Què és una bretxa de seguretat?

Segons els **RGPD** és tota **violació** que ocasioni la destrucció, pèrdua o alteració accidental o il·lícita de **dades personals** transmeses, conservades o tractades d'altra forma o la comunicació o accés no autoritzat a dites dades.

Així doncs tenim dos **requisits** *sine qua non*:

- Es produeixi la violació de seguretat d'acord amb la definició del RGPD
- Que la violació pugui comportar riscos pels interessats.

Què passa si es produeix?

Encara que les bretxes no produeixin cap risc pels drets i llibertats de les persones físiques, el **responsable del tractament haurà de documentar** qualsevol violació en la seguretat.

El responsable del tractament té com a **màxim 72 hores** des que tingui constància de la bretxa per notificar-ho a l'autoritat de control. El següent pas a tenir en compte serà la **comunicació a l'interessat**.

El **Reglament General de Protecció de Dades (RGPD)**, en el seu **article 33** contempla la obligatorietat de notificar una bretxa de seguretat (violació de les dades personals) quan la mateixa constitueixi un risc pels drets i llibertats de les persones físiques.

Quan no és necessària la comunicació a l'interessat?

Quan es doni alguna de les següents **condicions:**

- El **responsable** del tractament ha adoptat **mesures de protecció** tècniques i organitzatives apropiades i aquestes s'han aplicat a les dades afectades.
- El responsable del tractament ha pres **mesures posteriors** que garanteixen que ja no hi ha probabilitat que el risc es concreti.
- Suposi un **esforç desproporcionat**. En aquest cas s'optarà per una **comunicació pública** o una mesura semblant d'informació a l'interessat.

ARTICLE 34.3 DEL RGPD

La utilització del **xifrat** en la informació personal **elimina l'obligació de notificar als afectats que ha tingut lloc una bretxa en la seguretat**. Article 34. Comunicació d'una violació de la seguretat de les dades personals a l'interessat *1. Quan sigui probable que la violació de la seguretat de les dades personals comporti un alt risc per als drets i llibertats de les persones físiques, el responsable del tractament la comunicarà a l'interessat. 3. La comunicació a l'interessat al fet que es refereix l'apartat 1 no serà necessària si el responsable del tractament ha adoptat mesures de protecció tècniques i organitzatives apropiades i aquestes mesures s'han aplicat a les dades personals afectats per la violació de la seguretat de les dades personals, en particular aquelles que facin ininteꞏligibles les dades personals per a qualsevol persona que no estigui autoritzada a accedir a ells, com el xifrat.*

Exemples:

- Error de destinatari en l'enviament d'un correu electrònic que conté un fitxer amb dades de persones físiques.
- Pèrdua o sostracció de dispositius mòbils o portàtils amb fitxers amb dades (USB, disc externs, mòbils, portàtils)
- Accés a dades i possibilitat d'exportar-les i sostracció de les mateixes a personal que no hauria de tenir accés (personal de recepció que té accés a les dades de recursos humans).
- Accés a servidors propis, núvols, etc; sense les mesures de seguretat adients ni les garanties que aquests compleixin amb els requisits del RGPD.

Aplicacions Pont i Gri, S.L.
Carrer d[illegible] 17002 GIRONA
1807