Entendre el nou marc regulador de protecció de les dades, amenaça o oportunitat?

Per Daniel Gómez
Director Organització
Andbank

En l'actualitat, les empreses i les organitzacions públiques adquireixen i intercanvien un volum creixent d'informació incloent-hi, entre d'altres, les dades personals dels usuaris.

L'avenç tecnològic dels darrers anys ha conduït l'evolució digital en la relació empresa-client, però alhora ha incrementat significativament els riscos i amenaces de seguretat, deixant palès la necessitat d'establir un nou marc legislatiu que vetlli per la privacitat i per la protecció de les dades personals.

El 24 de maig de 2016, la Unió Europea (UE) va publicar el nou Reglament General de Protecció de dades (RGPD), que entrarà en vigor el proper 25 de maig de 2018 a tota la UE, substituint la regulació actual que es va aplicar fa 20 anys.

El reglament introdueix un marc homogeni en l'àmbit comunitari, que defineix les regles d'actuació per a qualsevol empresa privada o entitat púbica que gestioni dades personals de ciutadans de la UE, indistintament del lloc on es trobin, i amb independència que es tractin de clients, empleats o contactes.

El principal objectiu que persegueix aquesta nova regulació és recuperar el control sobre les dades pròpies com un dret fonamental de tota persona física.

Principals pilars del nou marc normatiu

El nou reglament es pot resumir en l'evolució d'una sèrie d'aspectes clau sobre el marc actual.

En primer lloc, s'amplia el concepte de dada personal a qualsevol informació que permeti relacionar o identificar la persona i incorpora nous tipus com són la localització geogràfica, dades biomètriques i genètiques, les fotografies o, fins i tot, el xip d'identificació de la mascota.

Així mateix, s'amplien els drets del ciutadà respecte al control de les dades pròpies: (i) limitació en el processat de les dades (ii) oblit, que permetrà requerir l'eliminació de les seves dades, i (iii) portabilitat, que permetrà l'extracció de les dades per tal de portar-les a una altra entitat.

Complementàriament, s'introdueix l'obligació d'obtenir un consentiment exprés e inequívoc per als tractaments de les dades que realitzi l'empresa per a fins propis. Això comporta, per tant, definir una política informativa per a facilitar el consentiment, que sigui de fàcil enteniment i accessibilitat, que expliqui per a quins usos es faran servir les dades, qui tindrà accés i per quant de temps es custodiaran.

Una altra de les mesures rellevants serà l'obligació de designar un responsable de protecció de les dades (DPO, *Data Protection Officer*). Les funcions d'aquest nou rol van més enllà de les de l'actual responsable de dades, atès que haurà d'assessorar l'entitat, establint les mesures tècniques i organitzatives apropiades per garantir les obligacions, i supervisar-ne el seu compliment. El DPO actuarà com a enllaç amb les autoritats de control i, entre d'altres obligacions, haurà de notificar tot compromís de seguretat en un termini màxim de 72 hores. S'estima que en tot el territori de la UE es necessitaran uns 28 mil DPO's.

... l'amenaça...

L'adopció de totes aquestes mesures suposarà un repte en sí mateix per a qualsevol entitat. Però més enllà, una de les principals motivacions serà evitar les quantioses sancions en cas

d'infracció de la normativa. Les entitats s'enfrontaran a multes d'un màxim de 20 milions €, o un 4 % del volum de negoci total anual, aplicant l'import de quantia més gran.

Exemples ben recents del que podrà ser l'exigència són les sancions que la Agència Espanyola (AEPD) ha establert a empreses com Whatsapp o Facebook en no haver comunicat als usuaris els usos que es farien de les seves dades i fer-ne ús per a fins propis sense haver obtingut un consentiment explícit. Si bé la sanció actual, 300 mil €, de ben segur no resultarà material per aquestes grans corporacions, estableix una clara advertència.

... i l'oportunitat de transformar

La severitat de les sancions obliga les entitats a revisar totalment tots els seus processos de negoci i de sistemes d'informació, per tal d'incorporar la dada com un requeriment més en la definició.

El govern de les dades obrirà un nou ventall d'oportunitats, tant entorn de la monetització de la dada com en l'oferiment de serveis relacionats amb els drets dels ciutadans. Generar la confiança permetrà fidelitzar el client, però alhora una intel·ligència més gran sobre les seves preocupacions i interessos, que poden afavorir a determinar els productes i serveis que millor encaixen amb les seves necessitats. Mesures com la portabilitat de les dades fomentaran la desintermediació i la lliure competència entre empreses.

Per tant, l'adopció del RGPD, així com d'altres recents normatives europees com el PSD2 (Directiva de serveis de pagament), no deixen de ser dinamitzadors de l'evolució i de la transformació digital en els models de negoci, l'eficiència operativa i l'experiència de client.