CINC | ASSESSORIA

S'ACOSTA LA FINALITZACIÓ DEL TERMINI PER ADAPTAR-SE AL REGLAMENT GENERAL DE PROTECCIÓ DE DADES (RGPD)

A partir del pròxim 25 de maig de 2018 entra en vigor el nou Reglament General de Protecció de Dades (RGPD), relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, una norma que serà d'aplicació obligatòria a partir d'aquesta data i que imposa a les empreses nombrosos deures en relació a la privacitat.

Queda, a més, pendent l'aprovació de la nova Llei orgànica de protecció de dades, que es troba actualment en tramitació parlamentària i que molt probablement no estarà llesta per al pròxim 25 de maig, data d'aplicació del reglament europeu. De totes maneres, això no suposa cap tipus d'avantatge o inconvenient, ja que el reglament europeu serà plenament exigible de totes maneres.

En què consisteix el RGPD?

El RGPD és un tipus de norma que té aplicació directa en tots els estats de la UE i, per tant, no és necessari cap tipus de mecanisme de transposició específic. Dit d'una altra forma, no fa falta que existeixi cap llei espanyola perquè el reglament europeu resulti obligatori, és exigible com si fos una llei nacional.

La meva empresa encara no s'ha adaptat al RGPD: per on començo?

És important establir un mapa de ruta per complir amb el nou reglament, ja que hi ha nombroses decisions jurídiques rellevants a tenir en compte.

El primer pas que totes les empreses haurien d'executar és identificar i analitzar les àrees de risc i documentar els tractaments de dades personals que es duen a terme, a través d'un inventari de totes les activitats de tractament que realitza la companyia. D'aquesta manera serà més senzill classificar les dades d'acord amb: la seva naturalesa, finalitat, categoria, origen, si són susceptibles de ser compartides, etc.

Quins són els canvis i obligacions derivats del RGPD que hauran d'assumir les empreses i a quins riscos s'enfronten en cas d'incompliment?

Són moltes les obligacions que tant les empreses, autònoms i organismes públics i privats que tractin dades de caràcter personal han de conèixer i el temps és escàs, per la qual cosa és necessari adoptar sense dilació les decisions necessàries per arribar a aquest termini en situació de compliment. El risc de no fer-ho és el de possibles sancions: les multes poden arribar fins als 20 milions d'euros o el 4% de la facturació anual global de l'infractor. L'autoritat de control pot actuar d'ofici o per denúncia dels interessats.

Pel que respecta als canvis i obligacions que afecten a les empreses, podem destacar entre d'altres els següents:

• Delegat de Protecció de Dades (DPD/DPO). El reglament obliga als qui realitzin certs tractaments, a nomenar un DPO, que podrà ser extern o intern. Un DPO haurà de ser una persona experta en protecció de dades i en mètodes i tècniques de seguretat de la informació.

• Exigència de la realització d'una avaluació d'impacte relativa a la protecció de dades per a certs tractaments.

• Violacions de la seguretat de les dades personals. Obligatorietat de comunicar-les en un termini de 72 hores a l'Agència Espanyola de Protecció de Dades, i en casos greus, als propis afectats.

• S'elimina el consentiment tàcit (per silenci), la qual cosa obligarà a les empreses a recaptar un nou consentiment per poder mantenir totes aquelles dades que en el passat es van obtenir tàcitament o buscar-los una altra cobertura legal.

• S'amplien les obligacions d'informació als afectats, la qual cosa obligarà posar-los al dia en aquesta informació als ja existents.

• S'amplia el contingut mínim en els contractes d'accés a dades per part de tercers, per la qual cosa s'hauran d'establir de nou els contractes amb els encarregats de tractament, atès que els actuals no compleixen amb el RGPD.

• El RGPD no estableix diferenciació entre dades personals i dades 'professionals' (dades de contacte de persones físiques que presten els seus serveis en una persona jurídica i empresaris individuals) com va establir el vigent reglament, la qual cosa obligarà a les empreses a haver de realitzar accions informatives a aquesta categoria de dades.

1.- CONSENTIMENT EXPRÉS

S'estableix l'obligació de les empreses d'obtenir un consentiment exprés, inequívoc i verificable, i no tàcit de la informació que s'obtingui dels seus clients. Es considera consentiment tàcit quan, després d'haver rebut la informació corresponent, l'usuari no diu que no (exemple: "si no em contestes abans de 30 dies, llavors t'enviaré informació comercial de tercers").

Per tant, el consentiment tàcit es considera vàlid, sempre que no es tracti de dades especialment protegides.

Atenció: a partir de l'entrada en vigor del nou RGPD, no es podrà seguir obtenint el consentiment dels afectats per omissió. Serà necessari revisar tots els tractaments anteriors, per adequar-los a les previsions de la nova normativa.

