Les 10 claus sobre el nou Reglament de Protecció de Dades (II)

16/05/2018
Suport Tercer Sector – Jurídic
Autor/a: Montse Agudo

La nova Llei de Protecció de dades començarà a aplicar-se el 25 de maig del 2018. Font: Pixabay

A partir d'ara, caldrà notificar a l'Agència de Protecció de Dades totes aquelles fallades de seguretat que puguin esdevenir. Font: Pixabay

La legislació estableix la figura del Delegat/da de Protecció de Dades. Font: Pixabay

Les 10 claus sobre el nou Reglament de Protecció de Dades (II)

16/05/2018
Suport Tercer Sector – Jurídic

Resum:
Tal i com hem començat a veure en el recurs anterior, el Reglament Europeu 2016/679 introdueix diverses novetats en matèria de protecció de dades, les quals seguim analitzant a continuació.

ÍNDEX

Obligació de dur un registre d'activitat del tractament de dades

El Reglament Europeu de Protecció de Dades aposta per la **responsabilitat proactiva** per part de les organitzacions a l'hora d'implementar les **mesures de seguretat** adients per a la correcta protecció de les dades de l'entitat.

En base a aquest principi, estableix la necessitat de dur **registres d'activitat del tractament de dades** amb la finalitat de poder demostrar l'efectiu compliment de la normativa. A més, la legislació recull que, pel que fa a aquests registres, cada entitat els haurà de **mantenir sota la seva responsabilitat**.

Les **principals informacions**, entre d'altres, que han de contenir aquests registres d'activitat són les següents:

- Identificació de les dades de contacte de la persona responsable del tractament i del delegat/da de protecció de dades.
- Finalitat del tractament.
- Descripció de les categories dels interessats/des i de les dades que disposa l'entitat.
- Categories de destinataris/es de les dades.
- Transferències internacionals de dades, en cas que n'hi hagi.

Relacionat amb aquest registre d'activitat, s'ha de tenir en compte que **desapareix** l'actual obligació d'**inscriure els fitxers a l'Agència de Protecció de Dades**, prevista a la Llei 15/1999.

Necessitat de realitzar avaluacions d'impacte

La nova legislació disposa que les entitats realitzin **avaluacions d'impacte** en matèria de protecció de dades quan es consideri que les operacions de tractament de les mateixes poden suposar un **alt risc per als drets i llibertats de les persones.**

Aquest risc, sobretot, es refereix a aquelles situacions en què les dades són especialment sensibles i quan s'utilitzen noves tecnologies per al seu tractament.

L'avaluació d'impacte consisteix en una anàlisi dels riscos que es poden derivar del propi tractament de les dades que fa l'entitat i que poden afectar la seva protecció. A més, a conseqüència d'aquesta anàlisi, s'han de prendre les **mesures necessàries per eliminar aquests riscos,** o almenys, reduir-los.

Les **principals qüestions** a tenir en compte a l'hora de realitzar l'avaluació d'impacte són les següents:

- Anàlisi en profunditat del projecte tenint en compte les dades a tractar, els fluxos d'informació i la tecnologia utilitzada per al seu tractament.

- Identificació dels riscos per a les dades personals i quins danys es produirien.
- Determinació de les mesures a adoptar per eliminar o disminuir el risc.
- Elaboració d'un informe final amb els riscos i les mesures a incorporar.
- Assegurar-se que el tractament compleix amb els requeriments legals establerts.
- Assignació dels recursos necessaris per implementar les mesures adequades.
- Revisió dels sistemes de tractament per comprovar l'efectivitat del resultat de l'avaluació d'impacte.

Notificació de les violacions de seguretat

Una altra novetat del Reglament és la notificació a l'Agència de Protecció de Dades de totes aquelles fallades de seguretat que puguin esdevenir.

Fins ara, la normativa només requeria portar un control **incidències a nivell intern**, a fi de poder dur un registre de les escletxes de seguretat que s'haguessin produït i les seves conseqüències.

Actualment, tot i que s'han de seguir establint els procediments interns necessaris per canalitzar les possibles violacions o escletxes de seguretat i establir les mesures adients per a la seva reparació, el Reglament Europeu estableix l'obligació per al responsable del tractament de **notificar totes les fallades de seguretat** a l'AEPD en un termini **màxim de 72 hores.**

S'ha de tenir en compte que, en el cas que la violació de seguretat fecti o impliqui un risc per a les **persones interessades**, també se'ls hi haurà de notificar.

Aquesta funció l'haurà d'assumir la figura del **Delegat/da de Protecció de Dades** i, en el seu defecte, la persona encarregada de coordinar el compliment de la normativa de protecció de dades dins de l'entitat.

Disposar d'un Delegat/da de Protecció de Dades

La legislació estableix la figura del Delegat/da de Protecció de Dades (DPO), el qual té com a funció **actuar com a garant del compliment de la normativa** de protecció de dades dins de l'entitat.

No totes les entitats han de disposar d'aquesta figura, sinó que està pensada, sobretot, per als organismes o empreses públiques, per a aquelles entitats que facin un tractament de dades a gran escala i requereixin una observació habitual i sistemàtica, i també per a les organitzacions que disposin de dades especialment sensibles o relatives a condemnes o infraccions penals.

El DPO pot ser una persona interna de l'organització o bé es podrà realitzar una contractació externa però, en tot cas, la persona que ha de desenvolupar aquesta tasca ha de tenir coneixements sòlids de dret i de protecció de dades, ja que es tracta d'una **persona experta** en la matèria que ha de vetllar per a la **coordinació i control de la normativa** de protecció de dades.

Les seves **funcions principals** són les següents:

- Informar i assessorar al responsable del tractament de dades de les seves obligacions per complir amb la normativa.
- Supervisar la implementació i aplicació de la legislació vigent.
- Dur un control de la documentació i comunicacions de les violacions de seguretat.
- Gestionar les sol·licituds d'exercici de drets per part dels interessats/des.
- Supervisar la realització de l'avaluació d'impacte.

- Ser el punt de contacte amb l'autoritat de control pel que fa al tractament de dades.
- Realitzar formació al personal de l'entitat.

Noves sancions

La nova legislació preveu diferents tipus de sancions que poden ser: advertències, sol·licituds d'atenció a l'exercici dels drets dels interessats/des, limitacions en el tractament i multes administratives.

Una de les qüestions més rellevants en la regulació europea és **la quantia de les sancions econòmiques.**

Fins ara, amb l'LOPD 15/1999, les sancions en matèria de protecció de dades podien anar des de 900€ fins a 600.000€.

A partir del 25 de maig, quan s'apliqui el Reglament Europeu, la quantia de les sancions s'eleva substancialment**, p**oden arribar aquestes a **20 milions d'euros** o al **4% del volum total de negoci** de l'organització que ha incomplert amb la normativa.

Informació relacionada:

Les 10 claus sobre el nou Reglament de Protecció de Dades (I)

Etiquetes: protecció de dades, Normativa entitat, LOPD, Legislació

URL d'origen: https://xarxanet.org/juridic/recursos/les-10-claus-sobre-el-nou-reglament-de-proteccio-de-dades