Implicacions del nou GDPR per als professionals TIC

El desplegament de la Regulació Europea de Protecció de Dades al nostre territori.

Noves figures professionals i oportunitats per al col·lectiu informàtic

Joaquín Garrido
Vicedegà adjunt a la presidència del COEINF
joaquin_garrido@enginyeriainformatica.cat

Juny 2018

el COEINF

informàTICs
Enginyeria en informàtica de Catalunya

- Institució oficial pública catalana i independent, creada per la Llei 3/2001 del Parlament de Catalunya 2001
- Aglutina els i les Enginyers/es en Informàtica, els representa, organitza, protegeix, tot vetllant per un adequat exercici de la professió, amb garantia de qualitat i voluntat de servei a la Societat

RGPD/GDPR

- Reglament General de Protecció de Dades / General Data Protection Regulation
- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades)
- Entrada en vigor
  - 24 de maig de 2016
- Període d'adaptació: 2 anys
- Compliment obligatori
  - 25 de maig de 2018

Principals motivacions

- Protecció de les persones físiques pel que fa al tractament de dades personals
  - **Dret fonamental** (art. 8 Carta Drets Fonamentals UE)
- Harmonitzar els drets i llibertat fonamentals
- Garantir la lliure circulació de dades personals entre els Estats de la UE
- Nous reptes amb els avenços tecnològics
  - Magnitud
  - Difusió
  - Necessitat de confiança
  - Capacitat d'identificabilitat
- Control per part del propietari
- Seguretat jurídica i pràctica

RGPD/GDPR

- Requeriment de un desenvolupament normatiu intern → Nova Llei Orgànica de Protecció de Dades (LOPD)
  - En tramitació parlamentaria
  - Aprovació del projecte de la nova Llei
    - 10 de novembre de 2017
  - Fase presentació de esmenes
    - Fins 3 d'abril de 2018
    - Multitud d'ajornaments
  - Aprovació Llei
    - ??

Nou enfocament

- La informació com un Dret
- Anticipació a la infracció o vulneració de drets vs. Evitar la infracció
- **Responsabilitat proactiva** (Accountability) vs. reactiva
  - Per part del responsable del tractament
  - Decidir i aplicar les mesures tècniques i organitzatives adequades (naturalesa, àmbit, context, finalitats i riscos)
  - Garantir i poder demostrar el compliment del RGPD (codis de conducta i certificacions)
  - Actualitzar i revisar periòdicament (auditoria interna i/o externa)
  - Actitud conscient, diligent i proactiva

Nou enfocament

- Tractaments de risc
  - Pot comportar discriminació, usurpació d'identitat o frau, pèrdues financeres, dany a la reputació, pèrdua de confidencialitat, reversió de la seudonimització, perjudici econòmic o social significatiu
  - Pot privar als interessats de drets i llibertats o no permetre exercir el control sobre les seves dades
  - Dades sensibles
  - Elaboració de perfils predictius
  - Dades de col·lectius vulnerables
  - Alt volum de dades de gran quantitat de persones
- Avaluació del risc
  - **Anàlisi de riscos** per a cada tractament
  - Mesures d'acord amb el nivell de risc
  - Ajuda per determinar el risc: DPD, Bones pràctiques, certificacions, ...
  - Mateixes dades amb mesures diferents en funció del risc

Nou enfocament

informàTICs
Enginyeria en informàtica de Catalunya

- **Des del disseny**
  - Aplicar el RGPD des de l'inici de la concepció d'un projecte
  - Conscienciació dels dissenyadors i desenvolupadors
  - Decidir i aplicar les mesures tècniques i organitzatives adequades (naturalesa, àmbit, context, finalitats i riscos)
  - Incloses les dades seudonimitzades
- **Per defecte**
  - Màxim grau de privacitat per defecte
    - Quantitat de dades
    - Transparència
    - Temps que es mantenen les dades
    - Accessibilitat a les dades
    - Autorització explícita per a la cessió de dades

Principals novetats

LOPD (1999-2018)	RGPD (2018-)
Fitxers	Registre de les activitats de tractament
Registre d'incidències	Notificació d'incidents a l'AEPD
Drets accés, rectificació, cancel·lació i oposició	Ampliats amb oblit, limitació del tractament i portabilitat
Responsable de seguretat	DPD/DPO
Informe d'auditoria	Avaluació d'impacte
Sancions: 900-600.000€	Sancions: 2%-4% facturació anual – 10-20 milions €
Consentiment tàcit	Consentiment inequívoc
Signatura contracte encarregat tractament	Certificat per verificar compliment de la normativa

