Agència Andorrana de Protecció de Dades

OBLIGACIONS I PROTOCOLS DE LA LQPD

L'Agència Andorrana de Protecció de Dades (APDA) elabora una breu guia d'orientació amb les obligacions i els protocols a establir i complir amb la Llei Qualificada de Protecció de Dades (LQPD) per saber com procedir en les situacions més quotidianes. Es tracta d'un **document orientatiu** amb recomanacions genèriques que no exempt els responsables i encarregats de tractament de dades personals d'analitzar els seus propis riscos i obligacions.

Obligacions genèriques

Documents interns:

- **Política de protecció de dades**: és el document principal on es descriu com es tractaran les dades i ha d'incloure la descripció del cicle de vida de les dades, és a dir, la forma de recollida, la manera com es tracten, emmagatzemen i usen, possibles cessions, transferències si es realitzen, els nomenaments de les diferents figures (per exemple, el Delegat de Protecció de Dades), mitjans a través dels quals es tracten les dades i la forma de destruir-les un cop ja no són necessàries per a l'organització.

- **Anàlisi de riscos**: és la documentació que contempla la revisió de les amenaces que poden existir en el tractament de les dades perquè, després de valorar la probabilitat en què podrien ocórrer i l'impacte que podrien tenir sobre el tractament, es valori el risc a què estan exposats i, en funció del grau, es revisin i apliquin les mesures de seguretat més efectives per evitar, mitigar, transferir aquests riscos, i en cas de ser analitzat com un risc molt baix per a l'organització, arribar a acceptar-los.

- **Procediment per atendre els drets dels afectats**: els drets que emparen els ciutadans són els d'accés, rectificació, supressió, oposició, limitació al tractament, portabilitat, dret a l'oblit i el dret a no ser objecte de decisions automatitzades amb efectes jurídics sobre els interessats. Per donar compliment a l'exercici per part dels interessats s'ha de tenir en compte el protocol establert tant per la normativa com per la mateixa organització, alhora que aquesta l'ha d'haver traslladat als treballadors perquè la coneguin i no es cometin errors.

- **Gestió de bretxes de seguretat**: davant qualsevol incidència que es produeixi en el tractament de les dades personals i que afecti els drets i les llibertats de les persones s'haurà de seguir una sèrie de procediments per complir amb la normativa, a més de les mesures de seguretat que es duguin a terme dins de l'entitat, perquè no pugui tornar a ocórrer una fallida.

  Notificacions de violacions de seguretat de dades personals

- **Protocol davant els treballadors**: s'ha d'entregar a cada treballador un document on se l'informi del tractament de les seves dades, així com dels seus drets. D'altra banda, i en cas que aquest accedeixi a dades personals, s'ha de garantir el seu compromís de confidencialitat. També se li lliurarà un manual per a usuaris autoritzats de tractaments de dades, a títol de normativa interna per a un tractament d'acord amb la LQPD. És preceptiu fer formacions per acabar d'establir les bases d'un bon tractament de dades de l'organització, ja que cal recordar que sempre és la responsable final del tractament de les dades.

Documents externs:

- **Garanties del dret d'informació per als interessats**: s'ha de comprovar que a les clàusules d'informació als formularis de recollida de dades es compleix aquest dret, donant transparència i claredat en el tractament de les dades. Es garanteix el compliment normatiu de l'entitat alhora que els interessats estan ben informats sobre allò que es farà amb les seves dades, finalitats, possibles cessions, períodes de conservació, drets que assisteixen, on exercir-los, etc. També s'hi analitzen les bases jurídiques del tractament.

  Guia de bones pràctiques del deure d'informació

- **Textos preceptius:** si l'entitat té pàgina web, cal disposar dels textos web preceptius, fet que implica que, quan correspongui, es disposi de l'avís legal, la política de privadesa i del bàner i política de galetes. Cal tenir en compte que els formularis web han de comptar amb la informació de primera capa i els *checks* corresponents sense estar marcats prèviament. La primera capa contindrà la informació bàsica amb les dades del responsable, la finalitat, la legitimació, els destinataris, els drets i un enllaç a la política de privadesa, que és la segona capa, on es conté tota la informació detallada que es requereixen pels articles 16 i 17 de la LQPD.

  Guia de bones pràctiques del deure d'informació
  Ús de Cookies, política de privadesa i avís legal

Altres:

- **Garanties de tractament**: entre encarregat i responsable de tractament s'ha de signar un contracte d'encarregat de tractament per complir l'article 31 de la LQPD; en aquests contractes es marquen les directrius per les quals es regirà la cessió de

dades als encarregats de tractament i els vincula amb els responsables de tractament corresponent.

- **Mesures de tipus tècnic i organitzatives**: per assegurar un bon tractament de dades, i sempre amb l'anàlisi prèvia dels riscos detectats, és importantíssim aplicar totes aquelles mesures tant tècniques com organitzatives que l'entitat consideri per garantir la confidencialitat, disponibilitat, integritat i resiliència de les dades. Exemples de mesures: xifrar la informació i les comunicacions, tenir credencials d'accés i mecanismes d'atribució i control de permisos a usuaris, nomenament de DPD, formacions al personal, etc.

Obligacions específiques

- **Registre d'Activitats de Tractament (RAT)**: en cas que es consideri procedent, és un document que substitueix l'obligació anterior de registrar els fitxers davant l'APDA. Aquest RAT s'elabora per a cadascun dels tractaments de dades duts a terme i conté, com a mínim, les dades del responsable, la finalitat, la categoria dels interessats i dades tractades, si es fan transferències internacionals, els terminis de supressió i les mesures tècniques i organitzatives de seguretat. El registre ha d'estar permanentment actualitzat i a disposició de l'autoritat de control o qualsevol interessat. És un document intern.

- **Delegat de Protecció de Dades (DPD)**: en cas que la seva figura sigui necessària, el DPD és qui garantirà el compliment de la normativa de protecció de dades a les organitzacions. Segons la normativa, és obligatòria la seva designació depenent del tipus d'entitat, i molt recomanable per a la resta, tot i que la llei no ho contempli específicament. En cas de designar un DPD, cal comunicar la designació a l'APDA.
  Guia pràctica per saber si la meva entitat ha de designar un Delegat de Protecció de Dades (DPD)
  La figura del Delegat de Protecció de Dades (DPD)

- **Avaluació d'impacte**: la LQPD preveu que quan és probable que hi hagi un risc alt es faci abans del tractament una avaluació d'impacte (AI) amb l'objectiu d'avaluar els riscos potencials a què estan exposades les dades personals. L'article 32 de la LQPD indica en quins supòsits és obligatori. És un document intern o extern (depèn del resultat).
  Guia informativa de l'Avaluació d'Impacte en Protecció de Dades (AI)

- **Regulació de les transferències internacionals**: per realitzar una transferència internacional de dades d'acord amb la LQPD cal dur-la a terme mitjançant les directrius marcades per la mateixa normativa, realitzant-la a països reconeguts com

de nivell adequat per l'APDA, a través de garanties específiques o complint algunes de les excepcions marcades per aquestes normatives. Fora d'aquests casos, no es podran fer les transferències.