Xerrada sobre el nou Reglament general de protecció de dades (RGPD)

Associacionisme i Voluntariat - Servei de Participació Ciutadana - Ajuntament de Sabadell

Impartida per Carles San José Amat (Cap de l'Àrea d'Inspecció de l'Autoritat Catalana de Protecció de Dades

Dijous, 14/06/2018

Introducció:

A mode d'introducció va comentar les següents idees:

- La privacitat és com la salut, la valorem quan la perdem
- Les administracions i els poders públics van ser els primers a acumular i disposar de grans quantitats de dades dels ciutadans. Després van fer-ho les empreses, singularment les grans empreses del món digital, les conegudes com a GAFA[1]
- L'any 1992 la Ley Orgánica 5/1992, de 29 d'octubre, de regulación del tratamiento automatizado de los datos de carácter personal, ja destacava que el temps i l'espai, ja llavors, no servien com la barrera protectora i salvaguarda de la privacitat que havien estat tradicionalment. I d'això fa 22 anys!

Conceptes del nou reglament

- El dret a la protecció de dades és un dret fonamental (deriva de l'art. 18.4 de la CE) connectat però independent del dret a la intimitat. És més aviat un «dret a la autodeterminació informativa». Proporciona control sobre la pròpia informació, és a dir sobre qualsevol dada relativa a una persona identificada.
- Aquell qui facilita les dades ha de ser sempre «l'amo» d'aquesta informació.
- El RGPD protegeix les persones. Les empreses No són persones i no estan emparades per aquest reglament però compte, els autònoms sí.
- **Responsable**: es defineix com la persona física o jurídica que és responsable últim de la informació, de custodiar-la, del seu tractament i de tot el que pugui passar.
- **Encarregats**: Són les persones físiques o jurídiques que s'encarreguen del tractament. Tenen obligacions específiques però és el Responsable qui determina què poden i què no poden fer, és a dir l'existència i finalitat del tractament.
- **Destinatari**: És qui rep el resultat del tractament. S'ha d'informar en recollir la dada.
- **Tercer**: Es considera un tercer a qualsevol altre destinatari diferent, aliè a l'entitat.
- **Elaboració de perfils**: Per poder-se fer cal demanar el consentiment específicament.
- **Seudonimització**: És un pas entremig de les dades amb filiació i les anònimes. S'utilitzen codis per protegir la identificació (com en els exàmens) però sempre hi ha algú que pot conèixer la identitat d'aquell a qui es refereix una dada.
- **Proactivitat (responsabilitat proactiva)**: És una de les principals novetats del RGPD. Es refereix a què no existeix cap descripció exhaustiva i detallada de normes, mesures ni mecanismes a seguir ja que la casuística de situacions possibles és inabastable i canviant. En lloc d'això s'exigeix que les organitzacions actuïn de forma conscient, diligent i proactiva. És a dir que analitzin i tinguin clars els riscos i decideixin les mesures més adients per minimitzar-los. Sense cap check-list previ d'actuacions, però podent demostrar en tot moment que el tractament és conforme al reglament.

[1] Google, Amazon, Facebook i Apple

Principis i deures

- **Licitud i lleialtat**: Podem resumir-ho en no mentir ni enganyar ni fer tractaments il·legals. I com assegurar-nos de fer-ho tot legalment?
    - Consentiment: demanar explícitament el consentiment dels propietaris de la informació pel tractament que volem fer-ne.
    - Execució d'un contracte: Si hi ha un contracte (cobrament de quotes, per exemple) el consentiment pels tractaments que se'n derivin ja va implícit.
    - Compliment d'obligacions legals. (és el cas de metges i serveis socials que si, per exemple, sospiten de maltractaments no necessiten el consentiment per informar les autoritats)
    - Per missions d'interès públic. (seria el cas de les identificacions policials)
    - Per satisfer interessos legítims sempre que no prevalguin els drets de l'interessat. (Les administracions no s'hi poden acollir)
- **Transparència**: De cara als propietaris de la informació. Què en farem? Per a què ho volem? Quant de temps ho tindrem? I tot explicat de forma comprensible.
- **Finalitat**: les dades recollides no es poden fer servir per altres finalitats diferents d'aquelles que es va informar en el moment de la recollida. I no són admissibles els consentiments genèrics; cal un consentiment per a cada finalitat
- **Minimització**: Recollir i tractar només les dades estrictament necessàries. (de vegades es demanen per sistema dades que ni se sap si caldran per res). En tot cas oferir opcionalitat.
- **Exactitud**: Cal vetllar per la fiabilitat de les dades.
- **Limitació termini de conservació**: Es tracta d'una novetat; només es poden tenir les dades el temps necessari per complir amb la finalitat.
- **Integritat i confidencialitat**: S'ha garantir la seguretat adequada mitjançant mesures tècniques i organitzatives «apropiades».

