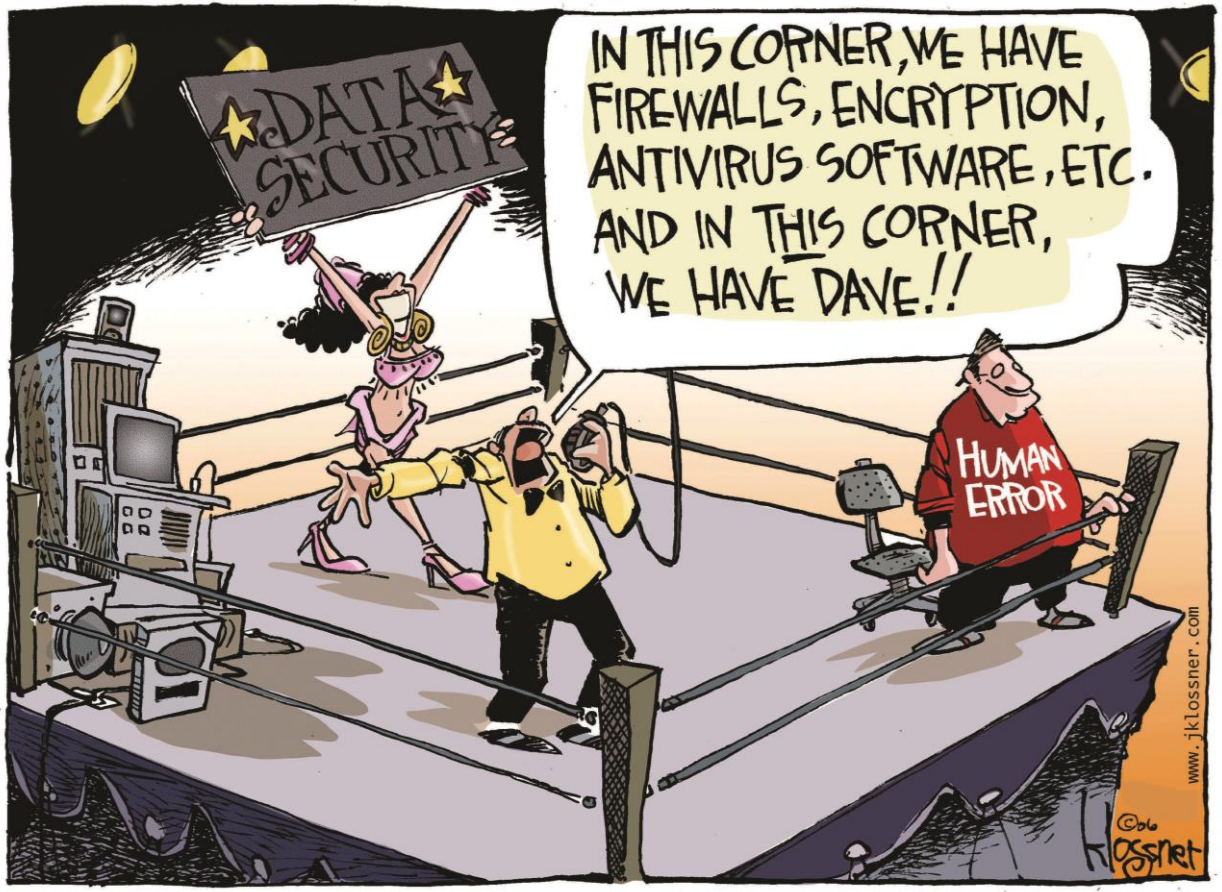

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

REGLAMENT GENERAL DE PROTECCIÓ DE DADES

"... des de el passat 25 de maig de 2018, la Unió Europea s'ha convertit en un gran ***ecosistema de respecte reforçat*** *de los dades personals i, per tant, de la privacitat del ciutadà"**

* Jorge García Herrero, advocat

FULL DE RUTA

INTRODUCCIÓ

De què parlem?

On estem?
Què ha passat?

