NOU REGLAMENT EUROPEU DE PROTECCIÓ DE DADES

PRINCIPALS NOVETATS I IMPLICACIONS PER AL **SECTOR SANITARI**

datax

Consultoria especialitzada en Protecció de Dades i Seguretat de la Informació

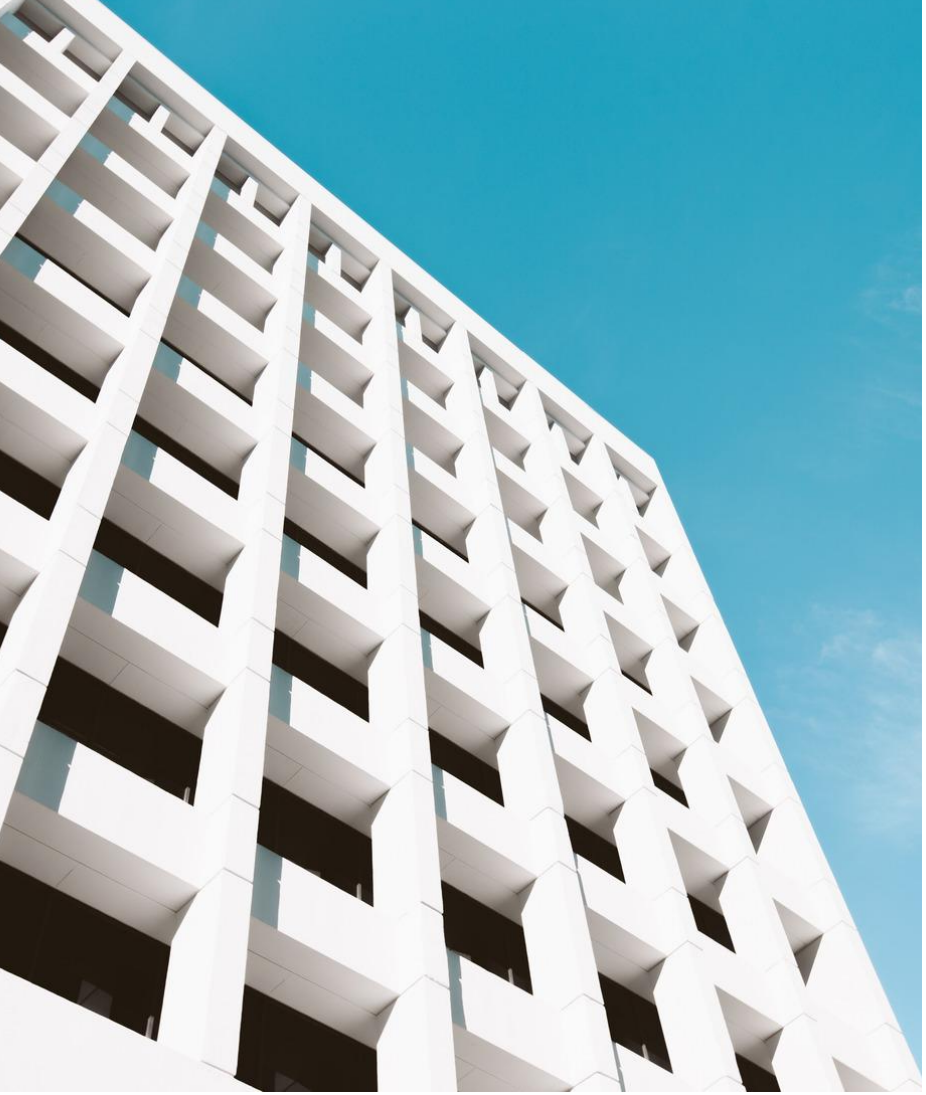
aces
ASSOCIACIÓ CATALANA D'ENTITATS DE SALUT

¿Què és el nou Reglament Europeu?

És la nova normativa europea de protecció de dades personals. Serà d'aplicació obligatòria a partir del **25 de maig de 2018**.