Conceptes a destacar

- **Responsabilitat proactiva**: Es tracta d'un dels principals conceptes nous que s'introdueixen amb aquest reglament. Es prescindeix de llistats exhaustius i rígids de normes obligatòries amb casuístiques complexes però, a canvi, les organitzacions:
    - Han de tenir una política de privacitat. (art. 24.2)
    - Ja no han de declarar els fitxers de dades que custodien a l'agència de control, però han de dur un registre de tractament (d'activitats de tractament). Aquest registre consisteix simplement a tenir un control intern, a descriure què tinc i que en faig del que tinc. Pot elaborar-se fàcilment a partir de les dades que anteriorment s'havien enviat a l'agència i que aquesta pot facilitar-nos per un procediment senzill que ja està previst.
    - Encara que no tothom està obligat a dur-lo (depèn de la categoria de les dades i del risc que puguin suposar pels drets i llibertats dels interessats) es recomana fer-ho per defecte.
    - Les violacions de seguretat s'han de registrar i comunicar a les persones afectades si es considera que hi ha un risc alt. Fins i tot, posa com a exemple, haver enviat un correu amb el llistat de destinataris en obert, és a dir en el camp 'per a' en lloc d'haver-ho fet en ocult. Conclou que, en cas de dubte, sempre és millor comunicar la incidència a l'agència que pecar per defecte.
- **Delegat Protecció de Dades**: A les entitats petites no ens afecta, a menys que tractem dades de categories protegides. El DPD no assumeix responsabilitats. Només s'encarrega del tractament seguint les indicacions del Responsable, que ha d'existir igualment.
- **Consentiment**: Ha de ser lliure, en condicions d'igualtat, informat i específic. També ha de ser inequívoc, amb acció positiva, no pot ser tàcit (allò de «si no em dius el contrari» o amb caselles prèviament-marcades)

- **Consentiment dels menors**: Fins ara era a partir dels 14 anys. Actualment, a la Unió Europea, es preveu elevar-ho a partir dels 16 anys però els països podran rebaixar-ho fins als 13. (A Espanya sembla que es farà així però per ara cal aplicar els 14 anys)
- **Categories especials (Protegides)**: Són les que hi havia fins ara més:
    - Dades genètiques
    - Dades biomètriques

  Per el tractament de les dades especials el consentiment sempre ha de ser explícit
- **Comunicació de dades**: No es regula de manera específica com feia la LOPD (art. 11) si no com qualsevol altre tractament que haurà de ser lícit conforme l'article 6. Tampoc es defineix el destinatari.

Drets dels interessats

Abans eren només els coneguts com ARCO (Accés, Rectificació, Cancel·lació i Oposició). Cal informar els propietaris de les dades dels seus drets: Qui ha d'informar? -> el responsable. Quan ha d'informar? -> En el moment de recollir les dades si les dóna el mateix interessat o en la 1ª comunicació si són rebudes o traspassades.

Hi ha situacions en què no cal informar, per exemple si ja s'ha fet abans. De tota manera s'han afegit moltes coses al que ja hi havia en relació a la informació que cal donar. Pot consultar-se el contingut als art. 13 i 14. Una idea és facilitar la informació «per capes» (Allò de clica aquí per veure més informació)

- **Accés**: (art. 15 RGPD) Què teniu de mi? (S'ha de respondre: No tinc res o tinc tot això)
- **Rectificació**: Facilitar la possibilitat de corregir o canviar
- **Dret de supressió**: Oblit
- **Limitació del tractament**: Permet conservar les dades limitant el que es pot fer amb elles. (Per exemple els morosos amb litigis amb les companyies no poden exigir ser esborrats però sí que les dades no siguin utilitzades per a la resta de finalitats)
- **Dret a la portabilitat**: Traslladar la meva informació a uns altres. (Dins les limitacions tècniques i la compatibilitat de formats)
- **Dret d'oposició**: Dret a què no es porti a terme o es cessi el tractament per:
    - Motius relacionats amb la situació personal (assetjaments)
    - màrketing directe (llistes Robinson)
    - oposició a decisions individuals automatitzades (sol·licitud de crèdits)

Sobre les persones difuntes

No tenen dret a la protecció de dades
El legislatiu està treballant per donar drets als successors

Garanties dels drets

Les persones poden reclamar (denunciar) davant l'autoritat de control (art. 77)
Hi ha previstes multes i també indemnitzacions si hi ha hagut danys morals

Consulta recurrent sobre els grups de Whatsapp: Si el grup és de l'AMPA cal demanar el consentiment però no si, per exemple, els grups de les classes són iniciativa personal dels pares. En qualsevol cas, si l'AMPA hi participa, s'aconsella regular l'ús i informar de la utilització.