Registre d'activitats

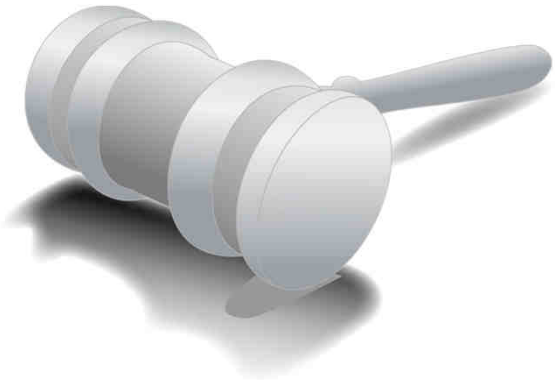
- Característiques
  - Desapareix l'obligació de crear fitxers i notificar-los
  - Els responsables/encarregats del tractament han de documentar un registre d'activitats de tractament
    - No obligats els que comptin amb menys de 250 treballadors i que duguin a terme tractaments que no puguin comportar un risc per als drets i llibertats i que no incloguin categories especials de dades personals o dades relatives a condemnes i infraccions penals
  - Informació a registrar
    - Nom i dades de contacte del responsable i DPD
    - Finalitats del tractament
    - Descripció de categories d'interessats i de dades
    - Terminis previstos per suprimir les dades
    - **Descripció mesures tècniques de seguretat**

Incidents seguretat

- Característiques
  - 72 hores per notificar qualsevol violació de la seguretat a l'autoritat de control
    - Excepte que sigui improbable que constitueixi un risc per als drets i llibertats
  - Si el risc és alt (probables danys importants)
    - Comunicació a les persones afectades
  - Documentar totes les violacions
  - Informació a incloure
    - Naturalesa de la violació
    - Categoria de dades i interessats afectats
    - **Mesures adoptades per solucionar la fallada**
    - **Mesures aplicades per pal·liar els efectes**

Drets dels propietaris

- Drets "clàssics" ARCO: Accés, Rectificació, Cancel·lació i Oposició
- Dret a l'oblit
  - Dades ja no necessàries, revocació del consentiment, oposició al tractament, tractament il·lícit, obligació legal, menors
  - Si s'han fet públiques → adopció de mesures raonables per informar de la supressió a qui estigui tractant les dades
  - Excepcions → llibertat d'expressió i informació, obligació legal, finalitat d'arxiu en interès públic
- Dret a la limitació del tractament
  - No s'aplicaran les operacions de tractament
- Dret a la portabilitat en format transmissible
- **Possibilitar l'exercici per mitjans electrònics**



DPD/DPO

- Personal propi o Contracte de serveis
- Exclusiu o Compartit – Del Responsable i/o de l'Encarregat
- **Requerit**
  - "*Autoritats/Organismes públics*"
  - "*Observació habitual i sistemàtica*" de dades "*a gran escala*"
  - Tractament "*a gran escala*" de dades de categories especials
- Designació pública
- Funcions
  - Supervisió de l'observança del RGPD
  - Assessorar respecte l'Avaluació d'impacte
  - Cooperar amb l'autoritat de control
  - Col·laborar en el manteniment de registres

DPD/DPO

- Facilitació del compliment del RGPD
  - Aplicació d'instruments de rendició de comptes
    - Avaluacions d'impacte
    - Auditories de protecció de dades
  - Intermediaris entre les parts interessades
- No responsable personalment en cas d'incompliment
  - Responsabilitat final del responsable o encarregat del tractament
- Requereix
  - Autonomia
  - Recursos suficients i participació activa
- Ha de facilitar la comunicació eficaç
  - Dades de contacte accessibles, idiomes, ...

