

# REGLAMENT GENERAL DE PROTECCIÓ DE DADES



*“... la Unió Europea es convertirà, el proper 25 de maig de 2018, en un gran **ecosistema de respecte reforçat** de les dades personals i de la privacitat del ciutadà”\**

# 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 personales

- El regulador español impone 600.000 euros de sanción por no ajustar factores como el número de tratamientos, el volumen de negocios y los 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

FACEBOOK

## Una fuga de dades de Facebook causa una tempesta política mundial

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

TECNOLOGIA

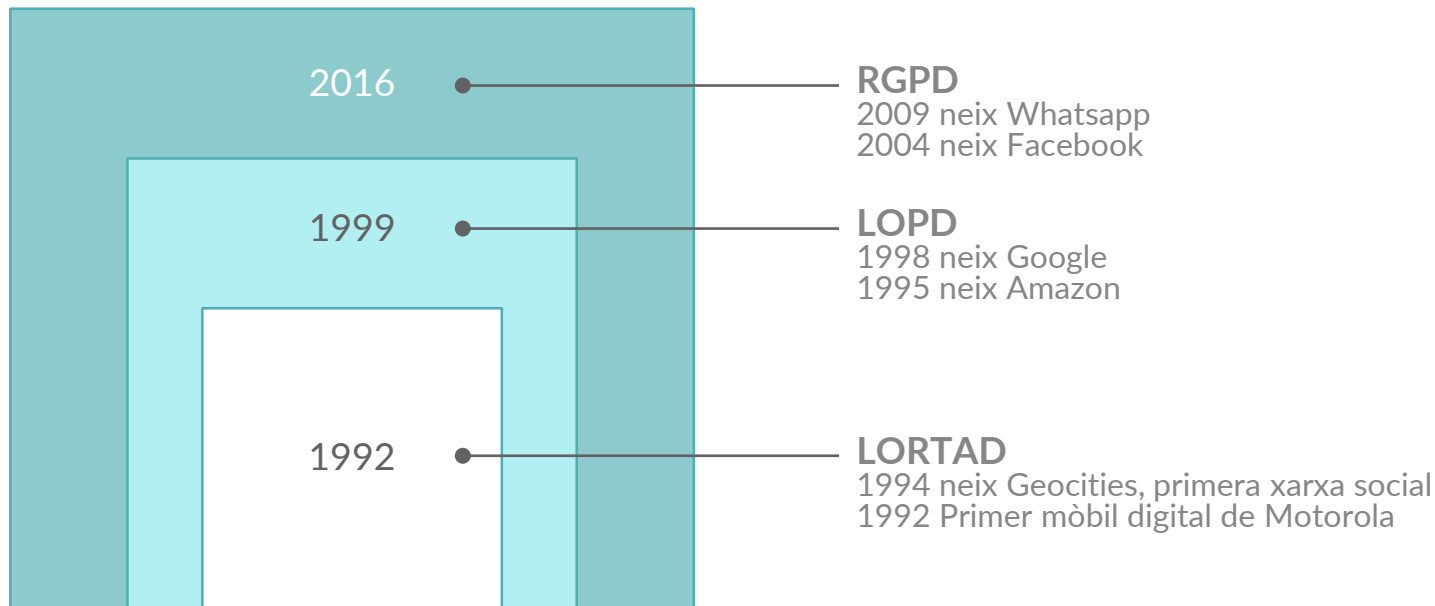
que



# RGPD: Introducció

# D'ON VENIM?

Més de 25 anys de protecció de dades



# PERQUÈ UN NOU REGLAMENT?

*Un nou paradigma*

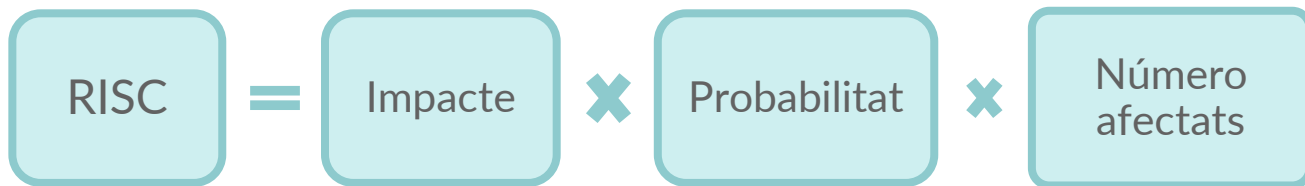
*“Es tracta d’una aposta de **generació de valor** a llarg termini, buscant la fidelització de l’usuari a base de tractar-lo el millor possible en termes de privacitat”\**

