NOVETATS EN EL NOU REGLAMENT EUROPEU DE PROTECCIÓ DE DADES (RGPD)

El nou reglament europeu de (UE) 2016/679, conegut com a **NOU REGLAMENT EUROPEU DE PROTECCIÓ DE DADES (RGPD),** que va entrar en vigor el maig de 2016, serà d'obligat compliment a partir del **25 de maig de 2018**, i, per tant, també per a les microempreses i les petites i mitjanes empreses[1]. Actualment, a Espanya s'està treballant en el Projecte de Llei Orgànica de Protecció de Dades Personals (LOPD), que entrarà en vigor en aquesta mateixa data.

L'objectiu del nou Reglament consisteix a establir un marc europeu comú en matèria de protecció de dades, per tal que totes les empreses i organitzacions que tracten dades de ciutadans europeus s'atenguin a única legislació en tota la UE, evitant així diferències de criteris i règims sancionadors segons el país en el qual es realitzi el tractament.

Abans d'aquesta data, les empreses han d'adaptar-se a la nova normativa, ja que en cas contrari podrien enfrontar-se a sancions de fins a 20 milions d'euros o el 4% de la facturació, danys en la reputació de l'empresa i la impossibilitat de signar contractes si no es donen les garanties adequades.

Què han de fer les empreses?

Totes les empreses estan obligades a preparar i implantar les mesures necessàries que estableix aquest reglament.

Les empreses que actualment compleixen amb la LOPD hauran de revisar els processos i sistemes d'informació amb tractaments de dades personals.

Principals novetats:

- ***Consentiment exprés.*** És un dret fonamental en el tractament de dades personals. En aquest sentit, el Reglament exigeix que aquest sigui lliure, informat, específic i inequívoc, i mai s'ha de deduir del silenci o de la inacció dels usuaris.
    - Per aquest motiu, la nova normativa requereix que els interessats manifestin aquest consentiment de forma expressa i revocable, per la qual cosa a partir del 25 maig 2018 no s'admetran altres tipus de consentiment (consentiment tàcit, per exemple).

[1] Reglament (UE) 2016/679, de 27 d'abril: Considerant núm. 13

- *Transparència i informació a l'interessat.* Tota informació subministrada a l'interessat s'ha de proporcionar de manera concisa, transparent, intel·ligible i fàcilment accessible, amb un llenguatge clar i senzill.

- *Adaptació de clàusules i polítiques informatives.* És obligatori informar els clients de les novetats que estableix la nova normativa de LOPD, mitjançant les eines de comunicació de l'empresa com: pàgines web, correu electrònic o butlletins informatius.

- *Avaluació de l'impacte en la protecció de dades.* Es tracta d'una eina que té com a finalitat assegurar la privacitat de les dades personals des del disseny del tractament i, d'aquesta manera, analitzar si posa en risc els drets dels interessats. Un cop obtinguts els resultats, cal aplicar les mesures de seguretat pertinents.

  L'Agència Espanyola de Protecció de Dades posa a disposició de totes les organitzacions les Directrius per a l'avaluació de l'impacte en la protecció de dades i la Guia d'anàlisi del risc. El RGPD estableix que les organitzacions que tracten dades personals han de realitzar una anàlisi de risc amb la finalitat d'establir les mesures que siguin necessàries per garantir els drets i llibertats de les persones. En aquells casos en què els tractaments impliquin un risc alt per a la protecció de les dades, el RGPD disposa que aquestes organitzacions estan obligades a realitzar una avaluació d'impacte[2].

- *Dret a la portabilitat de les dades*. Aquest dret implica que les dades de l'interessat es transmetran (prèvia sol·licitud) d'un responsable a un altre, sense necessitat que siguin transmesos prèviament a l'interessat, i sempre que això sigui tècnicament possible.

- *Nomenament d'un Delegat de Protecció de Dades*. És necessari que les empreses que tinguin un tractament massiu de dades personals comptin amb un Delegat de Protecció de dades (DPO, *Data Protection Officer*).

- *Obligació de notificar falles de seguretat.* Amb el nou Reglament s'han de notificar les anomenades "violacions de seguretat de les dades". El termini per realitzar aquesta comunicació és dins de les 72 hores següents al moment en què el responsable tingui constància d'aquest fet.

- *Introducció de certificats i segells*. Amb la finalitat d'ajudar les empreses a impulsar la seva reputació corporativa i la seva

[2] http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_02_28-ides-idphp.php

competitivitat, s'introdueixen nous mecanismes de certificació que garanteixen el compliment de la normativa europea i la qualitat de la protecció de dades.

- *Adhesió a codis de conducta.* Faciliten la correcta aplicació de la Llei de Protecció de Dades en diferents àmbits sectorials. Aquests codis són de caràcter voluntari i només obliguen els qui es comprometin a aplicar les seves disposicions.

És necessari que les empreses tinguin un Delegat de Protecció de Dades?

El nou Reglament General de Protecció de Dades (RGPD) i el Projecte de Llei de LOPD estableixen com a element clau la figura **del Delegat de Protecció de Dades**, per tal de garantir el compliment de la normativa de protecció de dades en les organitzacions, sense substituir les funcions que desenvolupen les autoritats de control.

