MET ASSOCIATS

C/ GIRONA 33 - GRANOLLERS
93 861 13 44
info@metassociats.com

LA SEVA EMPRESA COMPLEIX EL NOU REGLAMENT DE PROTECCIÓ DE DADES EUROPEU QUE VA ENTRAR EN VIGOR EL 25 DE MAIG DE 2018?

Ja és una realitat. El passat 25 de maig de 2018 va entrar el vigor el nou Reglament general de protecció de dades de la Unió Europea (RGPD), que afecta tant a les empreses, com als autònoms i organismes públics i privats que tractin dades de caràcter personal. Entre els grans canvis, s'hauran de comptar amb el consentiment explícit dels usuaris per a l'ús de les seves dades; aclarir quina informació tenen, on, quant temps, qui l'usa i per a què; complir amb el dret a l'oblit; i nomenar un delegat de dades que vetllarà pel compliment de la normativa. L'incompliment de la nova normativa podria arribar a implicar sancions de fins a 20 milions d'euros o del 4% del volum total global del negoci de la companyia, amb l'evident i greu perjudici de reputació que també suposaria per a l'organització.

Benvolgut/da client/a:

El passat 25 de maig de 2018 va entrar 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 és d'aplicació obligatòria i que imposa a les empreses nombrosos deures en relació a la privadesa.

A més queda pendent l'aprovació de la nova Llei orgànica de protecció de dades, que es troba actualment en tramitació parlamentària. De totes maneres, això no suposa cap tipus d'avantatge o inconvenient, ja que el reglament europeu serà plenament exigible de totes maneres.

> **Atenció.** El RGPD és un tipus de norma que té aplicació directa en tots els estats de la UE i, per tant, no requereix 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.

Les companyies que operin a Europa hauran d'acatar el RGPD, independentment que estiguin registrades en països que no pertanyen a la Unió Europea.

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

Què entenem per dades personals?

Es defineixen les dades personals de les persones com tota aquella informació que es pot vincular directament o indirecta a una persona. És a dir, poden anar des del nom complet o domicili d'un individu fins a informació sobre la seva condició social, estat civil o inclusivament adreça IP.

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.

Alguns dels punts bàsics d'aquest reglament són:

- Les dades personals són sempre del titular, no de qui les tracta.
- Les dades només s'han d'utilitzar per a la finalitat per la qual van ser recaptades.
- Els interessats poden exercir el dret a la portabilitat de les seves dades, i el responsable del tractament està obligat a facilitar una còpia completa de les dades en suport electrònic.

Les persones que viuen a la UE tenen dret a:

- Rebre informació clara i comprensible sobre qui processa les seves dades i per què.
- Accedir a les dades que les organitzacions tenen sobre ells.
- Demanar que s'eliminin les dades personals si no existeix un motiu legítim per guardar-les.
- Poder corregir les dades si són incorrectes.
- Moure les dades d'un proveïdor de serveis, com el correu electrònic o xarxa social, a un altre.

LES CLAUS DEL NOU RGPD

1. Consentiment exprés, no tàcit

La nova normativa estableix que les empreses han de comptar amb el permís exprés de l'usuari per disposar i utilitzar les seves dades. Fins ara valia amb el permís tàcit, és a dir, la presumpció que l'usuari acceptava el que no rebutjava.

Per procedir a la recollida i al tractament de dades personals les organitzacions han d'haver obtingut prèviament un acord escrit, clar o explícit dels titulars de les dades.

Per tant, les empreses necessitaran obtenir el consentiment voluntari, específic, inequívoc i informat de les persones per processar les seves dades. També necessitaran que els usuaris optin per acceptar el processament de les seves dades, no serà vàlid donar-los solament una opció "opt-out" o exclusió. En altres paraules, les empreses ja no podran demanar als consumidors que marquin una casella després d'un extens conjunt de termes i condicions que la majoria dels usuaris mai llegeix.

2. La legalitat del processament de dades

Les empreses que processin dades personals s'han d'assegurar que és legal, just i transparent. No poden usar dades per a finalitats diferents d'aquelles per a les quals es van recopilar, amb excepcions limitades.

El processament de dades és legal si:

- Un individu ha donat el seu consentiment.
- És necessari per a l'execució d'un contracte.
- És necessari complir una obligació legal en virtut de la legislació nacional o de la UE.
- És necessari per protegir els interessos vitals d'un individu.
- És necessari dur a terme una tasca d'interès públic en virtut de la legislació nacional o de la UE.
- És en interès legítim de la companyia, sempre que no s'imposi sobre els drets i llibertats fonamentals d'un individu.

Si una empresa va recopilar dades sobre la base del consentiment, no pot usar-los per a altres finalitats.

3. Temps i ús concret

Les companyies no només estan obligades al consentiment exprés, sinó que han d'especificar l'ús i el temps concret que tenen pensat disposar d'aquestes dades. El RGPD estableix que s'han de guardar no més del "temps necessari".

4. Portabilitat de dades

El RGPD preveu un mecanisme de portabilitat que ofereix la possibilitat de passar d'un servei a un altre. Un usuari pot sol·licitar a qualsevol empresa que li atorgui accés a totes les dades personals recol·lectades amb anterioritat, i d'aquesta forma transferir-les a una altra companyia, sí així ho desitja.

5. Robatori de dades

A més d'informar clarament als ciutadans per què i com processen les seves dades personals, hauran d'informar sobre possibles bretxes de seguretat en un termini màxim de 72 hores. Si, per exemple, un banc sofreix un ciberatac, els seus clients ho hauran de conèixer abans de tres dies.