- Preservar els drets i les llibertats: donar resposta als **nous riscos**
- Tornar el control de la privacitat a l’usuari: l’interessat és **sobirà** de les seves dades
- Afavorir el tràfic econòmic: el nou model genera més **confiança** perquè es basa en principis de licitud, lleialtat i transparència

# NOUS PRINCIPIS

*Inspiradors del nou RGPD – Un nou paradigma en la PD*

- Accountability (responsabilitat proactiva): poder **acreditar** el compliment de les obligacions relatives al tractament de les dades
- Enfoc al risc: tot tractament comporta un risc, cal **avaluar-lo** i prendre les mesures oportunes per mitigar-lo



- Privacy by Design / by Default: implementar mesures tècniques i organitzatives **des de l'inici** que demostrï que hem integrat la protecció de dades en els processos de l'organització i que només tractem les dades necessàries

# CONCEPTES BÀSICS

## Article 4 RGPD

- Dada personal: tota informació sobre una **persona física** identificada o identificable
- Categoria especial de dades: dades sensibles amb protecció addicional (p.e., salut)
- Tractament: qualsevol **operació** realitzada sobre dades personals com recollida, registre, organització, comunicació, consulta, modificació, difusió, ...
- Consentiment: manifestació de voluntat lliure, específica, informada e inequívoca per la que l'interessat accepta, amb una **clara acció afirmativa**, el tractament de les seves dades
- Responsable de tractament: persona física o jurídica, autoritat pública, servei o organisme que **determini** les finalitats i mitjans del tractament
- Encarregat del tractament: persona física o jurídica, autoritat pública, servei o organisme que tracti dades personals **per compte** del responsable del tractament

# RESPECTE PER LES DADES

*Tractament respectuós de les dades personals (Article 5 RGPD)*

- Licitud, lleialtat i transparència: en relació a l'interessat
- Limitació de la finalitat: finalitats determinades, explícites i legítimes
- Minimització: adequats, pertinents i limitats a la finalitat
- Exactitud: actualització de les dades
- Limitació de conservació: durant el temps estrictament necessari per el tractament
- Integritat i confidencialitat: garantir la inalterabilitat de les dades i impedir l'accés de tercers no autoritzats



# NOVES CATEGORIES ESPECIALS DE DADES

*Tractament de categories especials (Article 9 RGPD)*

## Fins ara

Origen ètnic o racial, opinió política, conviccions religioses, afiliació sindical, salut, orientació sexual, ...

## Ara afegim

- Dades **genètiques**
- Dades **biomètriques**

# RGPD: Principals novetats

# BASE DE LEGITIMACIÓ

Justificar la base de legitimació per el tractament

- Consentiment
- Relació contractual
- Interessos vitals del interessat
- Obligació legal
- Interès públic
- **Interès legítim prevalent** del responsable

# EL CONSENTIMENT

Obtenir el consentiment de **forma vàlida** (Article 7 RGPD)

*“Hem de ser capaços de **demostrar** positivament que l'interessat va consentir el tractament de les seves dades personals”*

- Consentiment **lliure, específic, informat i inequívoc**
- Per dades de categoria especial, necessitem consentiment **exprés** (article 9 RGPD)
- La sol·licitud s'ha de **distingir** d'altres assumptes
- **Avaluar** la llibertat alhora de donar el consentiment
- L'interessat ha de poder **retirar** el consentiment de forma fàcil en qualsevol moment
- Menors de 13 anys necessiten autorització titular pàtria potestat

# EL DRET D' INFORMACIÓ

Informació que ha de ser comunicada alhora de demanar dades personals (Article 13 RGPD)

- La base jurídica del tractament (legitimació)
- El temps màxim que es mantindran les dades
- La identificació, si procedeix, del Delegat de Protecció de dades
- Si hi haurà o no transferència internacional de dades
- El dret a presentar una reclamació
- La existència o no de decisions automatitzades

