RCD ALERT

Desembre 2017

PROTECCIÓ DE DADES I PRIVACITAT

COMPTE ENRERE PER A L'APLICACIÓ DEL REGLAMENT EUROPEU DE PROTECCIÓ DE DADES

RESUM

El 25 de maig de 2018 serà de plena aplicació el Reglament Europeu de Protecció de Dades (GDPR). El GDPR amplia les obligacions i responsabilitat de les empreses i altres entitats que tracten dades personals, d'acord amb l'ampliació dels drets de privacitat dels ciutadans. Aplica també a empreses de fora de la Unió Europea que tractin dades personals de ciutadans de la UE, i preveu importants sancions en cas d'incompliment dels principis bàsics de protecció de dades (s'estableixen multes de fins a 10 o 20 milions d'euros, o de fins al 2% o el 4% del volum de negoci total anual global), amb les quals es volen subratllar les obligacions de les empreses i entitats com la de prevenció i la de responsabilitat proactiva. No ha de ser vist com una amenaça, sinó com una oportunitat, però cal que tots els operadors s'assessorin adequadament per tal d'implementar les mesures necessàries en les seves respectives organitzacions, per garantir que, a 25 de maig de 2018, estiguin en condicions de complir amb el GDPR i en disposició de demostrar-ho.

El Reglament General de Protecció de Dades (GDPR per les seves sigles en anglès), Reglament UE 2016/679, de 27 d'abril de 2016, serà d'aplicació a partir del 25 de maig de 2018, data a partir de la qual serà obligatori en tots els seus elements i directament aplicable en cada Estat membre.

El GDPR s'aplicarà a qualsevol empresa establerta a la UE, i també a empreses no establertes a la UE però que tractin dades personals de ciutadans de la UE, ja sigui per oferir béns i serveis, o controlar el seu comportament dins de la pròpia UE (art. 3 GDPR). En aquest cas, aquestes empreses extracomunitàries hauran de designar un representant a la UE que atengui les consultes de les autoritats i interessats (art. 27 GDPR).

El GDPR es basa en la prevenció i el 'principi de responsabilitat proactiva' de les empreses i altres operadors, el que implica que cada empresa és responsable de complir el GDPR i ha d'estar en disposició d'acreditar-ho (arts. 5.2 i 24.1 GDPR).

Per això, cal que cada empresa s'assessori convenientment i analitzi els seus processos de tractament de dades personals per tal de decidir les mesures necessàries, en funció del seu propi model de negoci, costos d'implantació i riscos existents per als interessats, a fi de garantir el compliment del GDPR.

El GDPR estableix nous drets per als ciutadans, addicionals als ja coneguts drets ARCO (Accés, Rectificació, Cancel·lació i Oposició), com ara el dret de supressió o dret a l'oblit (art. 17 GDPR), el dret de limitació (suspensió i/o conservació) del tractament (art. 18 GDPR), el dret a la portabilitat de les dades incloent la seva transmissió entre empreses (art. 20 GDPR) o el dret a no ser objecte de decisions en base a processos purament automatitzats, com l'elaboració de perfils (art. 22 GDPR).

La referida ampliació dels drets dels interessats comporta, així mateix, un ampli ventall d'obligacions complementàries per a les empreses i altres operadors com ara:

- Les empreses amb més de 250 treballadors o que tractin dades sensibles (com ara les relatives a la salut o que revelin origen ètnic o racial, conviccions religioses o idees polítiques) han de portar un registre d'activitats de tractament de dades (art. 30 GDPR), que a Espanya substituirà la clàssica obligació de declarar els fitxers en l'Agència Espanyola de Protecció de Dades;

- la protecció de dades des del disseny (per exemple, quan una nova aplicació per a mòbils estigui en fase de desenvolupament) i, per defecte, garantint que les dades no siguin accessibles a un nombre indeterminat de persones sense la intervenció de l'interessat (art. 25 GDPR);

- notificar, en cas de violacions de seguretat (pirateria informàtica, virus, etc.) de les dades que constitueixin un risc (arts. 33 i 34 GDPR), a les autoritats i als interessats;

- valorar l'adequació de les mesures de seguretat necessàries segons el risc, com ara el xifrat de dades o la pseudonimització (art. 32.1 GDPR) i implementar-les;

- en determinats supòsits, designar un delegat de Protecció de Dades que supervisi el compliment del GDPR i actuï com a punt de contacte de les autoritats competents (arts. 37-39 GDPR); o

- també en determinats supòsits, avaluar els riscos sobre la privacitat abans d'efectuar determinats tractaments, en particular mitjançant l'ús de noves tecnologies (art. 35 GDPR).

D'altra banda, és aconsellable, com a segell distintiu en la gestió de la protecció de dades, que les empreses i entitats valorin l'adhesió a codis de conducta (art. 40 GDPR) en què es detallin les pràctiques concretes d'un sector, incloent allò relatiu a la protecció de dades, per exemple en relació amb temes com ara la pseudonimització o la informació proporcionada als nens i la seva protecció, ja que això pot ser tingut en compte positivament en la valoració de possibles sancions.

I no podem deixar de fer una referència, precisament, al sistema de sancions (art. 83 GDPR) previst pel GDPR, que estableix bàsicament dos llistats d'obligacions l'incompliment de les quals es sancionaria amb multes de fins a 10 o 20 milions d'euros, o de fins al 2% o el 4% del volum de negoci total anual global d'una empresa (s'optaria per la xifra de més quantia). En línia amb això, l'incompliment dels principis bàsics de protecció de dades o de les obligacions que afecten els drets dels interessats es troben entre les causes d'aplicació de les sancions més elevades.

En definitiva, el GDPR pretén generar un espai europeu de confiança que fomenti, precisament, el desenvolupament de l'economia en l'era digital, dominada per l'activitat *online* i els fluxos transfronterers de dades, a cada segon, a una escala sense precedents fins ara, i en tots els sectors d'activitat.

Per això, les empreses no han de considerar el GDPR com una amenaça, un llast o una càrrega burocràtica i limitadora de la possibilitat de fer negocis (com indica el GDPR (Considerant #4), "el dret a la protecció de dades personals no és un dret absolut"), sinó com un argument de posicionament i com una oportunitat de negoci, perfectament compatible amb el desenvolupament necessari i legítim de l'economia.

La prioritat que cada empresa o institució concedeixi a aquesta qüestió i la transparència amb què l'abordi seran factors competitius i diferenciadors de cada entitat, fet que explica que el mateix GDPR obligui que es promogui la creació de mecanismes de certificació, segells i marques de protecció de dades en els Estats Membres perquè les entitats que ho desitgin puguin demostrar davant els seus interlocutors el compliment de la norma (art. 42.1 GDPR).

TÉ ALGUNA CONSULTA?

Des de l'Àrea de Protecció de dades i Privacitat treballem per poder resoldre els dubtes que pugui plantejar aquest nou reglament i la seva afectació a l'activitat de les diverses empreses i organitzacions. Si té alguna consulta, no dubti en posar-se en contacte amb nosaltres.

CONTACTE:

Àrea de Protecció de dades i Privacitat d'RCD
rcd@rcd.legal
www.rcd.legal