UNITAT 4

ALTRES MESURES DE RESPONSABILITAT ACTIVA: DELEGAT DE PROTECCIÓ DE DADES. CODIS TIPUS. CERTIFICACIONS. TRANSFERÈNCIES INTERNACIONALS DE DADES

CONTINGUTS

1. **La figura del delegat de protecció de dades en les administracions públiques**
2. **Codis de conducta**
3. **Esquemes de certificació**
4. **Transferències internacionals de dades**

OBJECTIUS

1. **Reconèixer la figura del delegat de protecció de dades en les administracions públiques**
2. **Identificar tractaments sotmesos a transferències internacionals**
3. **Aplicar la normativa de protecció de dades en els expedients de contractació administrativa**

4.1. La figura del delegat de protecció de dades en les administracions públiques

4.1.1. Antecedents

Tant la LOPD com el seu reglament de desplegament no regulaven el delegat de protecció de dades, per la qual cosa la introducció d'aquest delegat en l'RGPD suposa una novetat en el nostre ordenament jurídic, per bé que la Directiva 95/46 sí que recollia la figura del delegat de protecció de dades. D'aquesta manera, alguns països de la Unió Europea, en transposar la Directiva esmentada, van tenir en compte en les seves respectives normes el delegat de Protecció de Dades, com són els casos d'Alemanya i Eslovàquia.

Abans de l'aprovació de l'RGPD, trobam un desenvolupament major del delegat de protecció de dades en el Reglament 45/2001, del Parlament Europeu i de Consell, de 18 de desembre de 2000.

4.1.2. Obligatorietat, perfil i aptituds

L'RGPD regula de manera detallada el delegat de protecció de dades en els articles 37-39 i estableix una sèrie de supòsits de designació obligatòria per part dels responsables i els encarregats:

- El tractament el dugui a terme una AUTORITAT O ORGANISME PÚBLIC, llevat dels tribunals que actuïn en exercici de la seva funció judicial.
- Que les ACTIVITATS PRINCIPALS del responsable o de l'encarregat consisteixin en operacions de tractament que, pel que fa a la seva naturalesa, abast i/o fins, requereixin una observació HABITUAL I SISTEMÀTICA D'INTERESSATS A GRAN ESCALA, o
- Que les activitats principals del responsable o de l'encarregat consisteixin en el tractament a gran escala de CATEGORIES ESPECIALS DE DADES PERSONALS de conformitat amb l'article 9 i de dades relatives a condemnes i infraccions penals a què es refereix l'article 10.

En aquest sentit, el Grup de l'Article 29, a través del document «Directrius sobre els delegats de la protecció de dades» ha precisat el següent sobre el supòsit d'obligatorietat en les administracions públiques:

> L'RGPD no defineix què es considera com a «autoritat o organisme públic», per la qual cosa aquesta noció ha de determinar-se de conformitat amb la legislació de cada país, que, tot i que s'entén que hi estan incloses les autoritats nacionals, regionals i locals, també hi poden ser inclosos altres organismes regits pel dret públic. Respecte a les organitzacions privades que hi participen a través de les diferents modalitats de contractació de la gestió dels serveis públics, per bé que no seria obligatòria la designació del delegat de protecció de dades, es recomana com a bona pràctica nomenar-lo i que la seva activitat cobreixi no només els tractaments relacionats amb aquesta gestió pública, sinó també els que no hi estiguin.

L'apartat 4 de l'article 37 de l'RGPD obre la possibilitat que els països de la Unió,

a través de la seva normativa específica, puguin establir altres supòsits en què calgui nomenar un delegat de protecció de dades. En aquest sentit, l'article 34 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), l'ha previst per als supòsits següents:

> *a)* Els col·legis professionals i els seus consells generals.
> *b)* Els centres docents que ofereixin ensenyaments en qualsevol dels nivells establerts en la legislació reguladora del dret a l'educació, així com les universitats públiques i privades.
> *c)* Les entitats que exploten xarxes i presten serveis de comunicacions electròniques de conformitat amb el que disposa la seva legislació específica, quan tracten habitualment i sistemàtica dades personals a gran escala.
> *d)* Els prestadors de serveis de la societat de la informació quan elaboren a gran escala perfils dels usuaris del servei.
> *e)* Les entitats incloses en l'article 1 de la Llei 10/2014, de 26 de juny, d'ordenació, supervisió i solvència d'entitats de crèdit.
> *f)* Els establiments financers de crèdit.
> *g)* Les entitats asseguradores i reasseguradores.
> *h)* Les empreses de serveis d'inversió, regulades per la legislació del mercat de valors.
> *i)* Els distribuïdors i comercialitzadors d'energia elèctrica i els distribuïdors i comercialitzadors de gas natural.
> *j)* Les entitats responsables de fitxers comuns per avaluar la solvència patrimonial i crèdit o dels fitxers comuns per gestionar i prevenir el frau, incloent-hi els responsables dels fitxers regulats per la legislació de prevenció del blanqueig de capitals i del finançament del terrorisme.
> *k)* Les entitats que desenvolupen activitats de publicitat i prospecció comercial, incloent-hi les d'investigació comercial i de mercats, quan duen a terme tractaments basats en les preferències dels afectats o fan activitats que impliquen elaborar-ne perfils.
> *l)* Els centres sanitaris legalment obligats al manteniment de les històries clíniques dels pacients.
> Se n'exceptuen els professionals de la salut que, tot i que estan legalment obligats al manteniment de les històries clíniques dels pacients, exerceixen la seva activitat a títol individual.
> *m)* Les entitats que tenen com un dels seus objectes l'emissió d'informes comercials que puguin referir-se a persones físiques.
> *n)* Els operadors que desenvolupin l'activitat de joc a través de canals electrònics, informàtics, telemàtics i interactius, de conformitat amb la normativa de regulació del joc.
> *o)* Les empreses de seguretat privada.
> *p)* Les federacions esportives quan tracten dades de menors d'edat.

El paràgraf segon de la norma fins i tot ha previst la possibilitat de la designació voluntària.

D'altra banda, l'RGPD, en l'article 37.5 i el considerant 97, determina que el delegat de protecció de dades ha de ser una persona amb coneixements especialitzats de dret i pràctica en matèria de protecció de dades. Aquests coneixements són exigibles en relació amb els tractaments que es facin, així com les mesures que hagin d'adoptar-se per garantir un tractament adequat de les dades personals objecte d'aquests tractaments.

El Grup de l'Article 29 ha introduït les precisions següents al respecte:

- **Coneixement**

Encara que l'RGPD no el defineix, el nivell de coneixement ha d'estar en consonància amb el tipus, la quantitat i la complexitat de dades que tracta una organització.

- **Qualificació professional**

Tampoc no està precisada en l'RGPD. No obstant això, el delegat de protecció de dades ha de tenir coneixement de les lleis nacionals i europees i del Reglament esmentat. En l'àmbit privat, ha de conèixer el sector empresarial. En l'àmbit públic, ha de tenir un coneixement sòlid de les normes i els procediments administratius.

- **Capacitat**

Per desenvolupar les seves tasques cal tenir en compte tant les seves qualitats personals i els seus coneixements com el lloc que ocupa en l'organització. Entre les de caràcter personal, s'inclourien la integritat i un nivell elevat d'ètica professional.

Si ens referim a l'àmbit de les administracions públiques, la provisió dels llocs de treball de delegats de protecció de dades requereix la selecció d'empleats públics que reuneixen aquests requisits i, en especial, els coneixements especialitzats en dret i la pràctica en protecció de dades que el Reglament exigeix.

La qualificació d'un delegat de protecció de dades pot acreditar-se mitjançant mecanismes voluntaris de certificació que tindran particularment en compte l'obtenció d'una titulació universitària que acrediti coneixements especialitzats en el dret i la pràctica en matèria de protecció de dades. L'Agència Espanyola de Protecció de Dades ha impulsat un esquema de certificació de delegats de protecció (ESQUEMA AEPD-DPD). ÉS UN ESQUEMA VOLUNTARI; EN CAP CAS NO POT EXIGIR-SE COM A REQUISIT NI EN UNA OPOSICIÓ, NI EN UNA LICITACIÓ DE SERVEIS.

4.1.3. Posició en l'organització administrativa

Com hem vist en l'apartat anterior, l'RGPD determina l'obligatorietat de designar un delegat de protecció de dades en l'àmbit de les administracions públiques. Amb caràcter general, es pot assenyalar, per exemple, que d'acord amb l'RGPD és possible designar un únic delegat per a un ministeri, una conselleria o un ajuntament. Alhora, no sembla aconsellable que aquest únic delegat actuï en grans unitats o òrgans amb entitat i tasques clarament diferenciades, per molt que orgànicament puguin dependre d'un departament ministerial, una conselleria o un ajuntament.

D'altra banda, i donades les funcions del delegat de protecció de dades, dins

l'estructura de l'organització se l'ha d'adscriure a òrgans o unitats amb competències i funcions de caràcter horitzontal. Així mateix, el nivell del lloc de treball ha de ser l'adequat per poder relacionar-se amb la direcció de l'òrgan o organisme en què desenvolupi les seves funcions.