BREU RESUM RGPD I LOPD-GDD

Nous principis

Conceptes

Mesures de seguretat

BRETXES DE SEGURETAT

Concepte

Responsabilitat

Principis SI

Art. 32 RGPD

Noves obligacions

CONCLUSIONS

Responsabilitat proactiva

Enginyers & Advocats

DE QUÉ PARLEM?

Protecció de dades > Privacitat > Protecció de les persones

LA QÜESTIÓ ...

Protección de Datos resuelve que es ilegal incluir a personas en grupos de WhatsApp sin su consentimiento

La decisión afecta a las administraciones públicas, pero no a quienes agreguen a sus familiares y amigos

Protección de Datos sanciona a Whatsapp y Facebook por ceder y tratar datos perso

- El regulador español impone 600.000 euros de sanción por no aj
  factores como el número de tratamientos, el volumen de negoci
  tratamientos de datos de carácter personal

Sanción a Google por captar sin consentimiento datos personales

- La Agencia de Protección de Datos le impone una multa de 300.000 euros
- Recogió datos de usuarios con redes abiertas a través de su servicio Street View

≡ EL PAÍS TECNOLOGIA

FACEBOOK

Una fuga de dades de Facebook causa una tempesta política mundial

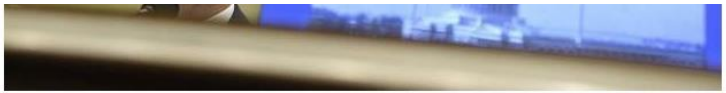
Polítics dels EUA i el Regne Unit reclamen que Zucke que una consultora electoral va manipular informació de

INTRODUCCIÓ

INTRODUCCIÓ

Exemples

¡Nuevos Derechos digitales!



Mark Zuckerberg durante su comparecencia en el congreso de EE UU tras el escándalo Cambridge Analytica. / AFP

detect deepfakes

INTRODUCCIÓ

On estem?

- Producció legislativa amb retard
  - RGPD: Entrada en vigor 2016 / aplicació maig 2018 / LOPD-GDD novembre 2018
- Adequació desigual
  - Aprovat just a grans empreses i administracions
  - Necessita millorar en pimes i administracions locals
- Adequacions força deficients o directament inacceptables
  - Petició de consentiment / Interès legítim / Texts web sense adequació / ...

INTRODUCCIÓ

Novetats LOPD-GDD - #NoConMisDatos

- Article 58bis. Utilització de mitjans tecnològics i dades personals en les activitats electorals
  - Tots els partits tindran **llibertat quasi absoluta** per recollir dades de pàgines web i RRSS
  - Podran crear **bases de dades ideològiques** partint de la informació recollida
  - Podran enviar "**spam**" sense que passi com a correu comercial
  - I perquè sigui legal, només necessiten complir unes **garanties bàsiques** encara no determinades

INTRODUCCIÓ

Novetats LOPD-GDD – Nous Drets Digitals

- Neutralitat a Internet
- Accés universal a Internet
- Seguretat digital
- Educació digital
- Protecció dels menors
- Dret de rectificació
- Dret actualització informació en mitjans de comunicació digital
- Dret a l'oblit (recerques i RRSS)
- Portabilitat
- Testament digital

- En l'àmbit laboral
  - Intimitat / ús dispositius digitals
  - Dret a la desconnexió digital
  - Intimitat / ús videovigilància
  - Intimitat / sistemes geolocalització
  - Dret digital en la negociació col·lectiva

INTRODUCCIÓ

Què ha passat?

Gestió Notificacions i Violacions de Seguretat, des de l'APDCAT*

* Carles San José, Cap Àrea d'Inspecció APDCAT

CONCEPTES BÀSICS RGPD

RGPD: LEGAL & TECNOLÒGIC

Un nou paradigma

*"L'adequació al nou Reglament ha deixat de ser un tema **únicament** jurídic"**

OBLIGACIONS DE CONTINGUT JURÍDIC
Compliment definit en el Reglament

OBLIGACIONS ORGANITZATIVES
Polítiques Seguretat de la Informació

OBLIGACIONS RELATIVES A MESURES TÈCNIQUES I DE SEGURETAT
Identificació
Salvaguarda

