Col·lecció Quaderns de legislació, 48

LEGISLACIÓ SOBRE PROTECCIÓ DE DADES

Generalitat de Catalunya
Agència Catalana de Protecció de Dades

REIAL DECRET 994/1999, D'11 DE JUNY, PEL QUAL S'APROVA EL REGLAMENT DE MESURES DE SEGURETAT DELS FITXERS AUTOMATITZATS QUE CONTINGUIN DADES DE CARÀCTER PERSONAL

(BOE núm. 151, de 25.6.1999, edició catalana en el suplement núm. 11, de 24.7.1999)

L'article 18.4 de la Constitució espanyola estableix que «la llei ha de limitar l'ús de la informàtica per garantir l'honor i la intimitat personal i familiar dels ciutadans i l'exercici ple dels seus drets».

La Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de dades de caràcter personal, preveu, en l'article 9, l'obligació del responsable del fitxer d'adoptar les mesures d'índole tècnica i organitzatives que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del mitjà físic o natural, i l'article 43.3.h) estableix que mantenir els fitxers, els locals, els programes o els equips que continguin dades de caràcter personal sense les degudes condicions de seguretat que per la via reglamentària es determinin constitueix una infracció greu en els termes que preveu la mateixa Llei.

Tanmateix, la falta de desplegament reglamentari ha impedit de disposar d'un marc de referència perquè els responsables promoguin les mesures de seguretat adequades i, en conseqüència, ha determinat la impossibilitat de fer complir un dels principis més importants de la Llei orgànica.

Aquest Reglament té com a objecte el desplegament del que disposen els articles 9 i 43.3.h) de la Llei orgànica 5/1992. El Reglament determina les mesures d'índole tècnica i organitzativa que garanteixin la confidencialitat i la integritat de la informació amb la finalitat de preservar l'honor, la intimitat personal i familiar i l'exercici ple dels drets personals en cas d'alteració, pèrdua, tractament o accés no autoritzat.

Les mesures de seguretat que s'estableixen es configuren com a les bàsiques de seguretat que han de complir tots els fitxers que continguin dades de caràcter personal, sens perjudici d'establir mesures especials per als fitxers que per la naturalesa especial de les dades que contenen o per les mateixes característiques de les dades exigeixen un grau de protecció més gran.

En virtut d'això, a proposta de la ministra de Justícia, d'acord amb el Consell d'Estat, i amb la deliberació prèvia del Consell de Ministres en la reunió del dia 11 de juny de 1999,

DISPOSO:

Article únic
Aprovació del Reglament

S'aprova el Reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal, el text del qual s'insereix tot seguit.

DISPOSICIÓ FINAL ÚNICA
Entrada en vigor

Aquest Reial decret entra en vigor l'endemà de la publicació en el *Butlletí Oficial de l'Estat*.

Madrid, 11 de juny de 1999

JUAN CARLOS R.

La ministra de Justícia,
MARGARITA MARISCAL DE GANTE Y MIRÓN

REGLAMENT
de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal

CAPÍTOL I
Disposicions generals

Article 1
Àmbit d'aplicació i finalitats

Aquest Reglament té com a objecte establir les mesures d'índole tècnica i organitzatives necessàries per garantir la seguretat que han de reunir els fitxers automatitzats, els centres de tractament, locals, equips, sistemes, programes i persones que intervinguin en el tractament automatitzat de les dades de caràcter personal subjectes al règim de la Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de les dades de caràcter personal.

Article 2
Definicions

A efectes d'aquest Reglament, s'entén per:

1. Sistemes d'informació: conjunt de fitxers automatitzats, programes, suports i equips utilitzats per emmagatzemar i tractar dades de caràcter personal.

2. Usuari: subjecte o procés autoritzat per accedir a dades o recursos.

3. Recurs: qualsevol part component d'un sistema d'informació.

4. Accessos autoritzats: autoritzacions concedides a un usuari per a la utilització dels diversos recursos.

5. Identificació: procediment de reconeixement de la identitat d'un usuari.

6. Autenticació: procediment de comprovació de la identitat d'un usuari.

7. Control d'accés: mecanisme que en funció de la identificació ja autenticada permet d'accedir a dades o recursos.

8. Contrasenya: informació confidencial, sovint constituïda per una cadena de caràcters, que es pot fer servir en l'autenticació d'un usuari.

9. Incidència: qualsevol anomalia que afecta o pot afectar la seguretat de les dades.

10. Suport: objecte físic susceptible de ser tractat en un sistema d'informació i sobre el qual es pot gravar o del qual es poden recuperar dades.

11. Responsable de seguretat: persona o persones a les quals el responsable del fitxer ha assignat formalment la funció de coordinar i controlar les mesures de seguretat aplicables.

