



Serveis de  
Protecció  
De Dades

# EL COMPLIMENT DE LA NORMATIVA DE PROTECCIÓ DE DADES A LES EMPRESSES I ALS DESPATXOS PROFESSIONALS

LLEI ORGÀNICA 15/1999  
REIAL DECRET 1720/2007

Montserrat Navarro Sánchez  
Diplomada en Ciències Empresarials  
Licenciada en Administració i Direcció d'Empreses  
Advocada

Rambla Catalunya, 57 - 3ª planta - 08007 Barcelona - Telf. 93 159 15 15  
Fax 932721990 e-mail: m.navarro@protecciondatos.com



## NOCIONS PRÈVIES

2

**FITXER:** Conjunt organitzat de dades de caràcter personal, en qualsevol modalitat de creació, emmagatzematge, organització i accés.

**DADES DE CARÀCTER PERSONAL:** Qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus concernent a persones físiques identificades o identificables.

SERVEIS DE PROTECCIÓ DE DADES



## NOCIONS PRÈVIES (continuació)

3

**FITXER:** Finalitat legítima i no es pot utilitzar per finalitats incompatibles amb les declarades.

La AEPD entén incompatible com diferent

### DADES DE CARÀCTER PERSONAL:

- Seran exactes i actualitzades
- Han de ser necessàries i precises
- Quan ja no siguin necessàries o pertinents, es cancel·laran

SERVEIS DE PROTECCIÓ DE DADES



## NOCIONS PRÈVIES (continuació)

4

### Definicions:

- Responsable del fitxer o tractament
- Encarregat del tractament
- Prestador de servei
- Tercer
- Cessió de dades: Consentida  
No consentida  
Obligatòria

SERVEIS DE PROTECCIÓ DE DADES



## NOCIONS PRÈVIES (continuació)

5

### ÀMBIT SUBJECTIU:

Empreses, empresaris, professionals, associacions, fundacions, comunitats..

**Fora de l'àmbit de la Llei:** exclusivament els fitxers personals de caràcter domèstic, tractats per persones físiques en àmbit privat i familiar.

### ÀMBIT OBJECTIU:

Totes les bases de dades informatitzades o en suport paper que continguin dades de caràcter personal, tractades en àmbit públic i privat.

SERVEIS DE PROTECCIÓ DE DADES



## NOCIONS PRÈVIES (continuació)

6

### NIVELL DE SEGURETAT DELS FITXERS:

#### Regla general (automatitzats, mixtes i paper):

- **NIVELL BÀSIC:** Dades identificatives, de comptabilitat o facturació, de pagament
- **NIVELL MIG:** Dades d'infraaccions, característiques de la Personalitat, solvència patrimonial i crèdit...
- **NIVELL ALT:** Dades de salut, religió, creences, tendències sexuals, origen raçal... i fitxers de la normativa de blanqueig de capital

SERVEIS DE PROTECCIÓ DE DADES



## NOCIONS PRÈVIES (continuació)

7

Malgrat, **es consideraran de NIVELL BÀSIC els de NIVELL ALT** en que:

- Les dades s'utilitzin amb la única finalitat de fer transferències dineràries a les entitats de les que els afectats hi són membres.
- Es tracti de fitxers no automatitzats (paper) en els que de forma incidental o accessòria continguin dades de nivell alt sense guardar relació amb la seva finalitat.
- Si contenen dades de salut referides exclusivament al grau de discapacitat o la simple declaració de la condició de discapacitat o invalidesa de l'afectat, per complir amb deures públics.

SERVEIS DE PROTECCIÓ DE DADES



## OBLIGACIONS DEL RESPONSABLE

8

- **Declaració de fitxers**
- **Confeccionar el DOCUMENT DE SEGURETAT**
- **Implantació de les mesures de seguretat**
- **Firma de contractes / fitxes de legitimació / afegitons informatius...**

SERVEIS DE PROTECCIÓ DE DADES



## OBLIGACIONS DEL RESPONSABLE (continuació)

9

### No s'aplicarà als tractaments:

- De persones jurídiques.
- Fitxers que incorporin dades de persones físiques com a contactes de persones jurídiques.
- Empresaris i comerciants individuals referent a les dades de la seva activitat. (No inclosos els professionals)
- Dades de persones difuntes (excepció dret de cancel·lació).

