EAPC - Gestió de la informació: transparència i protecció de dades

Introducció a les avaluacions d'impacte sobre la protecció de dades

02-10-2019

Les avaluacions d'impacte sobre protecció de dades (AIPD), regulades en l'article 35 del Reglament general de protecció de dades (RGPD), són una eina preventiva vinculada a la protecció de dades des del disseny i per defecte. Una eina que ajuda a complir el principi de responsabilitat proactiva.

L'AIPD es configura com una obligació dels responsables del tractament (persona física o jurídica que determina les finalitats i els mitjans del tractament) per als casos en què el tractament de dades personals pot comportar un risc especial per als drets i les llibertats de les persones afectades.

En concret, cal fer una AIPD quan:

1. Un tractament, per la naturalesa, l'abast, el context o els fins que té, suposi un alt risc per als drets i les llibertats de les persones físiques, especialment quan s'utilitzin noves tecnologies.
2. S'efectua una avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques basada en un tractament automatitzat, com l'elaboració de perfils, sobre la base de la qual es prenen decisions que produeixen efectes jurídics per a les persones físiques o que les afecten significativament de manera similar.
3. Es produeix un tractament a gran escala de les categories especials de dades (salut, ideologia, religió, orientació sexual, dades biomètriques, etc.)o de les dades personals relatives a condemnes i infraccions penals.
4. Es fa una observació sistemàtica a gran escala d'una zona d'accés públic.

També ens poden ajudar les orientacions del Grup de treball de l'article 29, Directrius, sobre l'avaluació d'impacte relativa a la protecció de dades, com, per exemple: fer un ús innovador de les tecnologies, tractar dades de col·lectius vulnerables o quan es pren una decisió automatitzada amb efectes jurídics o similars.

A més, el RGPD estableix que les autoritats de protecció de dades han de publicar una llista dels tipus d'operacions de tractament que requereixen una AIPD. L'APDCAT ha publicat una llista d'aquestes operacions de tractament.

Per tant, el primer pas que ha de fer el responsable del tractament és determinar si té o no l'obligació de fer una AIPD.

Un cop feta aquesta valoració, podem arribar a la conclusió que no cal fer-la. En aquest cas, cal documentar-ho a l'efecte de complir la responsabilitat proactiva.

Recordem que la documentació relacionada amb les avaluacions d'impacte ha d'estar a disposició de les autoritats de control, és a dir, no només l'informe final, sinó també el conjunt de documents de treball que s'han utilitzat per fer l'avaluació i que sustenten les decisions preses.

Si arribem a la conclusió que sí que hem de fer l'**avaluació d'impacte**, hem de triar la metodologia a emprar. El RGPD és flexible en relació amb la manera de dur a terme l'AIPD. Per tant, podem adoptar un mètode desenvolupat per tercers (una autoritat de control, un organisme d'estandardització, un sector empresarial, una associació, etc.) o bé aplicar un mètode propi, sempre que el resultat de l'avaluació compleixi els requisits, els continguts mínims i les finalitats que disposa el RGPD.

En definitiva, la metodologia ha de comportar una valoració dels riscos que permeti als responsables dels tractaments decidir les mesures més adequades per afrontar-los.

L'AIPD és un procés orientat a:

- Descriure detalladament les operacions de tractament
- Avaluar-ne la necessitat i proporcionalitat
- Ajudar a gestionar els riscos per als drets i les llibertats
- Identificar les mesures més adequades per eliminar-los o reduir-los.

Podeu trobar informació sobre com fer una AIPD en la Guia sobre l'avaluació d'impacte relativa a la protecció de dades en el RGPD (2.0) de l'APDCAT.

Finalment, si l'AIPD ens porta a concloure que les operacions de tractament generen un alt risc que no es pot mitigar (gestionar o controlar) d'acord amb la tecnologia disponible, o bé pels costos o les dificultats d'implantació de les mesures necessàries per reduir els riscos, cal efectuar una consulta prèvia a l'Autoritat Catalana de Protecció de Dades (APDCAT).

En aquest cas, el responsable del tractament, en presentar la consulta prèvia a l'APDCAT, l'ha d'acompanyar amb la informació següent:

1. Les responsabilitats del responsable, els corresponsables i els encarregats implicats en el tractament.
2. Les finalitats i els mitjans del tractament previst.
3. Les mesures i garanties que s'han establert per protegir els drets i les llibertats de les persones interessades, de conformitat amb el RGPD.
4. Les dades de contacte del delegat de protecció de dades.
5. L'AIPD efectuada.
6. Qualsevol altra informació que sol·liciti l'autoritat de control.

Joana Marí Cardona

Delegada de protecció de dades i responsable de projectes estratègics de l'Autoritat Catalana de Protecció de Dades