L'RGPD preveu que el delegat pot desenvolupar la seva activitat a temps complet o parcial i que pot formar part de la plantilla del responsable o de l'encarregat del tractament o desenvolupar les seves funcions en el marc d'un contracte de serveis.

En òrgans, organismes o ens grans en què existeixi un únic delegat l'habitual serà que desenvolupi les seves funcions a temps complet. Fins i tot, és possible que el Delegat formalment nomenat estigui fet costat per una unitat específicament dedicada a la protecció de dades.

En entitats més petites és possible que el delegat compagini les seves funcions amb altres. Si és el cas, cal tenir en compte la necessitat d'evitar conflictes d'interessos entre les diverses ocupacions.

A més, cal tenir en compte que el delegat actua com a assessor i supervisor intern, per la qual cosa aquest lloc no pot ser ocupat per persones que alhora facin tasques que impliquin decisions sobre l'existència de tractaments de dades o sobre la manera en què seran tractades les dades (p. ex.: responsables de TIC, o responsables de seguretat de la informació).

L'RGPD també ofereix la possibilitat que es contractin externament les funcions de delegat. Aquesta opció pot ser utilitzada en determinats casos, com podria ser el de municipis petits que es beneficien d'un servei que ofereix una diputació provincial o una comunitat autònoma o fins i tot que on aquest servei no existeixi puguin optar pels serveis d'entitats privades especialitzades.

D'altra banda, és necessari analitzar quin és la posició del delegat de protecció de dades en el marc de l'organització on presta serveis.

En aquest sentit, l'RGPD es refereix, en l'article 38, a l'encaix del delegat en el marc de l'entitat en què hagi estat designat:

- Participar de manera adequada i en temps oportú en totes les qüestions relatives a la protecció de dades personals;
- Rebre el suport del responsable o encarregat, que hauran de facilitar-li els recursos necessaris per complir les seves funcions;
- No rebre cap instrucció pel que fa a l'acompliment d'aquestes funcions i no ser destituït ni sancionat pel responsable o l'encarregat per causes relacionades amb aquest acompliment de funcions;
- Retre comptes directament al nivell jeràrquic més alt del responsable o encarregat. Aquesta característica ha d'interpretar-se en el sentit que el delegat ha de poder relacionar-se amb nivells jeràrquics que tenguin la

capacitat d'adoptar o promoure decisions basades en les recomanacions, les propostes o les avaluacions que faci.

- Convidar el delegat a participar amb regularitat en les reunions dels quadres directius alts i mitjans.
- Tenir presència en la presa de decisions amb implicacions per a la protecció de dades, de manera que tota la informació rellevant se li transmeti de manera oportuna perquè pugui prestar un assessorament adequat.
- La seva opinió ha de gaudir sempre de la consideració oportuna i cal documentant les raons per les quals no se segueix el seu consell.
- Se l'ha de consultar sense demora si es produeix una violació de dades o un altre incident.

A més, segons el document del Grup de l'Article 29 «Directrius sobre els delegats de protecció de dades», cal tenir en consideració certs elements:

- RECURSOS: l'article 38.2 del Reglament determina que l'organització ha de donar suport al delegat proporcionant-li els recursos necessaris i l'accés a dades personals i operacions de tractament per fer les seves funcions i mantenir el seu coneixement expert. L'alta direcció ha de donar suport actiu a les funcions del delegat, com el temps suficient perquè les dugui a terme; dotació de recursos econòmics, infraestructura i personal; accés a altres serveis (recursos humans, departament jurídic, tecnologies de la informació) que puguin donar suport al delegat; i equip de persones a càrrec del delegat en funció de l'estructura de l'organització.

- INDEPENDÈNCIA: l'article 38.3 del Reglament estableix unes garanties bàsiques perquè els delegats actuïn amb independència dins l'organització en què presten els seus serveis, incloent-hi que «no rebin cap instrucció relativa a l'exercici de les seves tasques». A més, és important assenyalar que els que estan obligats al compliment de l'RGPD són el responsable o l'encarregat del tractament, de manera que, si adopten decisions contràries a la norma i a l'assessorament prestat pel delegat, el delegat ha de tenir la possibilitat d'expressar amb claredat la seva opinió disconforme respecte a aquestes decisions.

- DESTITUCIÓ: l'article 38.3 esmentat també estableix que els delegats de protecció de dades «no han de ser destituïts ni penalitzats pel responsable o l'encarregat per dur a terme les seves funcions», fet que suposa un reforç de la seva autonomia i independència. Sí que podrien ser acomiadats o sancionats de conformitat amb la legislació contractual, laboral o penal aplicable de cada país, per causes diferents de l'acompliment de les seves funcions (per exemple, per robatori o assetjament sexual). Teniu en compte en l'àmbit de les administracions públiques el règim d'infraccions i sancions aplicables al seu personal.