Principals novetats

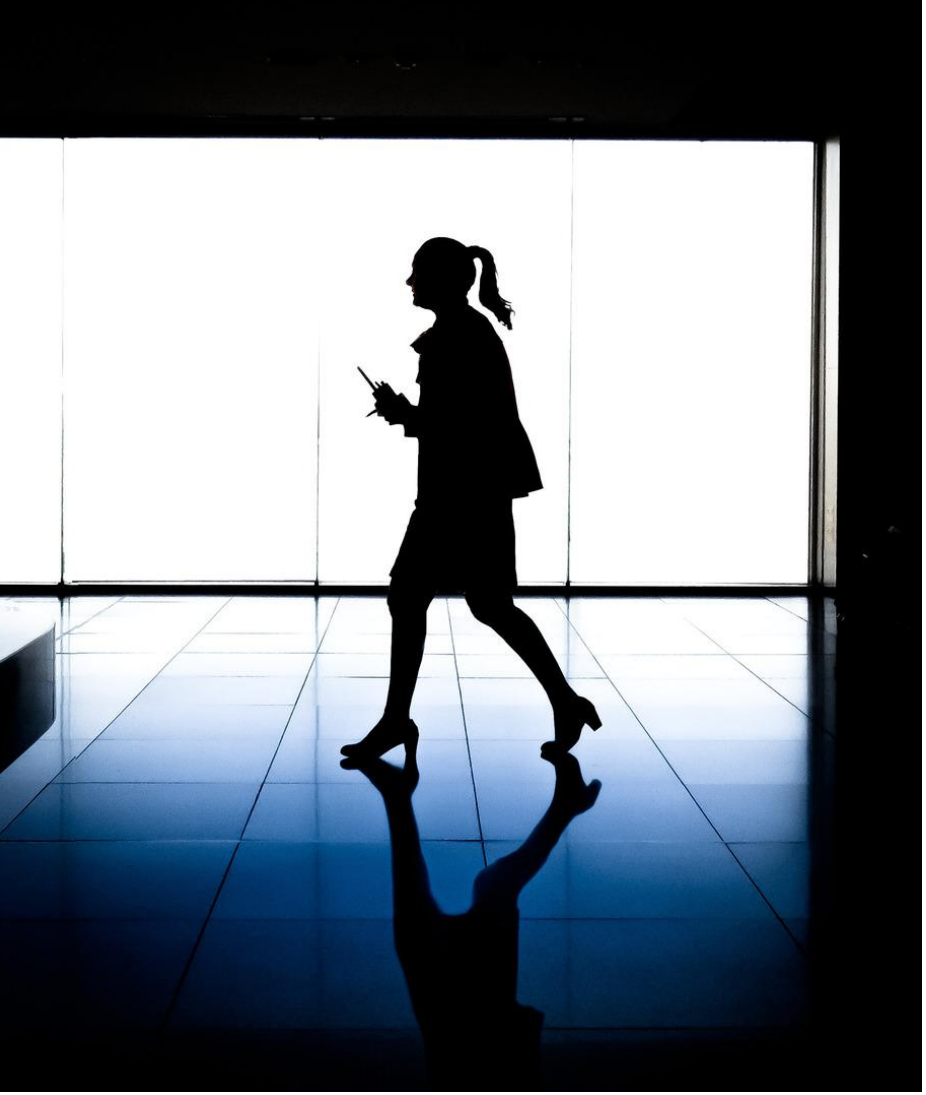
- Amplia els drets dels ciutadans europeus
- Estableix noves obligacions per a entitats de salut
- Introdueix el principi de Responsabilitat Proactiva
- Crea la nova figura del Delegat de Protecció de Dades
- Incrementa les sancions econòmiques



¿A qui afecta?

El Reglament Europeu afecta a totes les empreses, organismes o autoritats públiques que tracten dades personals de ciutadans europeus.

Incloses entitats de salut



¿Què és una dada personal?

Qualsevol informació relativa a persones físiques identificades o identificables.

Per exemple: nom, adreça, geolocalització...

¿Totes les dades són iguals?

L'RGPD estableix dades de categories especials que requereixen un tractament amb garanties reforçades.