SERVEIS DE PROTECCIÓ DE DADES



## CONSENTIMENT PER TRACTAR o CEDIR LES DADES:

10

- Norma general: Es necessitarà consentiment previ

### No caldrà el consentiment:

- Si ho autoritza una **norma amb rang de llei**
- Per satisfer un **interès legítim** del responsable o del cessionari
- Per complir una **obligació legal**
- Que siguin extreptes de fonts accessibles al **públic**

SERVEIS DE PROTECCIÓ DE DADES



## CONSENTIMENT PER TRACTAR o CEDIR LES DADES (continuació)

11

### No caldrà el consentiment **per tractar** les dades:

- Recollides per Administracions Públiques en les seves competències.
- Recollides en ocasió d'un contracte, precontracte, relació negocial, laboral o administrativa.
- Per necessitats mèdiques realitzat per professionals sanitaris.

### No caldrà el consentiment **per cedir**:

- La cessió que respongui a una relació jurídica.
- Cessions destinades al Defensor del Poble, M<sup>o</sup> Fiscal, Jutjats...
- Entre AAPP sempre que sigui amb finalitats històriques, que les reculli una Administració per lliurar a un altre o que tinguin competències idèntiques o sobre les mateixes matèries.
- Dades de salut entre serveis del Sistema Nacional de Salut.

SERVEIS DE PROTECCIÓ DE DADES



## CONSENTIMENT PER TRACTAR o CEDIR LES DADES (continuació)

12

- En totes les demás situacions el Responsable haurà d'obtenir el consentiment de l'afectat per a la cessió i el tractament de dades. Si es tracta de dades de nivell alt, haurà de ser exprés.
- La sol·licitud per al tractament haurà d'indicar el tractament concret, la finalitat i tots els extrems pertinents.
- L'afectat ha de ser informat a qui se li cediran les dades i per a quina finalitat, si no el consentiment és nul.
- Correspon al Responsable demostrar l'existència del consentiment.

SERVEIS DE PROTECCIÓ DE DADES



## CONSENTIMENT PER TRACTAR o CEDIR LES DADES (continuació)

13

### TRACTAMENT DE DADES DE MENORS:

- Els majors de 14 anys podran donar el consentiment per al tractament de les seves dades, tret dels casos que la Llei preveu l'assistència del pare o tutor.
- En el cas de menors de 14 anys es requerirà sempre el consentiment dels pares o tutors per el seu tractament.
- En cap cas es podran recaptar dades del menor que permetin obtenir informació del resta de membres de la família, o sobre característiques de la activitat professional dels progenitors, informació econòmica, dades sociològiques o qualsevol altres sense consentiment dels pares o tutors.

SERVEIS DE PROTECCIÓ DE DADES



## MANERA DE RECAPTAR EL CONSENTIMENT

14

- Procediment general Art. 14: Informar a l'afectat en els termes de l'art. 5 de la Llei Orgànica, i concedir-li 30 dies per manifestar la seva negativa al tractament, advertint-li que en el cas de no pronunciar-se s'entendrà que consenteix en el tractament de les seves dades.
- El mitjà per manifestar la negativa serà gratuït i fàcil.
- En el cas de responsables que prestin un servei que generi informació periòdica o reiterada, o facturació periòdica, aquesta comunicació es podrà incloure a la factura, sempre de manera clara i visible.

SERVEIS DE PROTECCIÓ DE DADES



## MANERA DE RECAPTAR EL CONSENTIMENT (continuació)

15

- En tot cas, el Responsable ha de poder conèixer si la comunicació ha estat tornada, llavors no podrà tractar-les.
- Si un interessat es nega al tractament, no es podrà tornar a preguntar fins que hagi passat un any.

### Recordar:

L'article 10 diu que **no caldrà el consentiment** per tractar les **dades de relacions negocials, laborals, precontractes o contractes ...**

SERVEIS DE PROTECCIÓ DE DADES



## MANERA DE RECAPTAR EL CONSENTIMENT (continuació)

16

### Important:

- Art. 15 Si el Responsable del tractament sol·licités el consentiment de l'afectat durant el procés de formació d'un contracte per a finalitats que no guardin relació directa amb el seu manteniment, haurà de permetre a l'afectat que manifesti expressament la seva negativa al tractament o comunicació de dades.
- S'entendrà que s'ha complert aquest deure si en el formulari hi ha una casella clarament visible que pugui marcar per indicar la seva negativa o un altre mitjà igualment visible i clar.