12. Còpia de seguretat: còpia de les dades d'un fitxer automatitzat en un suport que en possibiliti la recuperació.

Article 3
Nivells de seguretat

1. Les mesures de seguretat exigibles es classifiquen en tres nivells: bàsic, mitjà i alt.

2. Aquests nivells s'estableixen d'acord amb la naturalesa de la informació tractada, en relació amb la major o menor necessitat de garantir la confidencialitat i la integritat de la informació.

Article 4
Aplicació dels nivells de seguretat

1. Tots els fitxers que continguin dades de caràcter personal han d'adoptar les mesures de seguretat qualificades de nivell bàsic.

2. Els fitxers que continguin dades relatives a la comissió d'infraccions administratives o penals, hisenda pública, serveis financers i els fitxers amb un funcionament que es regeixi per l'article 28 de la Llei orgànica 5/1992, han de reunir, a més de les mesures de nivell bàsic, les qualificades de nivell mitjà.

3. Els fitxers que continguin dades d'ideologia, religió, creences, origen racial, salut o vida sexual, com també els que continguin dades sol·licitades per a finalitats policials sense el consentiment de les persones afectades han de tenir, a més de les mesures de nivell bàsic i mitjà, les qualificades de nivell alt.

4. Si els fitxers contenen un conjunt de dades de caràcter personal suficients que permetin d'obtenir una avaluació de la personalitat de l'individu han de garantir les mesures de nivell mitjà que estableixen els articles 17, 18, 19 i 20.

5. Cada un dels nivells descrits anteriorment tenen la condició de mínims exigibles, sens perjudici de les disposicions legals o reglamentàries específiques vigents.

Article 5
Accés a dades per mitjà de xarxes de comunicacions

Les mesures de seguretat exigibles als accessos a dades de caràcter personal per mitjà de xarxes de comunicacions han de garantir un nivell de seguretat equivalent al corresponent als accessos de manera local.

Article 6
Règim de treball fora dels locals de la ubicació del fitxer

L'execució de tractament de dades de caràcter personal fora dels locals de la ubicació del fitxer ha de ser autoritzada expressament pel responsable del fitxer i, en tot cas, s'ha de garantir el nivell de seguretat corresponent al tipus de fitxer tractat.

Article 7
Fitxers temporals

1. Els fitxers temporals han de complir el nivell de seguretat que els correspongui d'acord amb els criteris que estableix aquest Reglament.

2. Qualsevol fitxer temporal ha de ser esborrat quan deixa de ser necessari per a les finalitats que n'hagin motivat la creació.

Capítol II
Mesures de seguretat de nivell bàsic

Article 8
Document de seguretat

1. El responsable del fitxer ha d'elaborar i implantar la normativa de seguretat mitjançant un document de compliment obligatori per al personal amb accés a les dades automatitzades de caràcter personal i als sistemes d'informació.

2. El document ha de contenir, com a mínim, els aspectes següents:

a) Àmbit d'aplicació del document amb especificació detallada dels recursos protegits.

b) Mesures, normes, procediments, regles i estàndards destinats a garantir el nivell de seguretat que exigeix aquest Reglament.

c) Funcions i obligacions del personal.

d) Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten.

e) Procediment de notificació, gestió i resposta davant les incidències.

f) Els procediments de realització de còpies de seguretat i de recuperació de les dades.

3. El document s'ha de mantenir sempre actualitzat i ha de ser revisat quan es produeixin canvis rellevants en el sistema d'informació o en la seva organització.

4. El contingut del document s'ha d'adequar, en tot moment, a les disposicions vigents en matèria de seguretat de les dades de caràcter personal.

Article 9
Funcions i obligacions del personal

1. Les funcions i les obligacions de cada una de les persones amb accés a les dades de caràcter personal i als sistemes d'informació estan clarament definides i documentades, d'acord amb el que preveu l'article 8.2.c).

2. El responsable del fitxer ha d'adoptar les mesures necessàries perquè el personal conegui les normes de seguretat que afecten l'exercici de les seves funcions, com també les conseqüències en què pugui incórrer en cas d'incompliment.

Article 10
Registre d'incidències

El procediment de notificació i gestió d'incidències ha de contenir necessàriament un registre en què es faci constar el tipus d'incidència, el moment

en què s'ha produït, la persona que fa la notificació, a qui es comunica i els efectes que en derivin.

Article 11
Identificació i autenticació

1. El responsable del fitxer s'encarrega que hi hagi una relació actualitzada d'usuaris que tinguin accés autoritzat al sistema d'informació i d'establir procediments d'identificació i autenticació per a aquest accés.