I si les dades no provenen del interessat:

- L'origen de les dades
- La categoria de les dades

# NOUS DRETS

D'ARCO a ARCOPOL

*“Nous drets que milloren la capacitat de **decisió i control** dels ciutadans sobre les seves dades personals”*

- Accés
- Rectificació
- Cancel·lació
- Oposició
- Portabilitat de les dades
- Dret a l'oblit
- Limitació del tractament

# REGISTRE D'ACTIVITATS DE TRACTAMENT

De la inscripció de fitxer al Registre d'Activitats (Article 30 RGPD)

- L'obligació de inscriure els fitxers a l'AEPD s'ha substituït per el Registre d'Activitats de Tractaments (**RAT**)
- Ha de incloure les dades que es recullen, la finalitat del tractament, a qui es comuniquen, descripció de les categories, les mesures tècniques i organitzatives adoptades, ...
- A la pràctica és aplicable a tothom perquè tot tractament pot suposar un risc per els drets i llibertats dels interessats (Article 30.5 RGPD)

# L'AIP (PIA)

L'Avaluació d'Impacte, un exercici d'anàlisi dels riscos (Article 35 RGPD)

*“Quan un tractament suposi un **alt risc** per els drets i llibertats es farà una AIPD”*

## Finalitats de l'AIP

- Descriure els tractaments i finalitat
- Avaluació de la necessitat, proporcionalitat i idoneïtat
- Identificar i Gestionar els riscos

## Quan és necessari?

- Quan es recullen dades de categoria especial (salut, penals, racials, genètiques, biomètriques, geolocalització, ...), s'elaboren perfils o dades de menors
- Quan es fan tractaments a *gran escala* de dades sensibles



# LA FIGURA DEL DPO

El Delegat de Protecció de Dades

*“El DPO és l'enllaç entre l'organització i l'autoritat de control”*

## Què és la figura de DPO?

- Assessora a responsables / encarregats de tractament sobre normativa i AIPD
- Supervisa el compliment normatiu
- Atenció consultes interessats sobre tractament o exercici de drets

## Quan és necessari?

- Autoritats o Organismes Públics
- El tractament suposa una observació habitual y sistemàtica a gran escala
- Tractament de dades especials, menors o personals referits a condemnes o delictes

# SEGURETAT DE LES DADES PERSONALS

- El Responsable i l'Encarregat aplicaran mesures tècniques i organitzatives que garanteixin un nivell de seguretat adequat al risc.
- **Seudonimització** i xifrat de dades personals
- Garantir la confidencialitat, integritat, disponibilitat i **resiliència** dels sistemes i serveis de tractament
- Capacitat de restaurar la disponibilitat i l'accés a les dades en cas d'incident
- Procés de verificació, avaluació y valoració de l'eficàcia de les mesures

# NOTIFICACIÓ VIOLACIÓ DE **SEGURETAT**

Les **bretxes** de seguretat

*“El RGPD ens obliga a comunicar si les dades personals han estat **compromeses** i constitueix un risc per els drets i llibertats de les persones físiques”*

## Què és una bretxa de seguretat

- Modificació no autoritzada de les dades
- Pèrdua parcial o total de les dades
- Difusió no autoritzada de les dades
- Es notificarà a l'autoritat de control en el termini màxim de 72h.
- I als interessats quan comporti un risc alt per la seva privacitat

# RELACIONS RESPONSABLE - ENCARREGAT

- És el Responsable qui **determina** el tractament i la seva finalitat i s'assegura del compliment normatiu per part de l'encarregat del tractament
- La relació s'ha de formalitzar de forma **contractual** amb el contingut mínim que estableix el RGPD
- Els encarregats han d'oferir **garanties** suficients d'aplicació de les mesures tècniques i organitzatives per complir amb el RGPD
- És recomanable establir mesures de **control** del compliment