SERVEIS DE PROTECCIÓ DE DADES





## MANERA DE RECAPTAR EL CONSENTIMENT (continuació)

17

- L'afectat podrà revocar en qualsevol moment el seu consentiment. Se li haurà de permetre fer-ho gratuïtament i d'una manera senzilla. S'hauran de deixar de tractar les dades en un termini màxim de 10 dies.

- **SUPÒSITS ESPECIALS:**

En el cas que es produeixi una escissió, fusió, cessió global d'actius i passius o d'una branca d'activitat, etc. No es produirà una cessió de dades, sens perjudici del compliment del deure d'informació.

SERVEIS DE PROTECCIÓ DE DADES



## DRET D'INFORMACIÓ

18

**Art. 5 de la LOPD:** Els interessat a qui es demanin dades personals, hauran de ser prèviament informats de manera expressa e inequívoca de l'existència del fitxer, Responsable, de la finalitat, destinatari, possibilitat d'exercitar els drets...

**Important:**

- El deure d'informació s'ha de dur a terme de manera que el responsable pugui acreditar el seu compliment i s'ha de conservar tot el temps en que es realitzi el tractament de les dades.
- La conservació del suport on consti el compliment del deure d'informació es realitzarà per qualsevol mitjà tècnic o electrònic.

SERVEIS DE PROTECCIÓ DE DADES



## ENCARREGAT DEL TRACTAMENT

19

- **L'accés a les dades per part de l'encarregat** del tractament que resulti precís per tal de prestar el servei contractat pel responsable, no es considerarà comunicació de dades, sempre i quan es compleixi lo establert en la Llei Orgànica 15/1999.
- L'art. 12 LOPD, obliga a tenir firmat un contracte entre ambdues parts. El servei pot ser remunerat o no, temporal o indefinit, però ha d'estar subjecte a un contracte.
- El document de seguretat haurà d'incloure els fitxers tractats per tercers i la relació dels Responsables.

SERVEIS DE PROTECCIÓ DE DADES



## PRESTADOR DE SERVEI

20

- En el cas de que el servei es presti sense tenir accés a les dades, el contracte empararà expressament la prohibició d'accedir a les dades i la obligació de secret respecte de les dades que el personal hagi pogut conèixer amb motiu de la prestació del servei.
- El Document de Seguretat haurà d'indicar tots aquests extrems.

SERVEIS DE PROTECCIÓ DE DADES



## SUBCONTRACTACIÓ dels serveis

21

- L'Encarregat del tractament **no podrà subcontractar** amb un tercer el servei que li han encomanat sense l'autorització del Responsable.
- La subcontractació s'efectuarà en nom i per compte del Responsable.
- Serà possible subcontractar sense autorització sempre que:
  1. Estigui previst en el contracte quin serveis es poden subcontractar i, si es possible, s'haurà d'indicar la empresa que es subcontractarà.
  2. Si no fos possible, s'haurà de comunicar al Responsable les dades de la empresa subcontractada abans de procedir a la subcontractació.
  3. L'Encarregat del tractament i el subcontractista hauran de signar també el seu contracte de prestació de serveis.

SERVEIS DE PROTECCIÓ DE DADES



## DRETS D'ACCÉS, RECTIFICACIÓ, CANCEL·LACIÓ I OPOSICIÓ (ARCO)

22

- **Dret d'accés:** sol·licitud de quines dades té el Responsable
- **Dret de rectificació:** modificació de les dades.
- **Dret de cancel·lació:** pot ser total o parcial o simplement un bloqueig.
- **Dret d'oposició:** que no es porti a terme el tractament  
(fitxers que no requereixen consentiment o que no es poden cancel·lar)

SERVEIS DE PROTECCIÓ DE DADES



## DRETS D'ACCÉS, RECTIFICACIÓ, CANCEL·LACIÓ I OPOSICIÓ (ARCO) (continuació)

23

- Drets de **caràcter personalíssim**. Si no s'exerceixen en persona caldrà representació, en les administracions públiques haurà de ser per qualsevol vàlid en dret.
- Els drets s'han de **poder exercir de manera senzilla i gratuïta**.
- Hi ha uns **procediments i terminis** per contestar-los.