- CONFLICTE D'INTERÈS: encara que el delegat de protecció de dades pot fer altres funcions en l'organització, aquestes funcions no poden suposar un conflicte d'interessos. Per això, i tenint en compte l'estructura, les activitats i la mida de cada organització, es recomana que els responsables o els encarregats del tractament: determinin els llocs que serien incompatibles amb les funcions del delegat; elaborin normes internes per evitar aquests conflictes; declarar que el delegat no té conflicte d'interessos en relació amb les seves funcions; incloure salvaguardes en normes internes i garantir que l'anunci de la vacant per a delegat o el contracte de serveis sigui prou precís i detallat per evitar els conflictes esmentats.

L'estatut del delegat de protecció de dades per l'article 36 de la LOPDGDD, de conformitat amb el qual:

- Quan es tracta d'una persona física integrada en l'organització del responsable o l'encarregat del tractament, el delegat de protecció de dades no pot ser remogut ni sancionat pel responsable o l'encarregat per desenvolupar les seves funcions llevat que incorri en dol o negligència greu en el seu exercici. Cal garantir la independència del delegat de protecció de dades dins l'organització i s'ha d'evitar qualsevol conflicte d'interessos.

- En l'exercici de les seves funcions, el delegat de protecció de dades tindrà accés a les dades personals i els processos de tractament, a la qual cosa el responsable o l'encarregat del tractament no podrà oposar-se al·legant l'existència de qualsevol deure confidencialitat o secret, incloent-hi el que es preveu en l'article 5 d'aquesta Llei orgànica.

4.1.4. Funcions

Les funcions del delegat de protecció de dades, que seran d'informació, assessorament i supervisió, es troben especificades en l'article 39 de l'RGPD, i es poden concretar en les àrees següents:

- **Respecte al compliment**

  - Compliment de principis relatius al tractament, com els de limitació de finalitat, minimització o exactitud de les dades.
  - Identificació de les bases jurídiques dels tractaments.
  - Valoració de compatibilitat de finalitats diferents de les que van originar la recollida inicial de les dades.
  - Existència de normativa sectorial que pugui determinar condicions de tractaments específics diferents de les que estableix la normativa general de protecció de dades.
  - Contractació d'encarregats de tractament, incloent-hi el contingut dels contractes o actes jurídics que regulin la relació responsable-encarregat.
  - Identificació dels instruments de transferència internacional de dades adequats a les necessitats i les característiques de l'organització i de les raons que justifiquen la transferència.
  - Disseny i implantació de polítiques de protecció de dades.

- Auditoria de protecció de dades.
- Establiment i gestió dels registres d'activitats de tractament.

En aquesta matèria, l'article 36 de la LOPDGDD té en compte tasques molt específiques:

- El delegat pot inspeccionar els procediments relacionats amb l'objecte d'aquesta Llei orgànica i emetre recomanacions en l'àmbit de les seves competències.
- Quan el delegat de protecció de dades aprecïi l'existència d'una vulneració rellevant en matèria de protecció de dades l'ha de documentar i comunicar immediatament als òrgans d'administració i direcció del responsable o l'encarregat del tractament.

- **Respecte a la relació amb els interessats:**

  - Disseny i implantació de mesures d'informació als afectats pels tractaments de dades.
  - Establiment de mecanismes de recepció i gestió de les sol·licituds d'exercici de drets per part dels interessats.
  - Valoració de les sol·licituds d'exercici de drets per part dels interessats.

En aquest àmbit, la LOPDGDD dissenya un procés de mediació o intermediació directa amb les persones interessades en cas d'infracció en l'article 37:

> Article 37. Intervenció del delegat de protecció de dades en cas de reclamació davant les autoritats de protecció de dades.
> 1. Quan el responsable o l'encarregat del tractament hagin designat un delegat de protecció de dades, l'afectat pot, abans de presentar una reclamació contra aquells davant l'Agència Espanyola de Protecció de Dades o, si escau, davant les autoritats autonòmiques de protecció de dades, adreçar-se al delegat de protecció de dades de l'entitat contra la qual es reclama.
> En aquest cas, el delegat de protecció de dades ha de comunicar a l'afectat la decisió que s'ha adoptat en el termini màxim de dos mesos a comptar des que en va rebre la reclamació.
> 2. Quan l'afectat presenti una reclamació davant l'Agència Espanyola de Protecció de Dades o, si escau, davant les autoritats autonòmiques de protecció de dades, aquelles podran trametre la reclamació al delegat de protecció de dades a fi que hi respongui en el termini d'un mes.
> Si transcorregut aquest termini el delegat de protecció de dades no ha comunicat a l'autoritat de protecció de dades competent la resposta donada a la reclamació, aquesta autoritat continuarà el procediment de conformitat amb el que estableixen el títol VIII d'aquesta Llei orgànica i les seves normes de desplegament.