# Adequació del despatx al RGPD

# FULL DE RUTA

Fases per adequar el despatx

## EQUIP

- Definir l'equip
- Compartir la visió
- Formar al personal crític

## AUDITORIA

- Dades
- Consentiments
- Tractaments
- Avaluació Riscos
- Mesures de seguretat

## ADEQUACIÓ

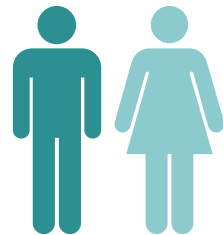
Identificar dades  
Avaluació de Impacte  
Registre Activitats  
Consentiment  
Informació  
Mesures seguretat  
Formació

## ADEQUACIÓ CONTINUA

Formació continua  
Consultes  
Revisions  
periòdiques

# CONFORMAR L'EQUIP

Un equip **format**, amb responsabilitat i autoritat



- Definir l'equip
  - Nomenar un responsable de l'adequació ("**campió**")
  - Nomenar Responsables / Encarregats de Tractaments
  - Nomenar Responsable de Seguretat
  - Preveure un DPO (si és necessari)
- Compartir la visió
  - Revisar els principis generals
- Implicar a l'àrea Jurídica, de Sistemes, d'Organització, (Mktg. / Comercial)
- Formar el personal crític

# AUDITORIA

Punt de partida



- Fitxers declarats a l'AEPD i Document de Seguretat (LOPD)
- Identificar dades personals
- Identificar tractaments
- Legitimació (consentiment)
- Informació i Drets
- Contractes responsable / encarregat
- Mesures de Seguretat > Organitzatives / Tècniques
- **Avaluació de riscos** (*obligatòria i permanent*)



# ADEQUACIÓ



- Avaluació d'Impacte
- Designació DPO
- Revisió legitimació (mecanismes consentiment)
- Informació i exercici Drets
- Registre d'Activitats de Tractament
- Contractes responsable / encarregat
- Mesures de Seguretat> Organitzatives / Tècniques
- Protocols de resposta (incidents, exercici drets, ...)
- Formació

# ADEQUACIÓ

Mesures de **Seguretat**



## Organitzatives

- Deure de Confidencialitat i Secret (evitar accés no autoritzat, no divulgació, ...)
- Drets dels Titulars de les Dades (procediment exercici ARCOPOL)
- Violacions de Seguretat (protocol de notificació AEPD)
- Captació amb Càmeres (deure informació, control laboral, ...)

## Tècniques

- Identificació (perfils, passwords, ...)
- Deure de salvaguarda (actualitzacions, xifrat de dades, còpies seguretat, ...)

# ADEQUACIÓ CONTINUA

L'adequació NO és una foto fixa



- Consultes sobre situacions noves
- Actualització de la formació
- Revisió periòdica de l'adequació
- Revisió mesures de seguretat

# RGPD: Ameaça o Oportunitat

# AMENANÇA O OPORTUNITAT

Convertir una amenaça en una oportunitat

## Alguns apunts

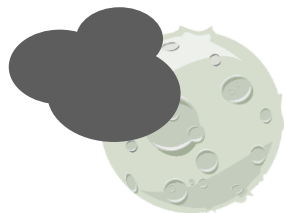
- Comunicació amb grups de interès
- Generació de confiança
- Valor a llarg termini amb la fidelització del client
- Organització
- Seguretat

# RGPD: Annexes

# ENLLAÇOS DE INTERÈS



- [Solicitud](#) de Copia de la Inscripción de Ficheros
- [Eina FACILITA](#) de l'AEPD
- [Hoja de Ruta](#) de adecuación (sector privado)
- [Llista](#) de verificació (per l'adequació)
- [Guías](#) de Análisis de Riesgo y Evaluación de Impacto
- [Guía](#) de Privacidad y Seguridad en Internet
- Principals [novetats](#) del RGPD
- [Reglament](#) (UE) 2016/679 del Parlament Europeu i del Consell
- [Documentació](#) de l'Autoritat Catalana de Protecció de Dades (tota)
- [Documentación](#) de la Agencia Española de Protección de Datos (toda)



## TECNOLAWYER

Ricard Castellet

M. 607 505 305

[rcastellet@tecnolawyer.com](mailto:rcastellet@tecnolawyer.com)

[tecnolawyer.com](http://tecnolawyer.com)

Crèdits:

\* Jorge García – Abogado

Grafisme llicenciat de DesignSmash - NYC

El perfil de Barcelona està llicenciat de Fotolia