DADES GENÈTIQUES
DADES BIOMÈTRIQUES
DADES RELATIVES A LA SALUT

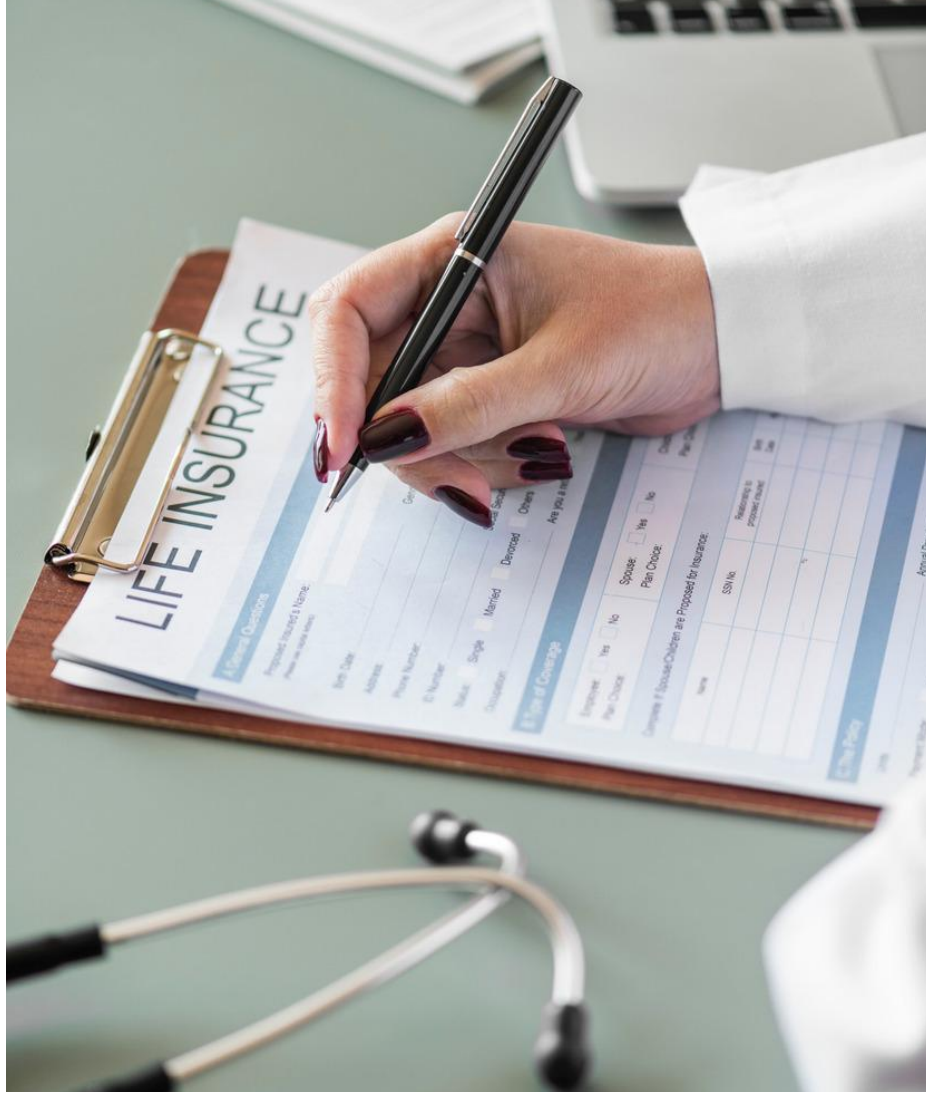
Com afecta a les persones?

Els pacients tindran nous drets i un major control i informació sobre el tractament de les seves dades personals.

Dret a la informació

L'RGPD amplia la informació que s'ha de facilitar als pacients en el moment de recollir el seu consentiment.

Concreta que s'ha de fer de manera concisa, entenedora i de fàcil accés, amb un llenguatge clar i senzill.



Nous drets

El responsable ha d'implementar mecanismes per facilitar l'exercici dels drets als titulars de les dades.

Accés
Rectificació
Oposició
Limitació de tractament
Supressió *(Dret a l'oblit)*
Portabilitat

Com afecta a les entitats de salut?

S'estableixen noves obligacions basades en la Responsabilitat Proactiva.

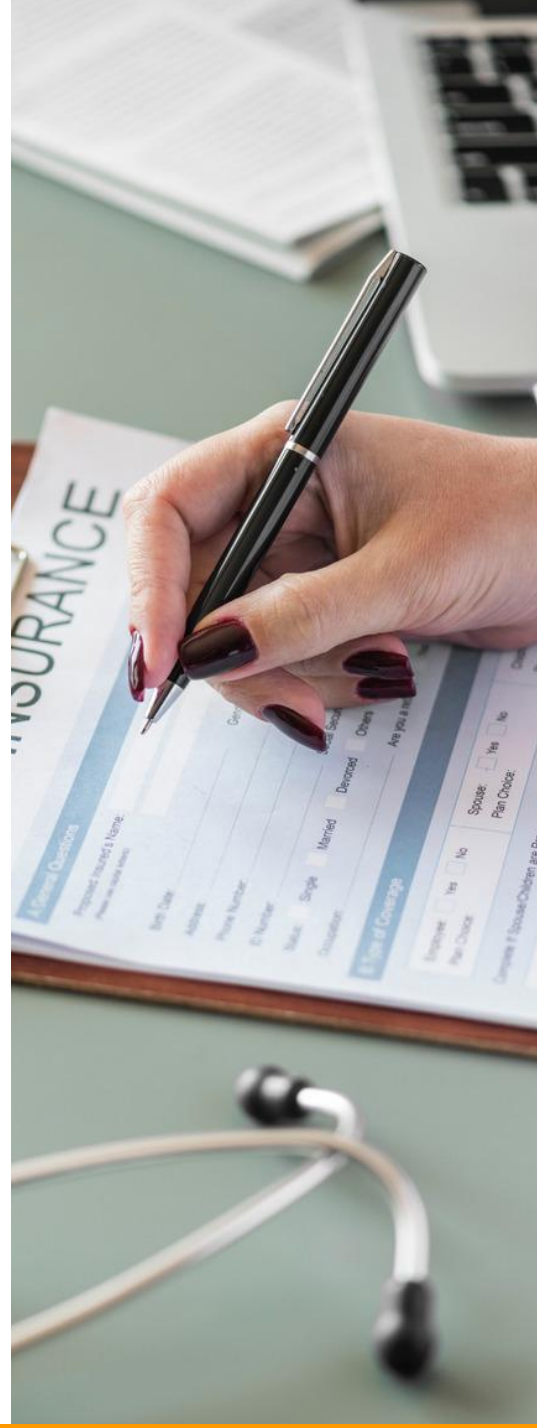
Aquest principi es basa en la **prevenció** i exigeix que s'apliquin mesures tècniques i organitzatives apropiades per **garantir** i **demostrar** el compliment del RGPD.