Pot ser inequívoc i atorgar-se de forma implícita quan es dedueixi d'una acció de l'interessat (per exemple, quan l'interessat continua navegant per una web i accepta així que s'utilitzin cookies para monitorar la seva navegació).

2.- TRANSPARÈNCIA EN LA INFORMACIÓ

Serà necessari que les empreses detallin explícitament i amb un llenguatge comprensible les dades i informació personal requerida a l'usuari o client i solament es podrà tractar les dades en cas que tinguin un interès legítim.

El deure d'informar als afectats sobre l'ús i les finalitats del tractament de dades, sofreix una important modificació amb el nou RGPD, ja que s'amplia considerablement la informació que se'ls ha de subministrar, inclosos aspectes no contemplats fins avui com:

• Base jurídica del tractament
• Intenció de realitzar transferències internacionals
• Dades del delegat de protecció de dades (si n'hi hagués)
• El termini o els criteris de conservació de la informació
• L'existència de decisions automatitzades o elaboració de perfils
• El dret a presentar una reclamació davant les autoritats de control

Els procediments, models o formularis dissenyats de conformitat amb la LOPD, hauran de ser revisats i adaptats al nou RGPD, tant per adaptar-los al nou contingut del deure d'informar, com per ajustar la seva forma als requisits de precisió i claredat que exigeix la nova normativa.

3.- SEGURETAT

Les empreses estan obligades a informar quan hagin sofert una bretxa de seguretat a les autoritats de control i, depenent de la gravetat, als afectats. Encara que és un assumpte necessari avui dia, el reglament estableix la necessitat de deixar plasmada una estratègia en matèria de seguretat.

En la nova normativa, les mesures de seguretat no apareixen tan detallades, sinó que cada organització haurà de comptar amb un nivell de seguretat adequat en funció dels riscos detectats en l'anàlisi prèvia.

A més, la tipologia de les dades no serà l'única variable a prendre en consideració a l'hora de determinar les mesures tècniques i organitzatives aplicables sinó que, per contra, el nou RGDP té en compte:

- El cost de la tècnica
- Els costos d'aplicació
- La naturalesa, l'abast, el context i les finalitats del tractament
- Els riscos per als drets i llibertats

Atenció. L'esquema de mesures de seguretat previst en el Reglament de desenvolupament de la LOPD no seguirà sent vàlid de forma automàtica. És necessari determinar, cas per cas, les mesures aplicables, sota un enfocament de risc, basat en el principi de la seguretat des del disseny i per defecte.

4.- ENCARREGATS DE TRACTAMENT

També la figura dels encarregats de tractament sofreix importants canvis en la nova regulació. En síntesi, aquests canvis es poden resumir en tres punts:

1) El nou RGPD estableix obligacions expressament dirigides als encarregats de tractament, com:

- Mantenir un registre d'activitats de tractament.
- Determinar les mesures de seguretat aplicables als tractaments que realitzen.
- Designar a un delegat de protecció de dades en els casos previstos pel RGPD.

2) S'accentua el deure de diligència en l'elecció de l'encarregat del tractament, de manera que els responsables hauran de triar únicament encarregats que ofereixin garanties suficients per aplicar mesures tècniques i organitzatives apropiades.

3) Es modifica el contingut mínim que ha d'incloure el contracte amb l'encarregat del tractament, inclosos aspectes com:

- Objecte, durada, naturalesa i la finalitat del tractaments
- Tipus de dades personals i categories d'interessats
- Obligació de l'encarregat de tractar les dades personals únicament seguint instruccions documentades del responsable
- Condicions perquè el responsable pugui donar la seva autorització prèvia, específica o general, a les subcontractacions
- Assistència al responsable, sempre que sigui possible, en l'atenció a l'exercici de drets dels interessats...

Atenció. S'han de revisar tots els contractes per encàrrec de tractament signats amb anterioritat, per verificar si compleixen les noves exigències del RGPD.

5.- DRETS DEL CIUTADÀ

El nou RGPD inclou nous drets com el dret a la portabilitat i el dret a l'oblit, el dret a no ser objecte de decisions individualitzades i el dret a la limitació del tractament.

EL DRET D'ACCÉS: és el dret a conèixer quines dades de caràcter personal teves són tractades per part del responsable, la finalitat d'aquest tractament, l'origen de les dades i si s'han comunicat o es comunicaran a un tercer.

Atenció: segons la LOPD, el responsable del tractament havia de facilitar totes les dades de base de l'afectat, però no còpies o documents. No obstant això, el nou RGPD reconeix expressament el dret dels afectats a obtenir gratuïtament una còpia de les dades personals objecte de tractament.