6. Descàrrega de tota la informació a un «clic»

Els usuaris tenen dret a saber tota la informació que les companyies posseeixen sobre ells i a tenir una còpia electrònica.

7. El dret a l'oblit

Encara que ja estava en vigor, a partir d'ara es reforça l'anomenat «dret a l'oblit» i podran sol·licitar a serveis d'internet i empreses que tracten dades personals que esborrin totes les seves dades o que s'estableixi el límit de temps que l'usuari dóna permís d'ús de la seva informació.

8. Més protecció dels menors

L'edat mínima augmenta dels 14 als 16 anys per accedir als diferents serveis digitals.

9. La lletra petita, reflectida de forma clara

El nou reglament estableix que els termes d'ús i les polítiques de privadesa de dades s'han de redactar i s'han de publicar d'una manera més senzilla i clara, és a dir, comprensible per a tothom.

10. El registre de fitxers a l'AEPD:

Al contrari que fins ara, la nova normativa no obliga a registrar fitxers a l'Agència Espanyola de Protecció de Dades (AEPD). Tot el compliment de la normativa serà responsabilitat dels obligats (institucions, empreses i organitzacions), que internament establiran els mitjans per a l'aplicació de la normativa.

Què passarà amb els fitxers registrats? Serà una obligació complerta sota una normativa anterior, ja no hi haurà cap procediment de presentació o de consulta dels fitxers comunicats.

11. Noves regles per a processadors de dades

El RGPD distingeix entre "controladors" de dades i "processadors" de dades. Un controlador de dades determina per què s'han de recopilar i processar les dades personals i com. Un processador de dades solament processa dades personals en nom del controlador i generalment és una empresa externa.

Per exemple, un detallista que contracta una empresa de recursos humans per manejar la nòmina i altres funcions és el controlador de dades, mentre que l'empresa de recursos humans és el processador de dades.

Sota el RGPD, els processadors de dades han de garantir els mateixos estàndards que els controladors i garantir que compleixin amb els requisits de la llei. Hi ha d'haver un contracte legal entre un processador i un controlador, i un processador no pot contractar una altra companyia per processar dades sense el consentiment del controlador.

12. Delegat de protecció de dades

Una de les exigències que introdueix el RGPD és la designació obligatòria d'un delegat de protecció de dades o Data Protection Officer (DPO, per les seves sigles en anglès). Ara neix una figura especialitzada en dret de protecció de dades que es crea al costat de les ja existents de responsable i encarregat del tractament de les dades. Les seves funcions s'orienten a garantir el compliment del reglament i assessorar al responsable del tractament de dades.

Les seves funcions són vetllar o supervisar que es realitza el compliment de la normativa de LOPD adequadament, en el cas d'autoritats i organismes públics, entitats que realitzin una observació habitual i sistemàtica de les persones a gran escala, i entitats que tinguin entre les seves activitats principals el tractament, també a gran escala, de dades sensibles.

13. Noves sancions per incompliment:

La quantia de les multes puja de forma substanciosa per evitar el que es coneix com les "infraccions rendibles". Per això, el RPGD parla que és possible xifrar les administratives amb quantitats d'entre 10 i 20 milions d'euros. Si fa referència a una empresa, la multa podria ascendir al 2 o 4% del volum de negoci total, sobre la base de l'anual global de l'exercici financer anterior.

PAUTES A SEGUIR:

1. Actualitzi els seus documents legals i realitzi auditories internes

En aquest primer punt, s'haurà de tenir en compte què es necessita per ajustar-se al nou reglament en cada cas particular.

2. Sol·liciti el certificat o permís per poder processar dades

Si el consentiment actual que té no compleix amb la nova normativa, haurà de sol·licitar-lo de nou.

3. Organitzi una auditoria d'informació

Li permetrà explicar als seus clients perquè emmagatzema les seves dades i com treballa amb elles, així com actualitzar les dades dels empleats.

4. Informi al seu equip de treball

És important que el seu equip sàpiga què és el RGPD i com pot afectar a l'empresa. A més de formar-lo perquè dugui a terme els procediments adequats per complir la normativa.

5. Eliminació de dades

És indispensable tenir un sistema eficient i eficaç que li permeti esborrar les dades quan se sol·liciti o no siguin necessàries.

6. Situació de crisi

És necessari elaborar i establir una estratègia de gestió de crisi per si la situació ho requerís.

7. Mostri que està complint la normativa

Actualitzi els seus diferents canals, pàgina web, xarxes socials i suports varis i posi de manifest que està posant en pràctica i complint el RGPD.

8. Canals d'accés

Aquells que estiguin interessats a formar part de les seves bases de dades, acceptin els termes i ho sol·licitin, se'ls inclourà. Per contra, aquells que no hagin donat la seva autorització no se'ls estarà permès i no haurien d'entrar a formar part de la base de dades de la companyia.

9. Protecció de dades per a menors de 16 anys

Els menors de 16 anys necessitaran el permís dels seus pares o tutor amb la nova Llei de protecció de dades.

10. Nou càrrec: delegat de protecció de dades (DPD)

Es recomana incloure la figura de delegat de protecció de dades per assegurar que es respecta i compleix amb l'establert en la RGPD. Aquest punt no és obligatori, però la UE sí que el recomana. El perfil de DPD abasta des d'un professional extern a l'empresa o algun treballador que n'assumeixi el rol.

Per a més informació, pot consultar també la pàgina web de l'AEPD:

https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

Es poden posar en contacte amb aquest despatx professional per qualsevol dubte o aclariment que puguin tenir sobre aquest tema.

Una salutació cordial,

MET ASSOCIATS