* Percentatges excloent contingut general i directrius. Font: X. Ribas / Pròpia

NOUS PRINCIPIS RGPD

Un nou paradigma

*"Som responsables del **100%** de l'adequació"*

Responsabilitat proactiva

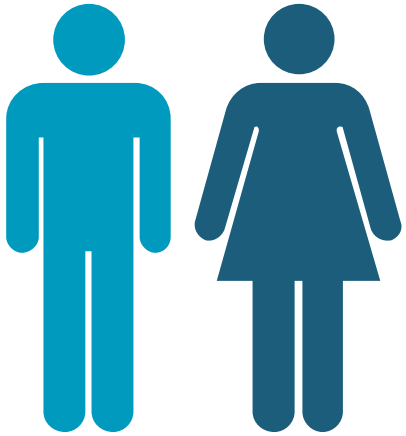
Avaluació de Risc / Avaluació d'Impacte

Des del principi / Minimitzar les dades

QUÈ SÓN DADES PERSONALS?

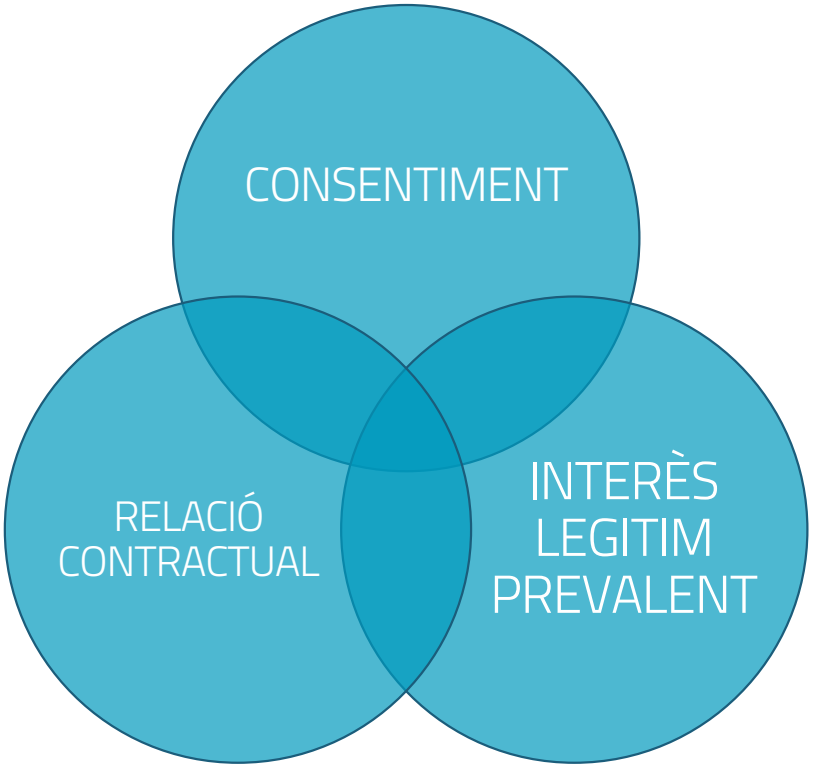
Dades que permeten identificar, directa o indirectament, a una persona física

- Nombre
- Adreça
- Localització
- Identificador en línia
- Informació sanitària
- Ingressos
- Perfil cultural
- IP
- ...



BASES DE LEGITIMACIÓ

Legitimació per el tractament



- Consentiment
- Relació contractual
- Interès legítim prevalent del RT
- Interessos vitals de l'interessat/da
- Obligació legal
- Interès públic

EL DRET A LA INFORMACIÓ

Informació que ens han de comunicar quan demanen dades personals (Article 13 RGPD)

- Base jurídica (legitimació)
- Temps màxim de conservació
- Identificació del DPD
- Transferències internacionals
- Decisions automatitzades
- Dret a reclamar

I si les dades no procedeixen del interessat:

- Origen
- Categoria

NOUS DRETS

D'ARCO a ARCOPOL

"Nous drets que millorin la capacitat de decisió i control dels ciutadans sobre les seves dades personals."