Si és possible, el responsable del tractament ha d'estar facultat per facilitar accés remot a un sistema segur que ofereixi a l'interessat un accés directe a les seves dades personals.

• EL DRET DE RECTIFICACIÓ: consisteix en la possibilitat de modificar aquelles dades que siguin inexactes o incompletes.

Atenció: a més de rectificar les dades inexactes, s'inclou el dret al fet que es completin les dades personals incompletes, inclusivament mitjançant una declaració addicional.

• EL DRET DE CANCEL·LACIÓ: permet la cancel·lació de dades personals que siguin inadequades o excessives.

Atenció: els interessats tenen dret al fet que les seves dades personals se suprimeixin i deixin de tractar-se:

- Si ja no són necessàries per a les finalitats per les quals van ser recollides o tractades d'una altra manera,
- si els interessats han retirat el seu consentiment per al tractament o s'oposen al tractament de dades personals que els concerneixen,
- si el tractament de les seves dades personals incompleix d'una altra manera el RGPD

• El DRET D'OPOSICIÓ: mitjançant l'exercici d'aquest dret l'interessat es pot oposar al tractament de les seves dades personals en els següents supòsits:

• Quan no sent necessari el seu consentiment per al tractament, existeixi un motiu legítim i fundat referent a la seva concreta situació personal (tret que una llei estableixi el contrari).
• Quan estiguem davant de tractaments de dades personals la finalitat de les quals sigui la realització d'activitats de publicitat i prospecció comercial
• Quan el tractament tingui com a fi l'adopció d'una decisió referida a la seva persona, basada únicament en un tractament automatitzat de les seves dades personals

• DRET A L'OBLIT: és una manifestació dels drets de cancel·lació o oposició en l'entorn en línia. El responsable del tractament que hagi fet públiques dades personals, està obligat a indicar als responsables del tractament que estiguin tractant aquestes dades personals, que en suprimeixin tot enllaç, o les còpies o les rèpliques.

Atenció: el dret a l'oblit té algunes limitacions com la llibertat d'expressió i el dret a la informació, l'interès públic en l'àmbit de la salut, la recerca així com la defensa de reclamacions.

• DRET A LA PORTABILITAT DE LES DADES: és una forma avançada del dret d'accés pel qual la còpia que es proporciona a l'interessat s'ha d'oferir en un format estructurat, d'ús comú i lectura mecànica. Implica que les dades personals de l'interessat es transmeten directament d'un responsable a un altre, sense necessitat que siguin transmesos prèviament al propi interessat, sempre que això sigui tècnicament possible.

• DRET A NO SER OBJECTE DE DECISIONS INDIVIDUALITZADES: l'interessat ha de tenir dret a no ser objecte d'una decisió, que pot incloure una mesura, que avaluï aspectes personals relatius a ell, i que es basi únicament en el tractament automatitzat i produeixi efectes jurídics en ell o l'afecti significativament de manera similar.

• DRET A LA LIMITACIÓ DEL TRACTAMENT: sol·licitar al responsable que suspengui el tractament de dades quan:

• S'impugni l'exactitud de les dades, mentre es verifica aquesta exactitud pel responsable.
• L'interessat ha exercitat el seu dret d'oposició al tractament de dades, mentre es verifica si els motius legítims del responsable prevalen sobre l'interessat.
• El tractament sigui il·lícit i l'interessat s'oposi a la supressió de les dades personals i sol·liciti en el seu lloc la limitació del seu ús.
• El responsable ja no necessiti les dades personals per a les finalitats del tractament, però l'interessat les necessiti per a la formulació, l'exercici o la defensa de reclamacions.

6.- REGISTRE

El reglament exigeix l'obligació de registrar documentalment les operacions de tractament, tant per part dels responsables del fitxer com pels encarregats de tractament.

Quines pàgines web han de sol·licitar un consentiment?

Qualsevol pàgina web o botiga en línia que reculli dades personals a través de formularis (de contacte, de subscripció o de sol·licitud de pressupost) ha de sol·licitar el consentiment dels usuaris per poder tractar les seves dades.

Puc enviar comunicacions comercials a clients sense consentiment?

Es permet l'enviament de missatges publicitaris o comercials per correu electrònic a aquells usuaris que prèviament ho haguessin sol·licitat o autoritzat de forma expressa. També s'admet l'enviament de comunicacions comercials a aquells usuaris amb els quals existeixi una relació contractual prèvia, en aquest cas el proveïdor podrà enviar publicitat sobre productes o serveis similars als contractats pel client.

Tens dubtes sobre la implantació de la RGPD?

Contacta sense cap compromís amb el Departament de Protecció de Dades de CINC Assessoria (monica.vilallave@cinc.es) per resoldre tots els teus dubtes.

Cordialment,

CINC Assessoria d'Empreses