



Circular 1/2011 del director general de Funció Pública i Interior adreçada a les prefectures orgàniques de la Direcció General de Funció Pública i Interior sobre l'aplicació de la normativa de protecció de dades personals

L'article 21.3 de la Llei 3/2003, de règim jurídic de l'Administració de la Comunitat Autònoma de les Illes Balears, estableix que són circulars les pautes d'actuació interna dictades pels òrgans superiors o directius i encaminades a recordar l'aplicació de determinades disposicions legals o a unificar criteris d'interpretació d'aquestes, amb la finalitat d'aplicar-ne en l'àmbit de l'actuació administrativa una interpretació homogènia.

La Direcció General de Funció Pública i Interior està revisant la implantació de les mesures previstes en la Llei orgànica 17/1999, de 13 de desembre, de protecció de dades de caràcter personal, i en el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica esmentada.

Els estudis que s'han fet han palesat la necessitat d'incidir sobre l'aplicació de determinats aspectes prevists en les normes esmentades, per tal d'assolir un nivell més elevat de compliment d'aquestes normes, i han conclòs fer una sèrie de recomanacions.

Per això, s'ha considerat convenient fer una circular per a tot el personal adscrit a la Direcció General de Funció Pública i Interior (àrea de Funció Pública), en què es recorda la necessitat d'aplicar determinades disposicions previstes en la normativa sobre protecció de dades de caràcter personal. Així doncs, s'ha de tenir en compte el següent:

1. Fitxers no automatitzats

Pel que fa a **fitxers no automatitzats (documents en paper)** s'han de tenir en compte les prescripcions següents:

- Els armaris arxivadors i altres elements que contenguin dades en paper, han d'estar proveïts de pany i clau, i han de restar tancats quan no sigui necessari accedir-hi. Quan les dades són de nivell alt, els armaris han d'estar en una zona determinada de l'espai; han de configurar un espai separat, i el personal ha de tenir especial cura d'aquesta zona. En dades de nivell alt, els accessos han de quedar registrats en una taula d'accessos.



- Tots els armaris han de disposar de portes que es puguin tancar amb clau o un altre mètode. Les claus han de ser custodiades per les persones responsables del tractament i no han d'estar a l'abast de persones no autoritzades. Quan acabi la jornada laboral, aquestes s'han de dipositar al Servei de Seguretat, en el lloc habilitat a aquest efecte.
- La documentació que es faci servir durant una tramitació ha de ser custodiada per la persona que l'estigui tractant. Si aquesta persona s'ha absentat del seu lloc de feina, la documentació s'ha de guardar en un calaix o una carpeta amb clau, de tal manera que no sigui accessible per personal no autoritzat, i, si la persona està sola en un despatx, el despatx s'ha de tancar amb clau. Quan acabi la jornada laboral el treballador que faci servir documentació sensible pot optar per tornar-la al seu lloc o deixar-la en un calaix o armari tancat, i ha de dipositar posteriorment la clau al Servei de Seguretat.
- Les còpies o reproduccions de documents que continguin dades de caràcter personal de nivell alt han de ser autoritzades per escrit pel cap de servei respectiu. Una vegada deixin de ser útils, les còpies s'han de destruir per mitjà dels contenidors de destrucció de paper que té habilitats la Direcció General de Funció Pública i Interior.
- Quan s'hagi d'enviar documentació que contengui dades de caràcter personal a dependències alienes a la Direcció General de Funció Pública i Interior, s'han de prendre les mesures per evitar l'accés o la manipulació de les dades. En qualsevol cas, tot el trasllat de la documentació s'ha de fer adoptant les mesures de seguretat adreçades a impedir l'accés o la manipulació de la informació.

Sempre que el trasllat de documentació contingui dades de nivell alt i/o informació sensible ha de dur la signatura del cap de servei, seguint el model que s'adjunta com a annex 7 del Document de seguretat. La tramesa s'ha de fer en sobres precintats i s'ha d'indicar la classificació de la informació, el sol·licitant del trasllat, la data i un comptador numèric. A la destinació s'ha de signar un rebut que s'ha de retornar al servei d'origen com a garantia de recepció. Els caps de servei han de dur un registre de les entrades i sortides d'aquests tipus d'enviaments, i ha de quedar registrat el tipus de document, la data, l'hora, l'emissor i el destinatari, el nombre de documents inclosos en l'enviament, el tipus d'informació que contenen



(sense deixar constància en el registre de dades personals protegides), i la persona encarregada del trasllat (annex 5).

