



EAPC blog

“Ja soc aquí”. Si parlés, això és el que ens diria l'RGPD – Carles San José

🕒 22 de maig de 2018



Certament, fa moltes setmanes que llegim i sentim la cita del 25 de maig de 2018 com a data en què l'RGPD aterra, definitivament, en el nostre dia a dia. Doncs ja el tenim aquí entre nosaltres, integrat en el nostre ordenament jurídic i d'aplicació plena i directa. Ara cal, doncs, que entre tots aconseguim que sigui efectiu.

L'RGPD substitueix les normes que cada estat de la UE havia aprovat a partir de la Directiva 95/46/CE, que ja no podia fer front als nous reptes que la ràpida evolució tecnològica i la globalització ha plantejat per a la protecció de dades. A això es refereix el considerant 6è de l'RGPD, i afegeix el següent: *“La magnitud de la recollida i de l'intercanvi de dades personals ha augmentat de manera significativa. La tecnologia permet que tant les empreses privades com les autoritats públiques utilitzin dades personals a una escala sense precedents (...). Les persones físiques difonen un volum cada vegada més gran d'informació personal a escala mundial.”*

L'RGPD també es refereix a la necessitat de garantir un nivell uniforme i elevat de protecció de les persones físiques, davant la situació prèvia de divergència entre les regulacions dels diferents estats, que no havien aconseguit un nivell adequat de coherència i homogeneïtat en l'aplicació de les normes de protecció de dades.

Quines novetats ens porta l'RGPD? Doncs no podem dir que ho canvia tot, però sí que altera diverses qüestions, algunes de molt rellevants. En aquest article, enumeraré les novetats que considero de més importància.

Responsabilitat proactiva (*accountability*) i enfocament del risc. Es produeix un canvi de paradigma, ja que l'RGPD exigeix a les organitzacions una actitud conscient, diligent i proactiva, per tal que cadascuna analitzi les dades personals que tracta i amb quines finalitats, quin context i quins són els riscos per als drets i les llibertats de les persones físiques. A partir d'aquí, el responsable i l'encarregat han d'aplicar les mesures tècniques i organitzatives apropiades i, a més, han d'estar en condicions d'acreditar davant de l'autoritat de control i dels interessats que el tractament efectuat s'ajusta a les exigències de l'RGPD. Així doncs, passem d'un sistema en què la norma detallava les mesures de seguretat concretes que calia implementar, d'acord amb la tipologia de les dades, a un sistema més obert en què cada organització, a partir de l'anàlisi que faci, ha d'aplicar les mesures apropiades per a la seguretat de les dades, és a dir per garantir-ne la confidencialitat, integritat i disponibilitat.

La mort del consentiment tàcit. Fins ara, hi havia una pràctica consistent a informar d'un determinat tractament, que s'entenia consentit si no s'indicava expressament el contrari. Això ja no és possible amb el nou RGPD, que exigeix que el consentiment sigui inequívoc i estigui basat en una declaració o acció clarament afirmativa.

Desapareix l'obligació de notificar fitxers. Amb l'RGPD, desapareix el deure formal de notificar els fitxers a les autoritats de control. Ara bé, en consonància amb el principi de responsabilitat proactiva, les entitats del sector públic estan obligades a disposar d'un registre de les activitats de tractament efectuades sota la seva responsabilitat.

Delegat de protecció de dades. Possiblement, una de les novetats més destacades de l'RGPD és l'obligació de designar aquesta figura del delegat, que és obligatòria per a les entitats que formen part del sector públic. Ha de tenir uns coneixements especialitzats del dret, pràctica en la protecció de dades i les capacitats i habilitats necessàries per exercir adequadament les funcions que té atribuïdes, que són, en essència, de supervisió i assessorament al responsable i a l'encarregat del tractament.

Notificació de violacions de seguretat. Si el responsable té coneixement d'una violació de la seguretat de les dades personals, l'ha de notificar a l'autoritat de control en 72 hores, tret que sigui improbable que aquesta violació constitueixi un risc per als drets i les llibertats de les persones. Si aquest risc s'ha de qualificar com a "alt", el responsable ha de notificar la violació també als afectats. En tot cas, fins i tot quan no és pertinent notificar-la a l'autoritat, el responsable l'ha de documentar internament, a fi de permetre que l'autoritat en pugui fer les verificacions pertinents.

Transparència. Aquest és un principi d'actuació que obliga el responsable del tractament a facilitar a l'interessat un seguit d'informació, de manera concisa, transparent, intel·ligible i d'accés fàcil, amb un llenguatge clar i senzill. Aquest principi s'ha de respectar tant en el moment de complir el deure d'informació com a l'hora de respondre una sol·licitud d'exercici del dret d'accés.

Nous drets dels interessats. Fins ara teníem els drets d'accés, rectificació, cancel·lació i oposició (ARCO). Amb el nou RGPD, el dret de cancel·lació es converteix en dret de supressió (o dret a l'oblit).

Així mateix, s'afegeixen nous drets *habeas data*, en concret el dret a la limitació del tractament, que comporta el marcat de les dades conservades per limitar-ne el tractament. I també el dret a la portabilitat de les dades, com el dret de qualsevol interessat a rebre les seves dades en un format estructurat, d'ús comú i de lectura mecànica, i que es transmetin a un altre responsable si es compleixen uns requisits determinats.

Multes molt elevades. Per tal d'assegurar al màxim la protecció efectiva de les dades personals, l'RGPD reforça els poders d'investigació i sanció de les autoritats de control. Respecte d'això, el considerant 148 afirma que qualsevol infracció de l'RGPD *"ha de ser castigada amb sancions, incloses multes"*. I l'article 83.1 de l'RGPD preveu que les multes siguin *"efectives, proporcionades i dissuasives"*. Per a les entitats del sector públic, l'RGPD faculta cada estat per decidir "si es pot, i en quina mesura, imposar multes administratives".

A grans trets, aquestes són les novetats més rellevants que ens porta l'RGPD. Les organitzacions han disposat de dos anys per adequar-s'hi, però a les autoritats de control som conscients de les dificultats per fer-ho, també en el cas concret de les entitats del sector públic. És per això que l'APDCAT, amb una clara finalitat preventiva, ha dissenyat i divulgat eines, materials i activitats formatives -en aquest darrer cas, en col·laboració amb l'EAPC- per ajudar els responsables i encarregats perquè l'RGPD tingui un *aterratge suau*.

Carles San José Amat

Cap de l'Àrea d'Inspecció de l'Autoritat Catalana de Protecció de Dades

◆ APDCAT, AUTORITAT CATALANA DE PROTECCIÓ DE DADES, CARLES SAN JOSÉ AMAT, FORMACIÓ, INNOVACIÓ, LOPD, PROTECCIÓ DE DADES