2. Si el mecanisme d'autenticació es basa en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzemament que en garanteixi la confidencialitat i la integritat.

3. Les contrasenyes s'han de canviar amb la periodicitat que determini el document de seguretat i mentre estiguin vigents s'han d'emmagatzemar de manera inintel·ligible.

Article 12
Control d'accés

1. Els usuaris tenen accés autoritzat únicament a les dades i els recursos que requereixin per a l'exercici de les seves funcions.

2. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a dades o recursos amb drets diferents dels autoritzats.

3. La relació d'usuaris a què es refereix l'article 11.1 d'aquest Reglament ha de contenir l'accés autoritzat per a cadascun d'ells.

4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anullar l'accés autoritzat sobre les dades i els recursos, d'acord amb els criteris que estableixi el responsable del fitxer.

Article 13
Gestió de suports

1. Els suports informàtics que continguin dades de caràcter personal han de permetre d'identificar el tipus d'informació que contenen, ser inventariats i emmagatzemar-se en un lloc amb accés restringit al personal autoritzat per fer-ho en el document de seguretat.

2. La sortida de suports informàtics que continguin dades de caràcter personal, fora dels locals en què estigui ubicat el fitxer, només pot ser autoritzada pel responsable del fitxer.

Article 14
Còpia de seguretat i recuperació

1. El responsable de fitxer s'encarrega de verificar la definició i l'apli-

cació correcta dels procediments de realització de còpies de seguretat i de recuperació de les dades.

2. Els procediments establerts per fer còpies de seguretat i per recuperar les dades han de garantir-ne la reconstrucció en l'estat en què estaven en el moment de produir-se la pèrdua o la destrucció.

3. S'han de fer còpies de seguretat com a mínim setmanalment, llevat que en aquest període no s'hagi produït cap actualització de les dades.

Capítol III
Mesures de seguretat de nivell mitjà

Article 15
Document de seguretat

El document de seguretat ha de contenir, a més del que disposa l'article 8 d'aquest Reglament, la identificació del responsable o els responsables de seguretat, els controls periòdics que s'hagin de fer per verificar el compliment del que disposa el mateix document i les mesures que calgui adoptar quan un suport hagi de ser rebutjat o reutilitzat.

Article 16
Responsable de seguretat

El responsable del fitxer ha de designar un o diversos responsables de seguretat encarregats de coordinar i controlar les mesures definides en el document de seguretat. En cap cas aquesta designació suposa una delegació de la responsabilitat que correspon al responsable del fitxer d'acord amb aquest Reglament.

Article 17
Auditoria

1. Els sistemes d'informació i les instal·lacions de tractament de dades s'han de sotmetre a una auditoria interna o externa que verifiqui el compliment d'aquest Reglament, dels procediments i les instruccions vigents en matèria de seguretat de dades, com a mínim, cada dos anys.

2. L'informe d'auditoria ha d'emetre dictamen sobre l'adequació de les mesures i els controls a aquest Reglament, identificar-ne les deficiències i proposar les mesures correctores o complementàries necessàries. També ha d'incloure les dades, els fets i les observacions en què es basin els dictàmens fets i les recomanacions proposades.

3. Els informes d'auditories han de ser analitzats pel responsable de seguretat competent, que ha d'elevar les conclusions al responsable del fitxer

perquè adopti les mesures correctores adequades, i queden a disposició de l'Agència de Protecció de Dades.

Article 18
Identificació i autenticació

1. El responsable del fitxer estableix un mecanisme que permeti la identificació de manera inequívoca i personalitzada de tots els usuaris que intentin accedir al sistema d'informació i la verificació que està autoritzat.

2. Es limita la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació.

Article 19
Control d'accés físic

Exclusivament el personal autoritzat en el document de seguretat pot tenir accés als locals on es trobin ubicats els sistemes d'informació amb dades de caràcter personal.

Article 20
Gestió de suports

1. S'ha d'establir un sistema de registre d'entrada de suports informàtics que permeti, directament o indirecta, de conèixer el tipus de suport, la data i l'hora, l'emissor, el nombre de suports, el tipus d'informació que contenen, la forma d'enviament i la persona responsable de la recepció que ha d'estar degudament autoritzada.

2. També s'ha de disposar d'un sistema de registre de sortida de suports informàtics que permeti, directament o indirecta, de conèixer el tipus de suport, la data i l'hora, el destinatari, el nombre de suports, el tipus d'informació que contenen, la forma d'enviament i la persona responsable del lliurament que ha d'estar degudament autoritzada.

3. Quan un suport hagi de ser rebutjat o reutilitzat, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació posterior de la informació emmagatzemada, abans de procedir a donar-lo de baixa en l'inventari.