- Accés
- Rectificació
- Supressió (cancel·lació)
- Oposició (i oposició a perfil)
- **Portabilitat**
- **Dret a l'oblit** (Internet)
- **Limitació del tractament**

TIPUS DE DADES

- **Bàsics** (identificatius): Nombre, direcció, correu, ...
- **Categoria especial** (sensibles): raça, orientació política o sexual, afiliació sindical, religió, salut, penals (antecedents i condemnes) ...

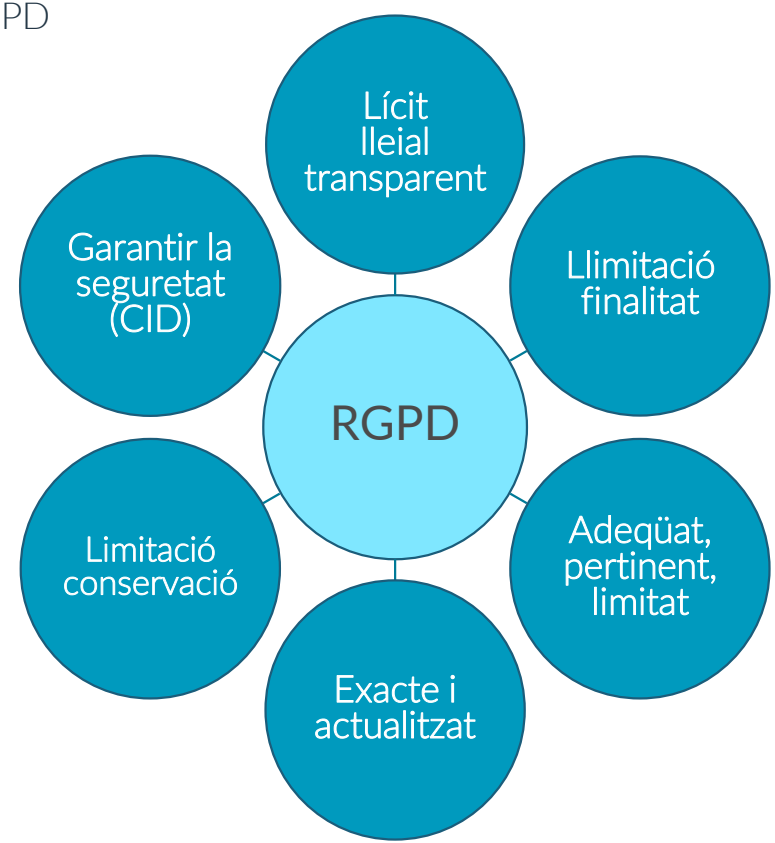
Noves categories de dades especials

- Dades **genètiques**
- Dades **biomètriques** *(empremta dactilar, iris, reconeixement facial, ...)*

PRINCIPIS DE TRACTAMENT

Article 5 RGPD

- Tractament: qualsevol operació realitzada sobre dades personals com recollida, registre, organització, conservació, comunicació, modificació, difusió, ...



REGISTRE D'ACTIVITATS DE TRACTAMENT

De la inscripció del fitxer a l'AEPD al Registre d'Activitats (Artícle 30 RGPD)

- L'obligació de inscriure els fitxers en l'AEPD se ha substituït per el Registre d'Activitats de Tractaments (RAT)

Estructura fitxer + **Auditoria RGPD** + **Estructura tècnica i organitzativa**

Finalitats / Origen dades / Categories interessats / Dades identificatives / Dades especials / Sistema tractament / ...

Principis de tractament / Responsabilitat / Política de informació / Política de seguretat / Mesures de protecció / ...

Departaments / Hardware / Software / Suports / Mobiliari / Usuaris / Encarregats de tractament / ...