Consentiment

El consentiment haurà de ser **exprés**.
Obtenció de forma lliure, específica, informada i inequívoca, mitjançant una **acció positiva**.

S'elimina el consentiment tàcit.

El consentiment informat clínic no legitima el tractament de dades.



Menors d'edat

+ de 13 anys

Consentiment lícit.

- de 13 anys

Necessari consentiment de pares o tutors legals.

Registre d'activitats

Les empreses han de registrar els tractaments de dades que realitzen, incloent-hi, com a mínim, la següent informació:

- *Dades de contacte del responsable, representant i delegat de protecció de dades.*
- *Finalitat del tractament.*
- *Categories dels interessats i dades.*
- *Destinataris existents i previstos.*
- *Transferències internacionals i garanties.*
- *Terminis de supressió.*
- *Descripció mesures de seguretat.*

Deure d'informar

El sector sanitari ha d'actualitzar les clàusules informatives dels tractaments de dades.

Les autoritats recomanen adoptar un model d'informació per capes sempre que sigui possible per complir amb les noves exigències del RGPD.

Aspecte a millorar segons l'estudi de l'AEPD a Hospitals públics.

Responsable-Encarregat

Els contractes que vinculen Responsables i Encarregats de tractament s'han d'actualitzar segons requisits del nou Reglament.

Exemple:
Si una clínica és intermediària en un contracte de crèdit al consum, haurà d'aparèixer com encarregada de tractament de l'entitat financera.

Anàlisi de riscos

Els responsables hauran d'analitzar i valorar el risc dels tractaments que realitzen amb l'objectiu d'establir mesures adequades.

FUGA DE DADES

És el risc més freqüent en el sector sanitari. Consisteix en la pèrdua de la confidencialitat de la informació privada d'una persona.

Mesures de seguretat

L'RGPD exigeix mesures que garanteixin un nivell de seguretat adequat al risc i que permetin demostrar el correcte compliment.

Aspecte a millorar segons l'estudi de l'AEPD a Hospitals públics.

Amenaces

Les amenaces més freqüents en la protecció de dades del sector sanitari:

- *Accés o tractament ilegítim*
- *Modificació no autoritzada*
- *Pèrdua o eliminació intencionada*

Mesures de seguretat

Algunes mesures per reduir el nivell del risc identificat:

- *Control d'accés*
- *Seudonimitzar i xifrar les dades*
- *Realitzar copies de seguretat*

Avaluació d'impacte

Els responsables hauran de realitzar una DPIA abans de començar un nou tractament que pugui suposar un alt risc per als drets i llibertats dels titulars de les dades.

Tractament de categories especials de dades personals com, per exemple, informació de registres mèdics.

Notificació d'incidències

Davant d'una violació de la seguretat de les dades que suposi un risc per als drets i llibertats dels titulars, s'ha d'informar a l'autoritat competent i als interessats.

El termini màxim és de 72 hores des que el responsable tingui constància de la incidència.

Codis de conducta i certificació

Per demostrar el correcte compliment, existeix la possibilitat d'adherir-se a codis de conducta o certificar-se segons esquemes del RGPD.

Aquests mecanismes serveixen de garantia de Proactivitat per a Responsables i Encarregats.

