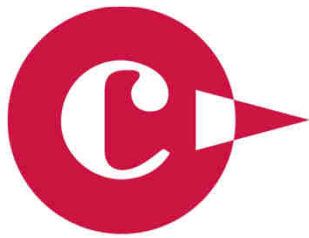


Reglament europeu de protecció de dades



Cambra de Comerç
de Manresa

REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL de 27 d'abril de 2016
relatiu a la protecció de las persones físiques en allò que respecta al tractament de de dades
personals i a la lliure circulació d'aquestes dades i pel que es deroga la Directiva 95/46/CE
(Reglament general de protecció de dades)

Preàmbul (on estem actualment)

- **Europa**
 - Directiva 95/46/CE
 - Decisió Marc 2008/977/JAI

- **Espanya**
 - Ley Orgánica 15/1999
 - Real Decreto 1720/2007 (Reglament Seguretat)

Legislació / requeriments en vigor (actualment)

- a) Identificació dels fitxers amb dades de caràcter personal.
- b) *Determinació del nivell de seguretat a aplicar en cada cas (nivell bàsic, mig o alt).*
- c) *Complimentar inscripció dels fitxers identificats al Registre General de la AGPD.*
- d) *Editar les llegendes i clàusules informatives, per a la recollida, tractament i/o cessió de dades de caràcter personal.*
- e) *Editar els contractes confidencialitat de l'accés a les dades per compte de tercers.*
- f) *Elaboració del Document de Seguretat, definint els recursos protegits i els procediments d'actuació.*
- g) *Implementació, formació, informació i auditories (si escaients)*

Reglament 2016/679 Protecció de dades

- **CAPÍTOL I - DISPOSICIONS GENERALS**
- **CAPÍTOL II – PRINCIPIIS**
- **CAPÍTOL III – DRETS DE L'INTERESSAT**
- **CAPÍTOL IV – RESPONSABLE DEL TRACTAMENT I ENCARREGAT DEL TRACTAMENT**
- **CAPÍTOL V – TRANSFERÈNCIA DE DADES PERSONALS A TERCERS PAISOS O A ORGANITZACIONS INTERNACIONALS**
- **CAPÍTOL VI – AUTORITATS DE CONTROL INDEPENDENTS**
- **CAPÍTOL VII – COOPERACIÓ I COHERÈNCIA**
- **CAPÍTOL VIII – RECURSOS, RESPONSABILITAT I SANCIONS**
- **CAPÍTOL IX – DISPOSICIONS RELATIVES A SITUACIONS ESPECÍFIQUES DE TRACTAMENT**
- **CAPÍTOL X – ACTES DELEGATS Y ACTES D'EXECUCIÓ**
- **CAPÍTOL XI – DISPOSICIONS FINALS**

Reglament (UE) 2016/679 - Protecció de dades

Àmbit d'aplicació del Reglament

Material

Segons el seu **art. 2** “El present Reglament s’aplica al **tractament total o parcialment automatitzat de dades personals**, així com al tractament **no automatitzat de dades personals continguts o destinats a ser inclosos en un fitxer.**”

Reglament (UE) 2016/679 - Protecció de dades

Àmbit d'aplicació del Reglament

Territorial

Art.3: “El present Reglament s’aplica al tractament de dades personals en el context de les activitats d’un establiment del responsable o de l’encarregat dins la Unió Europea, **independentment** de que el tractament es faci o no dins la Unió.”

S’aplica (punt 2) també a tractament de dades personals de residents a la Unió “**per part d’un responsable o encarregat no establert a la Unió, si relacionades amb:**

- a) oferta de bens o serveis, independent de pagament o no, o
- b) el control del seu comportament, en la mesura que el tractament es dugui a terme dins la Unió.”

Reglament (UE) 2016/679 - Protecció de dades

Entrada en vigor i aplicabilitat

Segons **art. 99**, el Reglament “entrarà en vigor **als 20 dies** de la seva publicació en el Diari Oficial de la Unió Europea.”