DPD/DPO

- Art. 37 apartat 5

  "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39"

- Nivell de coneixements
  - Adequats a la sensibilitat, complexitat i quantitat de les dades
  - Sector empresarial – Normes i procediments administratius
  - Jurídics / Protecció de dades
  - **Operacions de tractament**
  - **Sistemes d'informació**
  - **Necessitats de seguretat i protecció**

DPD/DPO

- Qualitats personals
  - Integritat
  - Ètica professional
  - Confidencialitat
  - Conflicte d'interessos
  - Capacitat de lideratge i priorització
- Certificacions
  - Esquema certificació DPD – AEPD & ENAC
  - No obligatori
  - Qui les ofereix
    - Entitats acreditades per l'ENAC: ANF, IVAC, AEC
    - Altres entitats reconegudes

DPD/DPO

informàTICs
Enginyeria en informàtica de Catalunya

- Pre-requisits certificació esquema (almenys un)
  - Almenys 5 anys d'experiència professional en projectes, activitats i/o tasques relacionades amb les funcions de DPD en matèria de protecció de dades
  - Almenys 3 anys d'experiència professional i formació mínima en entitats reconegudes de 60 hores en les matèries objecte del programa
  - Almenys 2 anys d'experiència professional i formació mínima en entitats reconegudes de 100 hores en les matèries objecte del programa
  - Formació mínima en entitats reconegudes de 180 hores en les matèries objecte del programa
- Justificació
  - Formació online o presencial
  - Experiència anterior i posterior al 25/05/2016
  - Fins un any d'experiència amb mèrits addicionals
    - Formació universitària
    - Altres: formació, certificacions, docència, ...

DPD/DPO

- Avaluació certificació esquema (examen)
  - 150 preguntes tipus test, 4 opcions, no resten les errades, 4 hores
  - 3 Dominis (50%-30%-20%)
    - Normativa general de Protecció de Dades
    - Responsabilitat activa
    - Tècniques per garantir el compliment de la normativa de Protecció de Dades i altres coneixements
  - Aprovat > 75% (<50% a cada Domini)
  - 30% de les preguntes: escenari pràctic
- Validesa del certificat durant 3 anys
- Requisits renovació
  - Formació mínima de 60 hores amb mínim de 15 anuals
  - Almenys 1 any d'experiència en funcions de DPD

Avaluació d'impacte

- Tractament que suposi un risc alt per la seva naturalesa, abast, context o finalitats
  - Elaboració de perfils sobre els que es prenen decisions amb efecte jurídic
  - Tractament a gran escala de dades sensibles
  - Observació sistemàtica a gran escala d'una zona d'accés públic
- Pot ser conjunta per a diversos tractaments similars
- Pot servir per avaluar l'impacte d'un producte tecnològic
- Objectius
  - Descriure el tractament, avaluar la necessitat i proporcionalitat
  - Ajudar a gestionar els riscos
  - Rendir comptes
- Consulta prèvia

Avaluació d'impacte

- Quan?
  - Prèvia al tractament, en el disseny de l'operació de tractament
- Qui?
  - Responsable amb el suport del DPD i els encarregats del tractament
  - Pot requerir recollir l'opinió dels interessats
- Quan?
  - Prèvia al tractament, en el disseny de l'operació de tractament
- Què?
  - Descriure les operacions del tractament i les finalitats
  - Avaluar la necessitat i proporcionalitat
  - Avaluar els riscos
  - Mesures previstes per gestionar els riscos
  - Demostrar compliment RGPD

Consentiment

- Característiques
  - Acte afirmatiu clar
  - Manifestació de voluntat lliure, específica, informada i inequívoca
  - Declaració escrita, per mitjà electrònic o verbal
  - Per a totes les finalitats (indeterminades?)
  - No s'accepta: silenci, caselles ja marcades o inacció (omissió)
  - Consentiment inequívoc vs. Explícit
  - > 16 anys (rebaixable a 13 anys)
- Bombardeig de correus els darrers dies
  - Necessari?
- **Requeriment de revisions i adaptacions**

Encàrrec tractament

- Nou contingut del contracte
  - Objecte i durada de l'encàrrec
  - Naturalesa del tractament
  - Tipus de dades personals
  - Categories d'interessats
  - Assistència al responsable en sol·licituds d'exercici de drets
  - Obligacions i drets del responsable
  - Confidencialitat
  - Supressió o devolució de dades al finalitzar
  - Facilitar informació al responsable per:
    - Demostrar compliment obligacions
    - Realitzar auditories i inspeccions
- Encarregats adherits a codis de conducta o certificats
  - Valor afegit → Garantia de compliment

Implicacions del nou GDPR per als professionals TIC

El desplegament de la Regulació Europea de Protecció de Dades al nostre territori.

Noves figures professionals i oportunitats per al col·lectiu informàtic

gràcies

informàTICs

Enginyeria en informàtica de Catalunya