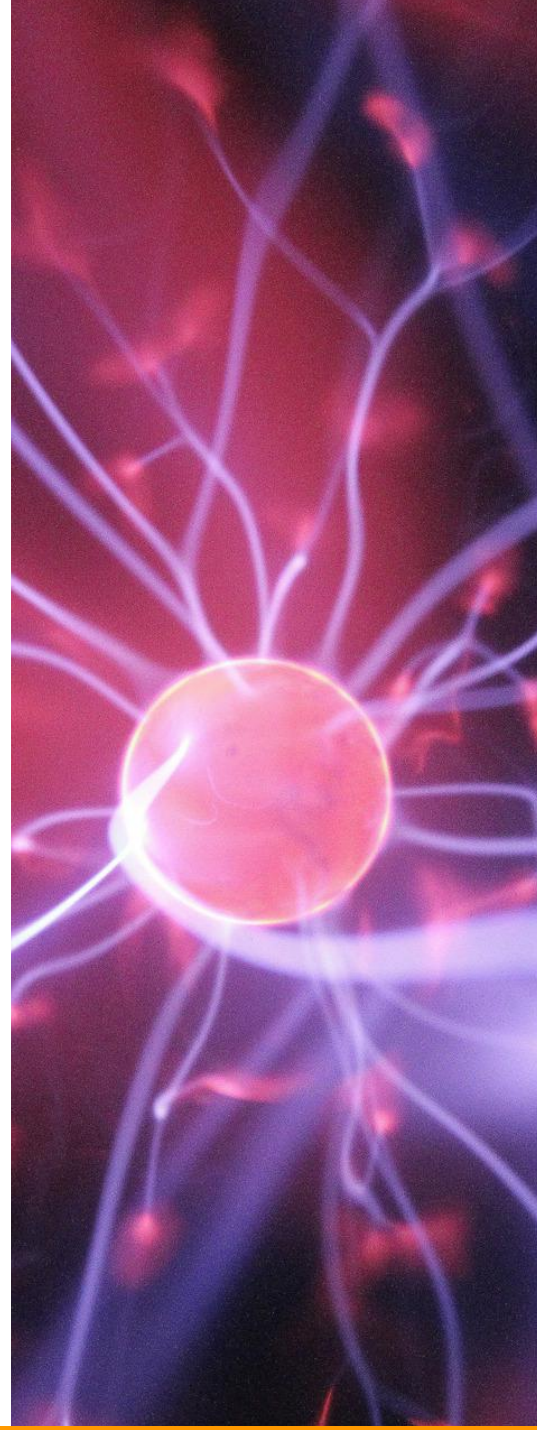
Delegat de Protecció de Dades

S'estableix la nova figura professional de *DPO*, l'encarregat de garantir el compliment de la normativa dins de les organitzacions.

La contractació d'un DPO serà obligatòria per a empreses del sector sanitari.

Sancions

L'incompliment del Reglament Europeu pot derivar en multes de fins **20 milions d'euros** o el 4% del volum de negoci anual.



RECOMANACIONS

PLA D'INSPECCIÓ DE L'AEPD A HOSPITALS

- Millorar la informació i sol·licitud del consentiment dels pacients.
- Establir controls d'accés a documents amb dades mèdiques per finalitats no assistencials i limitar l'accés a histories clíniques.
- Incloure o millorar la seguretat als espais per a l'accés a histories clíniques, prestant especial atenció als processos d'entrega i retirada de documentació.
- Incloure al contracte d'assaig clínic la prohibició de tractar dades per a altres finalitats diferents a la investigació, que fem amb les dades al acabar l'assaig i la seudonimització per la publicació de resultats.
- Sol·licitar consentiment per a finlitats diferents a la investigació o assistencial.
- Facilitar la informació sobre el tractament d'un assaig clínic de la forma més clara possible i sense ambigüitats.
- Implementar protocols i mecanismes de custodia de les dades personals un cop finalitzat l'assaig clínic.

PROPERS PASSOS

PLA ESTRATÈGIC DE L'AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES

2016 / 17
Pla d'inspecció sectorial d'ofici a Hospitals

2018
Estudi sobre reutilització d'informació clínica i Big Data al sector sanitari

2018 / 19
Pla d'inspecció sectorial d'ofici del sector sociosanitari

2018 / 19
Guia per a institucions i professionals sanitaris

2018 / 19
Guia per a pacients i usuaris de la sanitat

DATAX T'ADAPTA

AL NOU REGLAMENT EUROPEU DE PROTECCIÓ DE DADES

+ de 14 anys
d'experiència

Fem fàcil el que
és difícil

Responem
pel que fem

datax

Consultoria especialitzada en Protecció de Dades i Seguretat de la Informació

aces
ASSOCIACIÓ CATALANA D'ENTITATS DE SALUT