2. Fitxers automatitzats

Pel que fa als **fitxers automatitzats**, s'ha de tenir en compte el següent:

- L'extensió d'informació amb dades de caràcter personal en qualsevol tipus de suport extern i/o dispositiu mòbil resta prohibida. Només el responsable de seguretat per a aspectes organitzatius (cap de la Unitat de Sistemes d'Informació –cap de secció IV) de la Direcció General de Funció Pública i Interior pot autoritzar-ho expressament en casos puntuals.
- En els casos autoritzats els suports han d'anar etiquetats de tal manera que puguin ser fàcilment identificables pel personal autoritzat i difícilment pel no autoritzat. La Unitat de Sistemes d'Informació ha d'establir mecanismes per tal que només el personal autoritzat pugui accedir a la informació, com ara sol·licitar l'usuari i la contrasenya per a l'accés.

Els suports amb còpies temporals s'han de lliurar a la Unitat de Sistemes d'Informació per a la seva destrucció o reciclatge. Les còpies per a arxiu que excepcionalment i puntualment es puguin autoritzar han de ser inventariades i degudament custodiades.

- Amb caràcter general, l'enviament de dades personals per correu electrònic a personal no autoritzat fora de la direcció general competent en matèria de personal resta prohibida. Això no obstant, pot ser autoritzada puntualment. En aquest cas, l'usuari ha de contactar amb la Unitat de Sistemes d'Informació per tal de xifrar el correu electrònic.

En el casos en què es faci un enviament periòdic, ha de ser autoritzat pel director general de Funció Pública i Interior, amb l'informe favorable del/de la cap de la Unitat de Sistemes d'Informació i de l'assessor/a tècnic/a del Departament Jurídic. Aquests enviaments periòdics s'han de fer constar en el Document de seguretat.

- En els supòsits d'enviaments de suports (CD, DVD, USB, etc.) a dependències alienes a la Direcció General de Funció Pública i Interior (prohibits amb caràcter general), s'han d'aplicar mesures homogènies a les que s'han expressat per als fitxers en paper i les que s'han descrit per als



correus electrònics en el punt anterior. Als efectes del que estableix aquest punt, el cap de la Unitat de Sistemes d'Informació ha de dur, també, un registre homòleg al que s'estableix per als enviaments en paper (annex 5).

- Els usuaris que facin servir discs durs externs ho han de comunicar a la Unitat de Sistemes d'Informació per tal que en faci el xifratge i estableixi les mesures per incloure aquests dispositius en els protocols de còpies de seguretat.
- No es poden treure fora de les dependències vinculades a la Direcció General de Funció Pública i Interior dispositius portàtils que continguin dades de caràcter personal sense autorització del cap de la Unitat de Sistemes d'Informació, que ha de xifrar el disc dur per evitar accessos no autoritzats.
- Es prohibeix als usuaris emmagatzemar bases de dades ofimàtiques que continguin dades de caràcter personal de nivell alt fora d'H: de manera que per a l'accés sempre s'ha d'introduir l'usuari i la contrasenya. En qualsevol cas, l'usuari és responsable de les bases de dades que individualment creï.

La implantació d'aquestes mesures s'ha de fer com més aviat millor, per la qual cosa s'ha de fer arribar aquest escrit a tot el personal sota la vostra dependència jeràrquica.

Per a qualsevol dubte, us podeu adreçar al responsable de seguretat en aspectes organitzatius (el cap de la Unitat de Sistemes d'Informació —cap de secció IV) o al responsable de seguretat en aspectes legals (l'assessor tècnic de la Direcció General).

Aquestes mesures són addicionals a les contingudes en circulars anteriors.

Els responsables de seguretat dels fitxers automatitzats, com també els no automatitzats, tant per a aspectes organitzatius com per a aspectes legals, han d'establir els procediments i protocols necessaris per dur a terme les actuacions derivades d'aquesta circular.

Palma, 11 de maig de 2011

El director general de Funció Pública i Interior

Bernat Ramis Ripoll