitaciones de los dispositivos en IoT

Según el RGPD, se deben implementar mecanismos que preserven la seguridad y privacidad de los datos

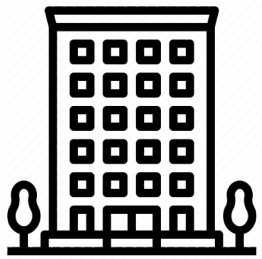
Sin embargo, estos dispositivos tienen un hardware limitado que dificulta implementar este tipo de mecanismos



Co-funded by the Erasmus+ Programme of the European Union

RGPD en Cloud Computing

Data Controllers
(Responsables)



Data Processors
(Encargados)

Co-funded by the
Erasmus+ Programme
of the European Union

RGPD en Cloud Computing

El RGPD aplica aunque los datos se almacenen fuera de la UE mientras los datos pertenezcan a sujetos de la UE

Tanto los responsables como los encargados tienen responsabilidades según el RGPD

Co-funded by the
Erasmus+ Programme
of the European Union

RGPD en Cloud Computing

Si se procesan datos de más de 5.000 sujetos durante más de 12 meses

Contar con Data Protection Officers (Delegado de Protección de Datos)

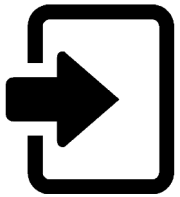
Propio o subcontratado

Co-funded by the Erasmus+ Programme of the European Union

RGPD en Cloud Computing

¿Qué obligaciones tenemos con los sujetos como responsables?

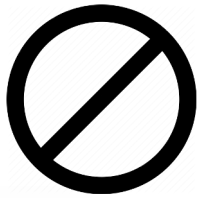
Derecho de acceso



Derecho de rectificación

Derecho al borrado

Derecho de restricción



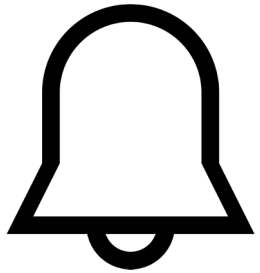
Derecho de portabilidad

Co-funded by the
Erasmus+ Programme
of the European Union

RGPD en Cloud Computing

¿Y si ocurre algo con los datos?

Notificar las brechas cuanto antes (máximo 72 horas)

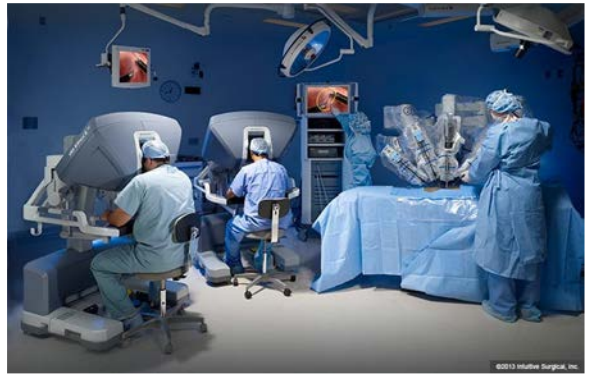


Brechas por negligencia
Sanciones

Co-funded by the Erasmus+ Programme of the European Union

RGPD en Robótica

Implicaciones legales, regulatorias y éticas de los robots y otros sistemas autónomos en la ley del RGPD.



Co-funded by the Erasmus+ Programme of the European Union

Source1: https://asia.nikkei.com/Business/Startups/Self-driving-cars-face-long-road-despite-industry-raising-35bn
Source2: Dereshev, Dmitry. (2019). SMART WONDER: CUTE, HELPFUL, SECURE DOMESTIC SOCIAL ROBOTS.
Source3: https://www.aarp.org/health/conditions-treatments/info-12-2013/robotic-surgery-risks-benefits.html

RGPD en Robots de Compañía

Comportamiento similar al IoT, pero además se mueven

Co-funded by the Erasmus+ Programme of the European Union

Source2: Dereshev, Dmitry. (2019). SMART WONDER: CUTE, HELPFUL, SECURE DOMESTIC SOCIAL ROBOTS.
Source3: https://www.aarp.org/health/conditions-treatments/info-12-2013/robotic-surgery-risks-benefits.html

PRIV8

Inteligencia Artificial (en inglés, AI)

- AI = conjunto de tecnologías y/o sistemas que permiten a un ordenador **emular la inteligencia humana**,
  - incluida la toma de decisiones o el aprendizaje.
- Para ello, es necesario recopilar una **gran cantidad de información** (Big Data),
  - incluyendo datos personales.
- Según algunos estudios*…
  - El 80% de los ejecutivos opina que la AI aumenta la productividad.
  - A medio plazo, los ejecutivos creen que se podrá usar la AI para aliviar tareas repetitivas, como…
    - el papeleo (82%),
    - la planificación (79%)
    - y la asignación/gestión de horarios (78%).
  - En 2025, se estima que el mercado de la inteligencia artificial superará los 100.000 millones de dólares.

*.- https://cmo.adobe.com/articles/2017/8/15-mindblowing-stats-about-artificial-intelligence-dmexco.html#gs.zd1500

Co-funded by the Erasmus+ Programme of the European Union

AI eXplicable (XAI)

- XAI = métodos y técnicas en la aplicación de AI que permiten que sus resultados **sean entendidos por expertos**.
  - XAI es una forma de hacer cumplir con el **derecho a la información**.
- Entendido, pero...
  - ¿Cómo abordamos el **compromiso** entre **privacidad y AI+XAI**?

Co-funded by the
Erasmus+ Programme
of the European Union

RGPD y XAI

- El RGPD aplica a la AI cuando esta se desarrolla **utilizando datos personales** y también cuando se utiliza para **analizar o tomar decisiones sobre personas**.
  - El artículo 22 establece que "*el interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que tenga efectos jurídicos en él o que le afecte de forma significativa*".
  - Los artículos 13 y 15 establecen que los interesados tienen derecho a "*información significativa sobre la lógica implicada*" y "*las consecuencias previstas*" de la toma de decisiones automatizada.
- La regulación espera que la AI se desarrolle siguiendo estos principios:
  - **justicia**,
  - **limitación de propósito**,
  - **minimización de datos**,
  - **transparencia**, y
  - el **derecho a la información**.
- Pero hay un problema… la mayoría de los sistemas de toma de decisiones son **cajas negras**.

Co-funded by the Erasmus+ Programme of the European Union