- **Respecte a la seguretat:**

  - Anàlisi de risc dels tractaments realitzats.
  - Implantació de les mesures de seguretat adequades als riscs i la naturalesa dels tractaments.
  - Establiment de procediments de gestió de violacions de seguretat de les dades, incloent-hi l'avaluació del risc per als drets i les llibertats dels afectats i els procediments de notificació a les autoritats de supervisió i als afectats.

- **Respecte a la prevenció:**

  - Determinació de la necessitat d'avaluar l'impacte sobre la protecció de dades.
  - Realització d'avaluacions d'impacte sobre la protecció de dades.

- Implantació de les mesures de protecció de dades des del disseny i la protecció de dades per defecte adequades als riscs i la naturalesa dels tractaments.

➢ **Respecte a la cooperació:**

- Relacions amb les autoritats de supervisió.

En aquest sentit, l'article 36.1 estableix que el delegat de protecció de dades «actuarà com a interlocutor del responsable o l'encarregat del tractament davant l'Agència Espanyola de Protecció de Dades i les autoritats autonòmiques de protecció de dades».

➢ **Respecte a la formació:**

- Implantació de programes de formació i sensibilització del personal en matèria de protecció de dades

A més dels preceptes del Reglament, als quals hem fet referència sobre la regulació del delegat de protecció de dades, la norma es refereix al delegat en altres preceptes:

➢ EN EL DRET D'INFORMACIÓ (ARTICLES 13 I 14): té en compte la possibilitat que quan es recullin les dades de caràcter personal dels interessats se'ls facilitin les dades de contacte del delegat de protecció de dades, en cas que hagi estat designat.

➢ EN EL REGISTRE D'ACTIVITATS (ARTICLE 30): l'han d'implementar tant el responsable com l'encarregat, i també hi haurien de figurar les dades de contacte esmentades.

➢ NOTIFICACIONS DE VIOLACIONS DE SEGURETAT (ARTICLE 33): s'han d'incloure les dades de contacte del delegat amb la finalitat de poder obtenir més informació sobre la violació ocorreguda.

➢ AVALUACIONS D'IMPACTE DE PROTECCIÓ DE DADES (ARTICLE 35): obligació que el responsable reculli l'assessorament del delegat de protecció de dades a l'hora de fer aquestes avaluacions. Si una vegada feta l'avaluació d'impacte, el tractament de dades pot suposar un risc alt si no es mitiguen els danys i, per tant, el responsable ha de consultar sobre això l'autoritat de control, ha d'incloure en la consulta les dades de contacte del delegat de protecció de dades.

➢ NORMES CORPORATIVES VINCULANTS (ARTICLE 47): en el seu contingut mínim s'han de reflectir les funcions del delegat de protecció de dades.

➢ RELACIÓ AMB LES AUTORITATS DE CONTROL DE PROTECCIÓ DE DADES (ARTICLE 57.3): les relacions entre el delegat de protecció de dades i la seva respectiva autoritat de control seran gratuïtes, sense cost econòmic per a l'entitat que ha designat el delegat.

4.2. Codis de conducta

En donar major rellevància als codis de conducta, l'objectiu principal de l'RGPD és que serveixin com a eines perquè els responsables i els encarregats puguin demostrar el seu compliment.

Els CODIS DE CONDUCTA són una forma d'autoregulació orientada a adoptar regles o estàndards específics que permetin harmonitzar els tractaments de dades fets per aquelles institucions, entitats o empreses que estan adherides al codi o que el promoguin, a facilitar l'exercici dels drets dels afectats i a afavorir el compliment de la normativa de protecció de dades, així com un instrument que pot ser utilitzat pels responsables i els encarregats per demostrar el compliment d'aquesta normativa.

En adoptar els codis de conducta, els responsables i els encarregats dels tractaments poden adequar les previsions normatives de protecció de dades a les característiques del sector en què operin i ampliar-les, i oferir transparència pel que fa a la seva actuació. Són instruments que aporten un valor afegit a la regulació.