Serà aplicable “a partir del 25 de maig de 2018”.

Como tot Reglament de la Unió i segons estableix en el seu punt final, “serà obligatori en tots els seus elements i directament aplicable en cada Estat membre”.

Reglament (UE) 2016/679 - Protecció de dades

Principis rectors

1. Un continent, una norma
2. Finestreta única
3. Europa es regeix per la normativa europea
4. Consideració dels riscos específics
5. Privacitat des del disseny (*Data protection by design*).
6. El consentiment per al tractament de les dades



Reglament (UE) 2016/679 - Protecció de dades

Nou concepte dels drets dels ciutadans

- ❖ Transparència (**art.12**)
- ❖ Informació (**arts. 13 a 14**)
- ❖ Accés (**art.15**)
- ❖ Rectificació (**art. 16**)
- ❖ Supressió o dret a l'oblit (**art. 17**)
- ❖ Limitació del tractament (**art.18**)
- ❖ Portabilitat de dades (**art.20**)
- ❖ Oposició (**art.21**)

Drets **ARCO** (Accés, Rectificació, Cancel·lació, Oposició). LOPD 15/1999

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

1. Principis aplicables al tractament de dades ([art. 5](#))
2. Condicions reconeixement validació consentiment prestat ([art. 7](#))
3. **Dret a l'oblit** (dret de supressió ([art. 17](#)))
4. **Principi de portabilitat de les dades** ([art. 20](#))
5. Responsabilitat del responsable del tractament de les dades ([art. 24](#))
- 6- Protecció de dades des del disseny i per defecte ([art.25](#))
7. Encarregat de tractament ([art.28](#))
8. **Registre de les activitats de tractament** ([art. 30](#))
9. **Notificació de les violacions de seguretat** ([art. 33](#) y [34](#))
10. **Avaluació d'impacte relativa a la protecció de dades** ([art. 35](#))
11. Consulta prèvia, cas d'identificar-se riscos en el tractament ([art. 36](#))
12. **Delegat de protecció de dades** ([arts. 37](#) a [39](#))
13. Regulació de las transferències internacionals de dades ([arts. 45](#) y [47](#))
14. Organismes de control i Comitè Europeu de Protecció dades ([arts.51](#) a [76](#))
15. Recursos, responsabilitat i sancions ([arts.77](#) a [84](#))
16. Situacions específiques de tractament ([arts. 85](#) a [91](#))

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

1. Principis aplicables al tractament de dades ([art. 5](#))

- ✓ Tractades de forma **Lícita, lleial i transparent**;
- ✓ Recollides amb **finalitat determinada**, explícita i legítima «limitació de la finalitat»);
- ✓ **Limitades a allò necessari** en relació amb les finalitats del tractament («minimització de dades»);
- ✓ **Exactes** i, si s'escau, actualitzades («exactitud»);
- ✓ Mantingudes de forma que se'n permeti la identificació dels interessats durant **no més temps del necessari** per a les finalitats del tractament de les dades personals («limitació del termini de conservació»);
- ✓ Tractades de tal manera que se'n **garanteixi una seguretat adequada** de les dades personals («integritat i confidencialitat»);

El responsable del tractament serà responsable del compliment dels punts anteriors i haurà de ser capaç de demostrar-ho («responsabilitat proactiva»).

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

2. Condicions per a entendre vàlidament prestat el consentiment ([art. 7](#))

- ✓ En cas de tractament basat en el consentiment de l'interessat, el responsable de tractament n'haurà de ser capaç de demostrar-ho, si sol·licitat.
- ✓ Consentiment en una declaració escrita en el que es tracten altres assumptes, el consentiment cal orientar-lo al assumpte que s'escaigui i amb distinció respecte als altres assumptes.
- ✓ Dret de retirada de consentiment. Facilitats per donar-lo com per a retirar-lo.
- ✓ Caldrà tenir en compte si la sol·licitud de consentiment es vincula a un contracte o una prestació de servei, quan aquestes dades no en son necessàries per a dur a terme el contracte o servei → no validesa

