El Reglament General de Protecció de Dades

• Entrada imminent d'una normativa que portarà molts maldecaps a algunes empreses i entitats

El proper 25 de maig de 2018 entrarà en vigor el Reglament (UE) 2016/679 del Parlament 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 –conegut per l'acrònim RGPD.

Tot i que ja fa dos anys de la seva aprovació, i hi ha hagut un lapse de temps considerable per a procedir a la seva posada en marxa a les empreses i la corresponent adaptació, fins al darrer moment moltes empreses no s'hi ha posat i ni la mateixa Administració responsable ha donat solució a alguns dels dubtes plantejats. El present article pretén ser un petit resum recordatori dels aspectes més importants que cal tenir ben en compte, adreçant-vos, per a ampliar la informació, a la fitxa Empresa 2.13 d'octubre de 2017 o al web de l'Agència Espanyola de Protecció de Dades i al de l'Autoritat Catalana de Protecció de Dades.

Les principals novetats i diferències amb l'actual i vigent normativa sobre tractament i protecció de dades personals són les següents:

- Cal que el **consentiment en facilitar les dades personals sigui fet de forma expressa i conscient**, no pot ser tàcita.

- S'introdueix la figura del **delegat de protecció de dades**, que serà la persona que s'ocuparà d'informar i supervisar les obligacions derivades del Reglament, d'assessorar i formar als encarregats del tractament de les dades personals, i fer de connexió amb els titulars de les dades personals. No serà necessari tenir-ne un a totes les empreses, sinó, a aquelles que de forma habitual observin un número d'interessats a gran escala, a les autoritats o organismes públics —inclou, entre d'altres, col·legis professionals, centres docents, establiments financers de crèdit, asseguradores, distribuïdors i comercialitzadors d'energia, prospecció comercial—, o a les que tractin a gran escala dades personals —dades genètiques, salut, origen ètnic, religiós o similars.

Haurà de tenir coneixements en Dret i en matèria de protecció de dades. Podrà formar part de la pròpia plantilla de l'empresa, o ser un tercer aliè contractat mitjançant prestació de serveis. En tot cas, no se li poden imposar instruccions, havent de ser independent en l'exercici del seu càrrec, rendirà comptes només amb els superiors de l'encarregat del tractament de dades i comunicarà a l'autoritat competent qualsevol vulneració de la normativa.

Abans del 25 de maig s'haurà d'haver comunicat a l'Agència Espanyola de Protecció de Dades el nom del delegat de protecció de dades.

- S'incorpora el **principi de responsabilitat proactiva**. El Reglament obliga als responsables dels fitxers a adoptar les mesures de protecció de les dades, així com a demostrar l'eficiència de les mateixes. En aquest punt cal dir que desapareix l'obligació d'inscriure els fitxers de dades a una Agència estatal i també desapareix el Document de Seguretat. Essent la veritable obligació haver adoptat dites mesures de prevenció: còpies de seguretat, control d'accés, seguretat física, política de contrasenyes, etcètera.

En aquest sentit s'implementen les **avaluacions d'impacte relatives a la protecció de dades**. Aquestes seran fetes sota l'assessorament del delegat de protecció de dades, qui col·laborarà amb l'autoritat de control —en el nostre cas l'Agència Espanyola de Protecció de Dades (AEPD). Fonamentalment han d'analitzar els riscos que certes operacions de tractament de dades —com ara origen ètnic, opinió política, convicció religiosa, afiliació sindical, dades biomètriques o de salut, orientació sexual, elaboració de perfils, condemnes i infraccions penals— poden

afectar als drets i llibertats dels interessats, incloure les mesures per afrontar-los i les mesures i mecanismes de protecció.

- Cada responsable ha de portar un **registre de les activitats de tractament efectuades** sota la seva responsabilitat. Aquest registre ha de contenir tota la informació següent: nom i dades de contacte del responsable i del delegat de protecció de dades, les finalitats del tractament, descripció de les categories d'interessats i de les categories de dades personals, categories de destinataris als quals s'han comunicat o es comunicaran les dades personals, les transferències de dades personals a un tercer país o a una organització internacional, els terminis previstos per suprimir les diferents categories de dades, descripció general de les mesures tècniques i organitzatives de seguretat.