L'RGPD assenyala els aspectes que, entre altres, haurien d'incloure aquests codis. Per fer-ho, segons el que assenyala l'article 40 de l'RGPD, les associacions i altres organismes representatius de categories de responsables o encarregats del tractament poden elaborar codis de conducta o modificar o ampliar els codis amb l'objecte d'especificar l'aplicació de l'RGPD, en relació amb:

- el tractament lleial i transparent;
- els interessos legítims perseguits pels responsables del tractament en contexts específics;
- la recollida de dades personals;
- la pseudonimització de dades personals;
- la informació proporcionada al públic i als interessats;
- l'exercici dels drets dels interessats;
- la informació proporcionada als infants i la protecció d'aquests infants, així com la manera d'obtenir el consentiment dels titulars de la pàtria potestat o tutela sobre l'infant;
- les mesures i els procediments per garantir la seguretat del tractament, així com la protecció de dades des del disseny i per defecte;
- la notificació de violacions de la seguretat de les dades personals a les autoritats de control i la comunicació d'aquestes violacions als interessats;
- la transferència de dades personals a tercers països i organitzacions internacionals, o
- els procediments extrajudicials i altres procediments de resolució de conflictes que permetin resoldre les controvèrsies entre els responsables del tractament i els interessats relatius al tractament, sens perjudici dels drets dels interessats.

L'RGPD preveu la possibilitat d'aprovar codis de conducta si tenen relació amb activitats de tractament en diversos estats membres o inclouen compromisos vinculants i exigibles per fer transferències internacionals de dades a través del mecanisme de coherència.

EN DEFINITIVA, ELS CODIS DE CONDUCTA són un instrument que no només permet

adequar l'aplicació de l'RGPD a les característiques de cada sector, sinó que serveixen per demostrar-ne el compliment i, en el cas d'Espanya, tant l'AEPD com els potencials promotors dels codis disposen d'un bon punt de partida en l'experiència desenvolupada durant la vigència de la LOPD i, en especial, del seu reglament de desplegament.

Respecte als procediments d'elaboració i adopció, caldria distingir dos supòsits:

- **Codis d'àmbit exclusivament nacional:**

Els codis de conducta han de ser aprovats per l'AEPD o, si escau, per l'autoritat autonòmica de protecció de dades competent, havent-ne avaluat prèviament la conformitat amb l'RGPD.

L'AEPD i les autoritats autonòmiques de protecció de dades han de dur un registre dels codis de conducta que han aprovat i dels que s'han aprovat de conformitat amb el mecanisme de coherència que s'estableix en l'article 63 de l'RGPD.

- **Codis que afecten tractaments en diversos estats de la UE:**

L'AEPD i, si escau, les autoritats autonòmiques de protecció de dades han d'enviar el codi de conducta, abans que sigui aprovat, al Consell Europeu de Protecció de Dades perquè emeti el dictamen sobre la seva adequació a l'RGPD i/o sobre les garanties que ofereix per a les transferències internacionals de dades, i s'ha de suspendre el procediment fins que s'emeti l'informe.

Si el dictamen és favorable, el Comitè Europeu de Protecció de Dades l'ha de presentar a la Comissió, que decidirà si el codi té validesa dins la UE i, en aquest cas, li'n donarà publicitat.

El Comitè Europeu de Protecció de Dades ha de dur un registre dels codis de conducta que afecten tractaments en diversos estats de la UE i els ha de posar a disposició pública.

A Espanya, l'Agència Espanyola de Protecció de Dades o, si escau, l'autoritat autonòmica de protecció de dades competent són les que aproven els codis de conducta. L'Agència Espanyola de Protecció de Dades o, si escau, les autoritats autonòmiques de protecció de dades han de sotmetre els projectes de codi al mecanisme de coherència esmentat en l'article 63 de Reglament (UE) 2016/679, en els supòsits en què sigui procedent segons l'article 40.7.

D'altra banda, l'Agència Espanyola de Protecció de Dades i les autoritats autonòmiques de protecció de dades han de dur registres dels codis de conducta accessibles a través de mitjans electrònics que hagin aprovat, els quals han d'estar interconnectats i coordinats amb el registre gestionat pel Comitè Europeu de Protecció de Dades. El contingut del registre i les especialitats del

procediment d'aprovació dels codis de conducta s'han d'establir per reial decret.

4.3. Esquemes de certificació

4.3.1. Línies generals de la certificació

Com ja hem vist, l'RGPD posa a disposició dels responsables i els encarregats de tractaments de dades personals diferents mesures de responsabilitat activa per tal de demostrar el compliment del que disposa el Reglament. Entre aquestes mesures hi ha la certificació.