Consentiment menors ([art.8](#))

- ✓ Menys de 16 anys (*mai menys de 13 anys*) → consentiment pares/tutors
- ✓ Verificació raonable per part del responsable tractament → recurs tecnològic

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

3. Dret de supressió («el dret a l'oblit» [art. 17](#))

Dret a que el responsable de tractament supprimeixi dades personals de l'interessat sense dilació indeguda si:

- ✓ Les dades ja no son necessàries per al finalitat per les que es van recollir
- ✓ Retirada del consentiment per part interessat
- ✓ Oposició al tractament per part de l'interessat
- ✓ El tractament s'ha fet il·lícitament
- ✓ Imperatiu obligatori legal derivat del Dret de la Unió o de l'Estat membre
- ✓ Les dades obtingudes corresponen a oferta de serveis a menors

Si han estat difoses públicament les dades per part del responsable de tractament, i se'n escau la seva supressió, aquest responsable adoptarà mesures tècniques més raonables per informar a altres responsables que estiguin tractant aquestes mateixes dades de la sol·licitud de supressió per part de l'interessat.

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

4. Principi de portabilitat de los dades ([art. 20](#))

- ✓ Dret de l'interessat a rebre dades personals que l'incumbeixin i que hagi facilitat a un responsable de tractament, en un format estructurat, d'ús comú i lectura mecànica per a poder-los transmetre a altre responsable de tractament.
- ✓ Si s'exerceix el dret a la portabilitat, l'interessat tindrà dret a que les dades siguin transmeses directament de responsable a responsable, si això és tècnicament possible. Tot i sens perjudici del dret de supressió.

No s'aplicarà el dret de portabilitat si el tractament es realitza per interès públic o en l'exercici de poders públics conferits al responsable de tractament.

El dret de portabilitat no podrà afectar negativament als drets i llibertats d'altres persones.

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

5. Responsabilitat del responsable del tractament de les dades per adopció i actualització de les mesures adequades ([art. 24](#))

- ✓ Segons naturalesa, àmbit, context, finalitats i riscos → garantia seguretat
- ✓ Definició de polítiques de protecció de dades (responsable)
- ✓ Adhesió a codis de conducta o mecanismes de certificació (art.40/art.42)



dreamstime.com

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

6. Protecció de dades des del disseny i per defecte (art. 25)

- ✓ Mesures tècniques i organitzatives adients (p.e. seudonimització, minimització de dades, integració de garanties en el tractament,...)
- ✓ Limitar l'accés «per defecte» al màxim possible de persones
- ✓ Podrà emprar-se un mecanisme de certificació aprovat per acreditar el compliment dels punts anteriors



dreamstime.com

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

7. Encarregat de tractament(art. 28)

- ✓ Responsabilitat del responsable tractament d'escollir Encarregat amb garanties
- ✓ No subcontractació de l'encarregat sense autorització escrita del responsable
- ✓ Contracte entre parts (sempre per escrit):
 - Tractament segons instruccions documentades del responsable
 - Garantia confidencialitat sobre el personal intern autoritzat del encarregat
 - Mesures de seguretat (p.e. Seudonimització, xifrat, recuperació, verificació regular de les mesures de seguretat,...)
 - Assistència i recolzament al responsable
 - Retorn i/o eliminació, segons instruccions del responsable
 - Disponibilitat informació sobre compliment d'accés per al responsable (incloent p.e. Auditories)
 - Responsabilitat encarregat 1 vs encarregat 2 front el responsable (mesures i compliment del 2 vs 1)
- ✓ Adhesió a codi conducta / certificació → element de demostració