Relació Responsables – Encarregats de Tractament

- Contracte entre les parts / El Responsable determina el què i el com

EL COST DE L'INCOMPLIMENT (RGPD)

Pot ser força elevat

- Advertència
- Amonestació
- Suspensió del tractament de dades
- Multa
  - Fins a 10 M EUR o 2% de la facturació anual del grup
    - *No consentiment menors / no disposar de RAT / No notificar violació de seguretat / No fer l'EIPD / ...*
  - Fins a 20 M EUR o 4% de la facturació anual del grup
    - *No complir principis RGPD / drets interessats / transferències internacionals / ...*

Facebook se enfrenta a una multa de 1.400 millones de euros por su nueva brecha de seguridad

- Una nueva vulnerabilidad detectada deja expuestas a más 50 millones de cuentas y otras 40 en cuarentena
- La Agencia Española de Protección de Datos va a colaborar con la autoridad irlandesa para ver si hubieran podido verse afectados datos de ciudadanos españoles

Mark Zuckerberg, fundador de Facebook, en una imagen de archivo - ZUMA Press

EL COST DE L'INCOMPLIMENT (MERCAT)

Pot ser encara més elevat

- Dany **reputacional** (pèrdua de confiança)
- Caiguda **valor** de la companyia
- Pèrdua **usuaris** / afiliats
- Descens de les **vendes**

Aviones de la flota de British Airways. Reuters

EMPRESAS

IAG se deja más de un 2% en Bolsa tras la brecha de seguridad en British Airways

BRETXES DE SEGURETAT

INTRODUCCIÓ

Exemples

Technology Intelligence

Uber to pay $148m for data breach cover-up

share

Save

Uber knew about the hack a year before it disclosed it CREDIT: REUTERS

BRETXES DE SEGURETAT

Conceptes

- Incident de seguretat: succés inesperat o no desitjat, en detriment de la seguretat del Sistema d'Informació
- Bretxa de seguretat: incident de seguretat que
  - Afecta a dades de caràcter personal
  - Pot comprometre al responsable del tractament, en compliment dels principis del RGPD.

- El RGPD les defineix com "les violacions de seguretat que ocasionin la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altre forma, o la comunicació o accés no autoritzat a aquestes dades".

BRETXES DE SEGURETAT

Responsabilitat en el RGPD

- Article 5.1.f Principis relatius al tractament
  - Les dades personals (...) seran tractades de manera que es garanteixi una seguretat adequada (...) mitjançant l'aplicació de mesures tècniques o organitzatives apropiades ("integritat i confidencialitat")
- 2.El responsable del tractament serà responsable del compliment i capaç de demostrar-ho ("responsabilitat proactiva")

BRETXES DE SEGURETAT

Seguretat de la Informació – Principis i tècniques

- Confidencialitat
  - Seudonimització / Criptografia / Gestió de identitats / Control d'accés
- Integritat
  - Gestió de continguts / Gestió de canvis / Firma digital / Funcions *hash*
- Disponibilitat
  - Replicació / Sincronització / Alta disponibilitat
- Resiliència
  - Gestió de crisis / Plans de Contingència i Continuïtat / Backup

BRETXES DE SEGURETAT

Mesures tècniques i organitzatives – Art. 32 RGPD Seguretat del Tractament

- Seudonimització i **xifrat** de dades personals
- Capacitat de garantir la **Confidencialitat**, **Integritat**, **Disponibilitat** i Resiliència permanents dels sistemes i serveis de tractament.
- Capacitat de restaurar la **disponibilitat** i **l'accés** a dades personals en cas d'incident físic o tècnic
- Procés de **verificació**, **avaluació** i **valoració** regulars de l'eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.

BRETXES DE SEGURETAT

Noves obligacions

- Mecanisme de notificació de incompliments
  - A l'Autoritat de Control
    - Abans de 72 hores des del coneixement de la violació
    - La notificació inclourà:
      - la naturalesa de la violació, categories i nombre aproximat d'afectats, nom del DPD, conseqüències, mesures adoptades per remeiar i mitigar els efectes negatius
      - Es documentarà amb la relació dels fets, els efectes i les mesures correctores
  - Als usuaris afectats
    - Quan hi hagi un risc elevat per els drets i llibertats de les persones físiques
    - Es faran excepcions quan s'hagin adoptat les mesures apropiades o suposi un esforç desproporcionat, entre altres