En els considerants, el Reglament subratlla que perquè aconsegueixi més transparència i compliment cal fomentar l'establiment de mecanismes de certificació i segells i marques de protecció de dades que permetin als interessats avaluar més ràpidament el nivell de protecció de dades dels productes i els serveis corresponents. Per això, insta els estats membres, les autoritats de control, el Comitè i la Comissió a promoure, en particular en l'àmbit de la Unió, la creació de mecanismes de certificació en matèria de protecció de dades i de segells i marques de protecció de dades, per demostrar el compliment del Reglament en les operacions de tractament, i fa una menció especial a tenir en compte les necessitats específiques de les microempreses i les petites i mitjanes empreses.

Per tant, cal distingir entre:

- CERTIFICACIÓ**:** procés metodològic d'avaluació mitjançant el qual una tercera part garanteix la conformitat d'una persona, un producte, un servei o un sistema d'informació amb uns criteris preestablerts.

- ESQUEMA DE CERTIFICACIÓ**:** estableix les regles i els procediments que han de seguir i les gestions que han de fer les persones i les organitzacions públiques o privades que es volen certificar.

En el cas de l'RGPD, el mecanisme de certificació afecta tant responsables com encarregats del tractament. És important aclarir que el simple fet que un responsable o un encarregat disposi d'una certificació no en limita la responsabilitat pel que fa al compliment. Per això, si escau, davant una irregularitat, l'autoritat de control pot exercir les seves funcions i poders, entre els quals hi ha el sancionador.

En aquest sentit, l'RGPD estableix entre les funcions de les autoritats de protecció de dades algunes relacionades amb les certificacions:

- Fomentar la creació de mecanismes de certificació de la protecció de dades i de segells i marques de protecció de dades i aprovar els criteris de certificació.

- Revisar periòdicament, si escau, les certificacions expedides.

Aquesta certificació és voluntària. És un mecanisme opcional que l'RGPD posa a disposició de responsables i encarregats per facilitar-ne el compliment. A més, la certificació ha d'estar disponible a través d'un procés transparent i ha de ser expedida pels organismes de certificació o per l'autoritat de control competent, sobre la base dels criteris aprovats per aquesta autoritat de control o pel Comitè. Cal tenir en compte que quan els criteris siguin aprovats pel Comitè això podrà donar lloc a una certificació comuna denominada Segell Europeu de Protecció de Dades.

Amb caràcter general, en qualsevol procés de certificació intervenen tres parts clarament diferenciades, que són:

- L'organisme que elabora les normes tècniques que determinen els requisits específics de la certificació (esquema de certificació).

- L'entitat o organisme de certificació, que és la que emet el document oficial que demostra el compliment de les normes tècniques.

- L'entitat o persona certificada.

A més, els organismes de certificació han d'expedir i renovar les certificacions una vegada informada l'autoritat de control, a fi que, si no es compleixen o deixen de complir-se els requisits per a la certificació, l'AEPD pugui retirar una certificació o ordenar a l'organisme de certificació que retiri una certificació emesa o que no s'emeti una certificació.

Per poder expedir, renovar o retirar certificacions, aquests organismes de certificació han de tenir un nivell adequat de perícia. Per això, l'RGPD estableix que els estats membres han de garantir que aquests organismes siguin acreditats per l'autoritat de control o per l'organisme nacional d'acreditació designat de conformitat amb la norma EN ISO/IEC 17065/2012 i amb els requisits addicionals establerts per l'autoritat de control competent (AEPD).[1]

El capítol IV sobre codis de conducta i certificació del títol V de la LOPDGDD regula aquesta qüestió en l'àmbit nacional. A més de les funcions de l'autoritat de protecció de dades, l'article 39 atribueix funcions de certificació a l'Entitat Nacional d'Acreditació (ENAC) al nostre país, la qual ha de comunicar a l'Agència Espanyola de Protecció de Dades i a les autoritats de protecció de dades de les comunitats autònomes les concessions, les denegacions o les revocacions de les acreditacions, així com la seva motivació.

4.3.2. Consideració especial sobre la certificació de delegats de protecció de dades

1 Segons la norma esmentada, el nostre organisme d'acreditació és l'Entitat Nacional de Certificació (ENAC), associació sense ànim de lucre, declarada d'utilitat pública, que va ser designada pel Govern per operar a Espanya com l'únic organisme nacional d'acreditació.

L'AEPD, en col·laboració amb l'Entitat Nacional de Certificació (ENAC), ha posat en marxa un procés per certificar, de manera voluntària, delegats de protecció de dades, amb la finalitat d'oferir seguretat i fiabilitat tant als professionals de la privacitat com a les empreses i els ens que incorporen la figura del delegat en les seves organitzacions. Aquesta certificació serveix per acreditar la seva qualificació i capacitat professional.