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

8. Registre de les activitats de tractament ([art. 30](#)) (sempre per escrit)

- ✓ Registre d'activitats de tractament gestionat pel responsable:
 - Nom i contacte del responsable,.. I del delegat de protecció de dades
 - Finalitats del tractament
 - Descripció de categories d'interessats i categories de les dades
 - Categories de destinataris de les dades (nacionals/internacionals...)
 - Identificació tercer país o organisme internacional receptor i garanties escaients (art.49), si s'escau
 - Terminis per la supressió de les categories de dades, si possible
 - Descripció general de mesures de seguretat tèc/organitz, si possible
- ✓ Registre d'activitats de tractament gestionades per l'encarregat:
 - Nom i dades contacte del responsable / encarregats tractament 2
 - Categories de tractament vs responsables
 - Identificació tercer país o organisme internacional receptor i garanties escaients (art.49), si s'escau

No aplicable a empreses de menys de 250 treballadors, excepte tractaments de risc, no siguin ocasional o incloguin categories especials (art.9) o incorporin dades de condemnes o infraccions penals (art.10)

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

8. Notificació de les violacions de seguretat (art. 33)

- ✓ Notificació a l'autoritat de control (màxim en termini 72 hores), a menys que constitueixi un risc pels drets i llibertats persones físiques.
- ✓ Comunicació de l'encarregat al responsable, cas de violacions seguretat detectades
- ✓ Les notificacions cal que incorporin, com a mínim:
 - Naturalesa de la violació de seguretat (nº afectats i nº registres)
 - Comunicar nom i dades de contacte del delegat de protecció de dades
 - Descripció de les possibles conseqüències de la violació de seguretat
 - Descripció de les mesures de contingència i correctores posteriors
- ✓ Lliurament progressiu a l'autoritat de control, si no disponible al 100% inicialment
- ✓ Registre intern de la incidència de violació, a disposició de l'autoritat de control per verificar-ne el compliment

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

9. Notificació de les violacions de seguretat (art. 34)

- ✓ Notificació al interessat, sempre que comporti un alt risc pels drets i llibertats de les persones físiques.
- ✓ En llenguatge clar i senzill i les mateixes dades de: *delegat protecció dades, conseqüències possibles i mesures adoptades pel responsable*
- ✓ Excepcions a la comunicació:
 - Adopció de mesures de seguretat adients per part del responsable (p.e. Xifrat de dades)
 - El responsable adopta posteriorment mesures de seguretat per garantir la no probabilitat de concreció en alt risc pels drets i llibertats.
 - Suposi un esforç desproporcionat. → Comunicació pública o mesura similar com alternativa
- ✓ L'autoritat de control podrà exigir al responsable que es compleixin mesures de comunicació als interessats.

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

10. Avaluació d'impacte relativa a la protecció de dades (art. 35)

- ✓ Avaluació de l'impacte segons probabilitat de risc i del tipus de tractament, abast, context, finalitats,.. Per part del responsable de tractament
- ✓ Participació del delegat de protecció de dades designat
- ✓ Avaluació d'impacte, en cas de:
 - Avaluació sistemàtica i exhaustiva de tractaments automatitzats, com p.e. elaboració de perfils, i que en base a aquests es prenguin decisions amb efectes per a les persones físiques
 - Tractaments a gran escala de categories de dades especials o dades de condemnes o infraccions penals
 - Observació sistemàtica a gran escala d'una zona d'accés públic
- ✓ L'autoritat de control establirà i publicarà una llista dels tipus d'operacions de tractament als que s'escaigui fer una avaluació d'impacte prèvia al tractament.
- ✓ L'avaluació contindrà, com a mínim:
 - Descripció operacions tractament i finalitats, necessitat i proporcionalitat
 - Avaluació dels riscos vs drets i llibertats dels interessats. Mesures previstes front riscos. Revisió de l'avaluació d'impacte, en cas de canvis substancials en el tractament