- Els **principals drets dels ciutadans s'amplien**, respecte de l'actual normativa. Entre els principals tenim:

– Informació que s'ha de facilitar quan s'obtenen les dades: identitat del responsable i del delegat de protecció de dades, finalitat específica —no genèrica— i tractament a què es destinen les dades, destinataris de les dades, si es té intenció de transferir les dades, termini durant el qual es conservaran les dades, el dret d'accés, rectificar i suprimir les dades, o limitar el tractament així com la portabilitat de les dades.

– Obtenir informació del responsable del tractament de si es tenen dades personals, quines són les seves finalitats, la categoria de les dades, els seus destinataris, el termini de conservació de les dades, i el dret al seu accés, rectificar, suprimir i la portabilitat de les dades.

– Dret de rectificació de les dades personals inexactes. Els canvis han de ser notificats als destinataris als quals se'ls ha comunicat les dades personals.

– Dret de supressió ("dret a l'oblit") de les dades quan ja no siguin necessàries per a la finalitat per a la qual es van obtenir. Si el responsable del tractament ha fet públiques les dades personals, tenint en compte la tecnologia disponible i el cost d'aplicar-la, s'ha d'adoptar mesures raonables, incloses mesures tècniques, per informar els responsables que estan tractant aquestes dades de la sol·licitud de l'interessat de suprimir qualsevol enllaç a aquestes dades personals, o qualsevol còpia o rèplica existent.

– Limitació del tractament de les dades, quan hi ha una inexactitud i s'ha de comprovar, o quan en un tractament il·lícit per comptes de la supressió es demana la limitació.

– Dret a la portabilitat de les dades per a transmetre-les a un altre responsable de tractament.

- Obligació de **notificar les violacions de seguretat de les dades personals**, en un màxim de 72 hores. Es refereix als casos en els que l'escletxa de seguretat suposi la destrucció, pèrdua o alteració accidental o il·lícita de dades personals trameses, conservades o tractades d'altre forma, o la comunicació o accés no autoritzats a dites dades.

Hauran de tenir-se en compte diferents criteris a l'hora de determinar si s'ha produït el risc o no: tipus d'escletxa soferta, la naturalesa, volum i caràcter sensible de les dades personals afectades, la gravetat de les possibles conseqüències per als titulars de les dades —morals, econòmics, reputació, etcètera—, que afecti a categories especials de dades o responsables del tractament específics.

La comunicació s'haurà de fer a l'autoritat competent, indicant les dades de contacte del delegat de protecció de dades de l'empresa o entitat, les possibles conseqüències de l'escletxa de seguretat i les mesures de seguretat adoptades o proposades pel responsable del tractament. En els casos d'alt risc pels drets i llibertats de les persones físiques, caldrà notificar-ho individualment als interessats. Excepte que això suposi un esforç desproporcionat o el responsable hagi dotat mesures posteriors que mitiguin o resolguin la violació.

- **Increment considerable de les sancions**, que poden arribar fins als 20 milions d'euros o el 4% del volum de negoci anual global d'una empresa. Pel cas de les violacions de seguretat cal tenir present que, apart de la multa que se'n pugui derivar, hi ha els efectes de la pèrdua de reputació de l'empresa respecte de la societat i clientela, el que sovint pot ser molt més greu.

Actualment ja hi ha en tràmit un projecte de Llei Orgànica de dades de caràcter personal per tal de fixar determinats aspectes que el Reglament comunitari no ha concretat o sobre el qual dóna marge als Estats Membres per a regular-ho: fixar en els 13 anys l'edat de consentiment per al tractament de dades, tenir present les dades de les persones mortes en base a la petició dels hereus, el principi de transparència respecte al dret d'informació, i els drets d'accés, rectificació, supressió, limitació i portabilitat. Aquesta substituirà l'actual Llei Orgànica 15/1999 de protecció de dades de caràcter personal.

Per tot plegat és molt aconsellable que les empreses i entitats que encara no hagin fet els deures, ho facin en breu. Especialment el nomenament del delegat de protecció de dades, implantar els protocols de notificació de les escletxes de seguretat, així com l'adopció de les mesures de seguretat adients per evitar ciberatacs o filtració de dades personals.