4. Quan el suports hagin de sortir fora dels locals en què estiguin ubicats els fitxers com a conseqüència d'operacions de manteniment, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació indeguda de la informació emmagatzemada.

Article 21
Registre d'incidències

1. En el registre que regula l'article 10 s'han de consignar, a més, els procediments efectuats de recuperació de les dades, i indicar la persona que hagi executat el procés, les dades restaurades i, si s'escau, quines dades s'han hagut de gravar manualment en el procés de recuperació.

2. Cal l'autorització per escrit del responsable del fitxer per a l'execució dels procediments de recuperació de les dades.

Article 22
Proves amb dades reals

Les proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent al tipus de fitxer tractat.

Capítol IV
Mesures de seguretat de nivell alt

Article 23
Distribució de suports

La distribució dels suports que continguin dades de caràcter personal s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que aquesta informació no sigui intel·ligible ni manipulada durant el transport.

Article 24
Registre d'accessos

1. De cada accés s'ha de guardar, com a mínim, la identificació de l'usuari, la data i l'hora en què s'hagi fet, el fitxer a què s'ha accedit, el tipus d'accés i si ha estat autoritzat o denegat.

2. En cas que l'accés hagi estat autoritzat, cal guardar la informació que permeti d'identificar el registre a què s'ha accedit.

3. Els mecanismes que permeten el registre de les dades detallades en els paràgrafs anteriors estan sota el control directe del responsable de seguretat competent sense que s'hagi de permetre, en cap cas, de desactivar-los.

4. El període mínim de conservació de les dades registrades és de dos anys.

5. El responsable de seguretat competent s'encarrega de revisar periòdicament la informació de control registrada i ha d'elaborar un informe de les revisions efectuades i dels problemes detectats una vegada cada mes com a mínim.

Article 25
Còpies de seguretat i recuperació

S'ha de conservar una còpia de seguretat i dels procediments de recuperació de les dades en un lloc diferent d'aquell en què es trobin els equips informàtics que els tracten i complir, en tot cas, les mesures de seguretat que exigeix aquest Reglament.

Article 26
Telecomunicacions

La transmissió de dades de caràcter personal per mitjà de xarxes de telecomunicacions s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers.

Capítol V
Infraccions i sancions

Article 27
Infraccions i sancions

1. L'incompliment de les mesures de seguretat descrites en aquest Reglament és sancionat d'acord amb el que estableixen els articles 43 i 44 de la Llei orgànica 5/1992, quan es tracti de fitxers de titularitat privada.

El procediment que s'ha de seguir per a la imposició de la sanció a què es refereix el paràgraf anterior és el que estableix el Reial decret 1332/1994, de 20 de juny, pel qual es despleguen determinats aspectes de la Llei orgànica 5/1992, de 29 d'octubre, de regulació del tractament automatitzat de les dades de caràcter personal.

2. Quan es tracti de fitxers dels quals siguin responsables les administracions públiques cal atenir-se, pel que fa al procediment i a les sancions, al que disposa l'article 45 de la Llei orgànica 5/1992.

Article 28
Responsables

Els responsables dels fitxers, subjectes al règim sancionador de la Llei orgànica 5/1992, han d'adoptar les mesures d'índole tècnica i organitzatives

necessàries que garanteixin la seguretat de les dades de caràcter personal en els termes que estableix aquest Reglament.

Capítol VI
Competències del director de l'Agència de Protecció de Dades

Article 29
Competències del director de l'Agència de Protecció de Dades

De conformitat amb el que estableix l'article 36 de la Llei orgànica 5/1992, el director de l'Agència de Protecció de Dades pot:

1. Dictar, si s'escau i sens perjudici de les competències d'altres òrgans, les instruccions necessàries per adequar els tractaments automatitzats als principis de la Llei orgànica 5/1992.

2. Ordenar el cessament dels tractaments de dades de caràcter personal i la cancel·lació dels fitxers quan no es compleixin les mesures de seguretat previstes en aquest Reglament.

Disposició transitòria única
Terminis d'implantació de les mesures

En el cas de sistemes d'informació que estiguin en funcionament a l'entrada en vigor d'aquest Reglament, les mesures de seguretat de nivell bàsic que preveu aquest Reglament s'han d'implantar en el termini de sis mesos des de la seva entrada en vigor, les de nivell mitjà en el termini d'un any i les de nivell alt en el termini de dos anys.

Quan els sistemes d'informació que estiguin en funcionament no permetin tecnològicament la implantació d'alguna de les mesures de seguretat que preveu aquest Reglament, l'adequació d'aquests sistemes i la implantació de les mesures de seguretat s'han de fer en el termini màxim de tres anys a comptar des de l'entrada en vigor d'aquest Reglament.