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

11. Consulta prèvia (art. 36)

- ✓ Consulta prèvia a l'autoritat de control, cas que el resultat de l'avaluació d'impacte comporti un alt risc si no es prenen mesures de minimització del risc.
- ✓ Resposta de l'autoritat de control en màxim 8 setmanes (pròrroga 6 setmanes)
- ✓ Consulta per part del responsable a l'autoritat de control. Contingut:
 - Responsabilitats del responsable i encarregats de tractament
 - Finalitats i mitjans pel tractament previst
 - Mesures i garanties establertes per protegir dret i llibertats
 - Dades de contacte del delegat de protecció de dades
 - L'avaluació d'impacte relativa a la protecció de dades
 - Qualsevol altre dada sol·licitada per l'autoritat de control
- ✓ L'autoritat de control disposa de potestats com òrgan consultiu per legislació dels estats membres i per vetllar especialment per obligar als responsables del tractament a fer-los-hi les consultes prèvies, especialment en tractament de dades de l'àmbit social i de la salut pública.

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

12. Delegat de protecció de dades (art. 37)

- ✓ Responsable i encarregat de tractament han de designar un delegat de protecció de dades si:
 - a) El tractament correspon a una autoritat o bé organisme públic (excepció tribunals)
 - b) El tractament requereixi operacions d'observació habitual i sistemàtica d'interessats a gran escala
 - c) L'activitat principal del responsable o encarregat siguin operacions de tractament a gran escala de categories de dades especials o de condemnes i infraccions penals
- ✓ Podrà haver-hi un únic delegat de protecció de dades dins un grup empresarial
- ✓ Igualment en el cas d'autoritat o organismes públics
- ✓ Els delegats podran representar igualment a associacions o altres organismes que representin a categories de responsables o encarregats.
- ✓ Designació basada en les capacitats (coneixement del dret, qualitats professionals)
- ✓ Podrà ser subcontractat o en plantilla
- ✓ Publicació dades de contacte del delegat i comunicació a l'autoritat de control

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

12. Delegat de protecció de dades (art. 38)

Posició del delegat de protecció de dades

- ✓ Participació en qüestions relatives a la protecció de dades de l'organització
- ✓ Responsable i encarregat recolzen a Delegat de protecció de dades aportant recursos per a realitzar la seva tasca (accés a dades, accés a les operacions de tractament, i manteniment del coneixement especialitzat en matèria de protecció de dades i la seva seguretat)
- ✓ Garantia de independència del delegat de protecció vs instruccions del responsable o encarregat. Línia directe amb el nivell jeràrquic més alt del responsable o encarregat.
- ✓ Interessats tindran línia directa amb el delegat de protecció de dades
- ✓ Obligació de secret i confidencialitat per part del delegat de protecció de dades
- ✓ Podrà fer altres funcions, sempre que no entrin en conflicte d'interessos

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

12. Delegat de protecció de dades (art. 39)

Funcions mínimes del delegat de protecció de dades

- ✓ Informar i assessorar al responsable o al encarregat de tractament i als empleats que s'ocupen de tractament de dades personals, de les obligacions legals aplicables
- ✓ Supervisar el compliment de requisits de seguretat (incloent responsabilitats, formació, auditories,..)
- ✓ Oferir l'assessorament en relació a les avaluacions d'impacte i supervisar-ne la seva aplicabilitat quan s'escaigui
- ✓ Cooperar amb l'autoritat de control, actuant com a punt de contacte entre ambdues parts i en el cas de consultes prèvies o d'altres consultes

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

13. Regulació de les transferències internacionals de dades (art. 44 a 46)

✓ Principi general de transferència:

- Sols es podran fer transferències internacionals de dades a un tercer país o organització internacional, si el responsable i l'encarregat de tractament de dades compleixen els requisits del capítol V del Reglament, incloent-t'hi les posteriors transferència des dels receptors externs a altres tercers països o organismes internacionals.