CONCLUSIONS

CONCLUSIONS

Responsabilitat proactiva

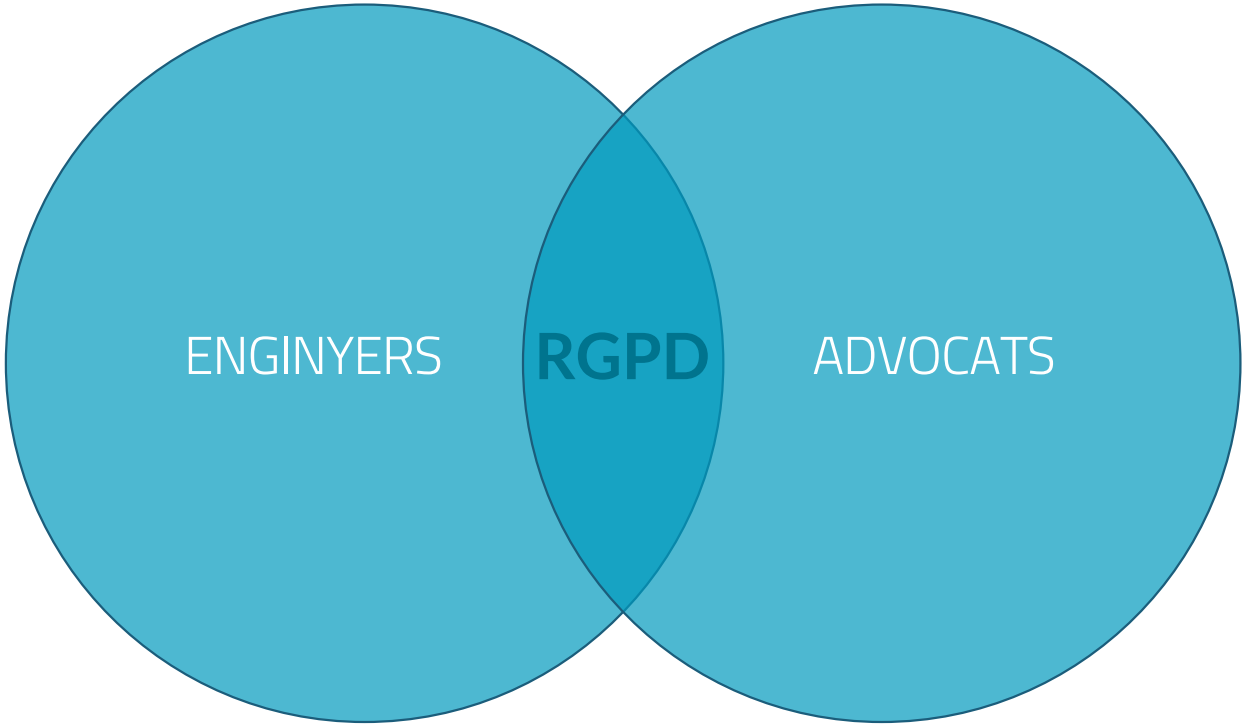
- Hem d'avaluar els riscos
- Cal garantir la seguretat de les dades personals mitjançant l'aplicació de mesures organitzatives i tècniques apropiades
- El responsable del tractament serà responsable del compliment i capaç de demostrar-ho
- El cost del incompliment és elevat

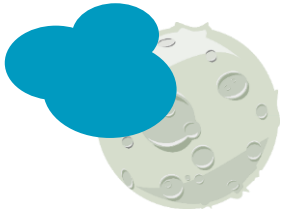
CONCLUSIONS

Enginyers & Advocats

- Oportunitats en Mercat en creixement
- Responsabilitat professional
  - Treball conjunt
  - Oportunitats creuades
- Noves fites professionals
  - RGPD
  - Seguretat de la Informació

CONDEMNATS A ENTENDRE'NS





Gràcies!

Ricard Castellet
M. 607 505 305
rcastellet@tecnolawyer.com
tecnolawyer.com