Aquesta figura, coneguda popularment com **DPO** (*Data Protection Officer*), pot ser interna o externa, persona física o jurídica. Haurà de tenir autonomia, recursos necessaris i accés total a les dades i tractaments. Ha de tenir independència, no pot rebre instruccions, ni pot ser sancionat pel desenvolupament de les seves funcions.

Segons el Reglament i el Projecte de Llei de LOPD, serà obligatòria la presència d'un Delegat de Protecció de Dades (DPO) a les següents empreses:

- Autoritats i organismes públics.
- Quan es realitzi el tractament a gran escala de dades sensibles.
- Col·legis professionals i els seus consells generals.
- Centres docents que ofereixen ensenyament i a les universitats públiques i privades.
- Les empreses que presten serveis de la societat de la informació quan elaborin a gran escala perfils dels usuaris del servei.
- Les entitats d'ordenança, supervisió i solvència d'entitats de crèdit.
- Els establiments financers de crèdit.
- Les entitats asseguradores i reasseguradores.
- Les empreses de serveis d'inversió.
- Els centres sanitaris legalment obligats a guardar historials clínics dels pacients.
- Les entitats que tinguin com un dels seus objectius l'emissió d'informes comercials que puguin referir-se a persones físiques.

- Les operadores que desenvolupin l'activitat del joc mitjançant canals electrònics, informàtics, telemàtics o interactius.

- Qui desenvolupi les activitats de seguretat privada.

- Els distribuïdors i comercialitzadors d'energia elèctrica i gas natural.

- Les entitats responsables de fitxers comuns per a l'avaluació de la solvència patrimonial i crèdit o dels fitxers comuns, per a la gestió i prevenció del frau, incloent-hi els responsables dels fitxers de prevenció de blanqueig de capital i finançament del terrorisme.

- Les entitats que desenvolupin activitats de publicitat i prospecció comercial, les d'investigació comercial i de mercats, quan es porten a terme tractaments basats en les preferències dels afectats o es realitzin activitats que impliquin l'elaboració dels seus perfils.

Encara que no sigui obligatòria, la figura del DPO no eximeix les empreses de complir amb la responsabilitat de realitzar un tractament correcte de les dades.

Quines són les funcions del Delegat de Protecció de Dades?

- Informar i assessorar el responsable o l'encarregat i els treballadors sobre les obligacions que imposa la normativa de protecció de dades.
- Supervisar que es compleix la normativa.
- Assessorar respecte de l'avaluació d'impacte relativa a la protecció de dades.
- Cooperar amb l'autoritat de control.
- Actuar com a punt de contacte per a qüestions relatives al tractament.

El Delegat de Protecció de Dades s'ha de nomenar tenint en compte les seves qualificacions professionals i, en particular, el seu coneixement de la legislació i la pràctica de protecció de dades. Això no significa que el DPD hagi de tenir una titulació específica. Tenint en compte que entre les funcions del DPD s'inclou l'assessorament al responsable o l'encarregat en tot el referent a la normativa sobre protecció de dades, els coneixements jurídics en la matèria són, sens dubte, necessaris.

L'Agència Espanyola de Protecció de Dades (AEPD) ha impulsat una certificació amb la col·laboració de l'Entitat Nacional d'Acreditació (ENAC), per garantir la seguretat en el tractament de dades a totes aquelles empreses que incorporin la figura del Delegat de Protecció de Dades. Per poder certificar-se s'estableix una sèrie de requisits bàsics o previs que hauran de tenir els candidats a la certificació[3].

[3] https://www.agpd.es/portalwebAGPD/temas/certificacion/index-ides-idphp.php

Llista de verificació simplificada

El passat 26 de gener de 2018 l'AEPD va fer pública la Guía del RGPD para responsables de tratamiento.

Aquest document conté una llista de verificació simplificada[4] que inclou les principals qüestions que **els responsables del tractament de dades que realitzin un nombre limitat de tractaments** hauran de formular-se, prèviament, si volen confirmar que la seva organització es troba en condicions de fer una correcta aplicació del RGPD.

Les qüestions que s'inclouen en aquesta llista de verificació simplificada estan relacionades amb:

- La identificació de la base jurídica per al tractament de les dades
- La verificació de la informació que es proporciona als interessats
- L'establiment d'un registre d'activitats en el tractament de les dades
- L'exercici dels drets dels interessats
- La identificació de les mesures de seguretat
- La verificació de les relacions entre el responsable i els encarregats del tractament de les dades

La llista de verificació simplificada és vàlida en el cas de les pimes i micropimes que realitzen un **tractament bàsic de les dades i no implica un nivell de risc elevat en el seu tractament**, com podria ser la creació de perfils de clients, l'ús de dades sensibles, tecnologies d'anàlisi massiva de la informació, etc.

Si necessiteu informació més detallada al respecte, podeu posar-vos en contacte amb PIMEComerç a través del correu pcomerc@pimec.org o el telèfon: 934964500.

[4] Punt núm. 10, pàgina 34, de la *Guía del RGPD para responsables de tratamiento*.