- ❖ Transferències basades en una decisió d'adequació (per part de la Comissió Europea (reconeixement garanties) → no necessitarà autorització específica
- ❖ Transferències mitjançant garanties adequades (responsable o encarregat ofereixen garanties adequades i interessats compten amb drets exigibles i accions legals efectives). P.e. Clàusules tipus, mecanismes de certificació,...., compromisos vinculants de seguretat en el país receptor,...)
- ❖ Normes corporatives vinculants (cal que siguin aprovades per l'autoritat de control)
- ❖ Transferències o comunicacions no autoritzades pel dret de la Unió
- ❖ Excepcions per a situacions específiques → consentiment amb informació riscos

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

14. Autoritats de control i Comitè Europeu de Protecció de dades (art. 51 a 76)

- ✓ Autoritat de control (conceptualment a nivell de la UE):
 - Independència, membres, normativa de funcionament i gestió, competència, funcions i poders.
- ✓ Competència de l'autoritat de control principal (a nivell dels estats membres):
 - Funcions, poders, informes d'activitat anuals, cooperació entre autoritats de control, assistència mútua, operacions conjuntes, mecanismes de coherència, dictàmens del Comitè, resolució de conflictes pel Comitè, procediments d'urgència,
- ✓ Comitè Europeu de Protecció de dades
 - Independència, funcions, informes, procediments, presidència, funcions de presidència, secretaria, confidencialitat.

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

15. Recursos, responsabilitats i sancions (arts. 77 a 84)

- ✓ Dret a presentar una reclamació front l'autoritat de control
- ✓ Dret a la tutela judicial efectiva contra una autoritat de control
- ✓ Dret a la tutela efectiva contra un responsable o encarregat de tractament
- ✓ Representació dels interessats
- ✓ Suspensió dels procediments
- ✓ Dret a indemnització i responsabilitat



CONDICIONS GENERALS PER IMPOSICIÓ DE MULTES ADMINISTRATIVES (art.83)

Fins a 10.000.000 EUR ó del 2% com a màxim del volum anual global darrer exercici

Fins a 20.000.000 EUR ó del 4% com a màxim del volum anual global darrer exercici

- ✓ Sancions (autoritats de control han de notificar a la Comissió UE les disposicions legislatives sobre sancions, abans del 25 de maig 2018)

Reglament (UE) 2016/679 - Protecció de dades

Principals novetats que incorpora el Reglament

16. Situacions específiques de tractament (arts. 85 a 91)

- ✓ Tractament i llibertat d'expressió i d'informació
- ✓ Tractament i accés del públic a documents oficials
- ✓ Tractament del número nacional d'identificació
- ✓ Tractament en l'àmbit laboral
- ✓ Garanties i excepcions aplicables al tractament amb finalitats arxiu interès públic, finalitats d'investigació o històrics
- ✓ Obligacions de secret
- ✓ Normes vigents sobre protecció de dades de les esglésies i associacions religioses

Reglament (UE) 2016/679 - Protecció de dades

Altres elements que incorpora el Reglament

- ❖ Codis de conducta (**arts. 40 a 41**)
- ❖ Certificació (**arts. 42 a 43**)
- ❖ Derogació de la Directiva 95/46/CE a partir del 25 de maig del 2018



Reglament (UE) 2016/679 - Protecció de dades

Conclusions

- ☐ Hi ha menys de 15 dies per adequar-se al RGPD.
- ☐ Cal aprofitar-ho per ajustar les mesures tècniques i organitzatives per una implementació efectiva (en temps i cost) per tal fer els deures de forma adient.
- ☐ Les empreses petites i mitjanes tenen previsiblement menys feina d'adaptació, però cal identificar en cada cas les implicacions particulars que l'afectin (delegat de protecció si o no, encarregats de tractament externs,...) . Mentrestant, manteniment del Document de seguretat i alerta i observació a les novetats.
- ☐ Les empreses que encara no estiguin en fase de adequació al RGPD, no han de deixar-ho ja per més temps. No es preveu cap pròrroga en el temps per adaptació.

Gràcies por la vostra atenció

Document elaborat per:

Ernest Rovira Torras

Director d'ASSERTIS

Consultor associat CCM



Cambra de Comerç
de Manresa