SERVEIS DE PROTECCIÓ DE DADES



## FITXERS TEMPORALS I CÒPIES DE TREBALL DE DOCUMENTS :

24

- Els **fitxers temporals** són els documents informàtics que es tenen durant un temps i després, les seves dades, passen a un programa definitiu o són destruïts.
- Les **còpies de treball de documents** són aquells documents en suport paper en els quals hi ha algunes dades que després s'inclouen en documents definitius i només tenen utilitat mentre s'elaboren.
- Ambdós, **es destruiran o s'esborraran** quan ja no facin falta.

SERVEIS DE PROTECCIÓ DE DADES



## TRANSFERÈNCIES INTERNACIONALS DE DADES

25

- Per realitzar transferències internacionals de dades caldrà l'autorització del Director de la AEPD, excepte en els casos previstos en l'art. 34 de la LOPD.
- No caldrà l'autorització quan la transferència és realitzi a Estats que ofereixin un nivell adequat de protecció (llista de països en el full web de la AEPD)
- En tot cas, s'haurà d'indicar al declarar el fitxer.

SERVEIS DE PROTECCIÓ DE DADES



## TRANSFERÈNCIES INTERNACIONALS DE DADES (continuació)

26

### En països que no ofereixin un nivell adequat:

- Haurà d'aportar contracte escrit en el que constin les garanties.
- Els grups multinacionals d'empreses hauran d'adoptar regles vinculants per les empreses del grup on constin les mesures de protecció.

SERVEIS DE PROTECCIÓ DE DADES



## INFRACCIONS I SANCIONS

27

### Tipus de infraccions:

- Lleus: No declarar, modificar, etc. un fitxer  
Incomplert del deure d'informació al recabar dades  
Contractar encargat de tractament sense formalitats art. 12 LOPD
- Greus: No recabar el consentiment quan sigui obligatori  
Tractar dades o fer-les servir conculcant els principis i garanties del art. 4  
Vulnerar el deure de guardar secret  
Impedir o obstaculitzar els drets d'accés...  
No tenir els fitxers, programes, locals sense les degudes mesures de seguretat  
No atendre a la Agencia Española de Protección de Datos.  
Cedir dades sense legitimació ni autorització

SERVEIS DE PROTECCIÓ DE DADES



## INFRACCIONS I SANCIONS (continuació)

28

### Tipus de infraccions:

- Molt greus: Recollir dades de manera enganyosa o fraudulenta  
Tractar o cedir dades especialment protegides sense consentiment  
No deixar de tractar dades quan hi ha un requeriment previ de l'Agència per no fer-ho.  
La transferència internacional de dades a països que no garanteixen el nivell de protecció sense l'autorització de la Agència.

SERVEIS DE PROTECCIÓ DE DADES



## INFRACCIONS I SANCIONS (continuació)

29

### Tipus de sancions:

- Lleus: de 900 a 40.000 €
- Greus: de 40.001 a 300.000 €
- Molt greus: de 300.001 a 600.000 €

La graduació de la sanció es farà atenent diversos criteris (entre d'altres):

El caràcter continuat de la infracció	Si tenia mesures de seguretat implantades
El volum de negoci	El volum de tractaments efectuats
El beneficis obtinguts	El grau d'intencionalitat...

SERVEIS DE PROTECCIÓ DE DADES



## REQUISITS TÈCNICS

30

### OBJECTIUS Art. 9 LOPD:

- Evitar tractament i accessos indeguts
- Evitar pèrdues de dades
- Evitar alteracions

La Llei no especifica les mesures, dona objectius

SERVEIS DE PROTECCIÓ DE DADES



## REQUISITS TÈCNICS (continuació)

31

### MESURES MÍNIMES

Per evitar accessos indeguts:

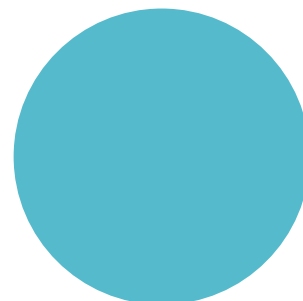
- Noms d'usuari i contrasenyes úniques
- Antivirus, Firewall, spyware...
- Servidors centrals amb carpetes per usuaris

Evitar pèrdues de dades

- Bon sistema de còpies de seguretat
- Sistema d'arxiu eficient (paper)

Evitar alteracions

- Definir l'accés per usuari i tipus d'accés



SERVEIS DE PROTECCIÓ DE DADES