En aquest sentit, tenint en compte les parts que hi intervenen i atenent amb caràcter general els requisits que s'han exposat anteriorment, ha quedat configurat de la manera següent:

- L'organisme propietari de l'esquema de certificació és l'Agència Espanyola de Protecció de Dades, que rep suport i assessorament d'un comitè tècnic representat per les associacions sectorials els associats de les quals estan obligats a nomenar un delegat de protecció de dades, així com entitats que ja compten amb un certificat de professionals de la privacitat, a més de representants de les universitats.

- L'ENAC és l'encarregada que les entitats de certificació compleixin els requisits necessaris per acreditar-se com a tals.

- Les entitats de certificació són les que emeten el document oficial que certifica que el delegat de protecció de dades compleix els requisits exigits per l'Esquema de Certificació, disposa dels coneixements necessaris i està en disposició d'exercir les seves funcions com a tal.

El propòsit de l'esquema de certificació és establir les normes i el procediment que han de seguir les persones o els professionals que volen certificar-se com a delegats de protecció de dades. S'hi inclouen els prerequisits que ha de complir abans de presentar-se a l'examen i el temari que ha de conèixer per superar-lo. Si aprova l'examen, pot aconseguir el certificat.

En l'Esquema també s'inclou tota la informació, els requisits i els procediments exigits a les entitats de certificació per poder atorgar, suspendre o retirar certificats.

4.4. Transferències internacionals de dades

4.4.1. Marc general de les transferències

L'RGPD assenyala en el considerant 6 que

> «L'evolució tecnològica ràpida i la globalització han plantejat nous reptes per a la protecció de les dades personals. La magnitud de la recollida i de l'intercanvi de dades personals ha augmentat de manera significativa. [...] La tecnologia ha transformat tant l'economia com la vida social, i ha de facilitar encara més la lliure circulació de dades personals dins la Unió i la transferència a tercers països i organitzacions internacionals

> i alhora garantir un nivell elevat de protecció de les dades personals.»

Segons el considerant 101,

> «Els fluxos transfronterers de dades personals a i des de països que no pertanyen a la Unió i organitzacions internacionals són necessaris per a l'expansió del comerç i la cooperació internacionals. L'augment d'aquests fluxos planteja nous reptes i inquietuds pel que fa a la protecció de les dades de caràcter personal. No obstant això, el fet que les dades personals es transfereixen de la Unió a responsables, encarregats o altres destinataris en tercers països o a organitzacions internacionals no ha de menyscabar el nivell de protecció de les persones físiques garantit en la Unió per aquest Reglament, ni tan sols en les transferències ulteriors de dades personals des del tercer país o organització internacional a responsables i encarregats en el mateix país o en un altre tercer país o organització internacional. En qualsevol cas, les transferències a tercers països i organitzacions internacionals només poden dur-se a terme de plena conformitat amb aquest Reglament. Una transferència només podria tenir lloc si, a reserva de les altres disposicions d'aquest Reglament, el responsable o l'encarregat compleix les disposicions d'aquest Reglament relatives a la transferència de dades personals a tercers països o organitzacions internacionals.»

Com a principi general per a la transferència internacional, l'RGPD, en l'article 44, estableix que

> «Només es poden fer transferències de dades personals que siguin objecte de tractament o ho hagin de ser després de ser transferides a un tercer país o organització internacional si, a reserva de les altres disposicions d'aquest Reglament, el responsable i l'encarregat del tractament compleixen les condicions que s'estableixen en aquest capítol, incloent-hi les relatives a les transferències ulteriors de dades personals des del tercer país o organització internacional a un altre tercer país o una altra organització internacional. Totes les disposicions d'aquest capítol s'han d'aplicar per assegurar que el nivell de protecció de les persones físiques garantit per aquest Reglament no es veu menyscabat.»

Tanmateix, atès que l'RGPD no inclou una definició de transferència internacional de dades, potser resulta adequat, a l'efecte de claredat didàctica i amb caràcter general, tenir com a referència la definició encara vigent de l'article 5.1.*s*) de l'RLOPD:

> «tractament de dades que suposa transmetre-les fora del territori de l'Espai Econòmic Europeu (EEE), tant si constitueix una cessió o comunicació de dades com si té per objecte dur a terme un tractament de dades a compte del responsable del fitxer establert en territori espanyol».

Per tant, quan la transmissió de les dades tengui com a destinació algun estat de l'EEE (UE més Noruega, Islàndia i Liechtenstein), no es produeix una transferència internacional de dades des de la perspectiva jurídica. Només s'està davant una transferència internacional de dades, quan es transmeten fora de l'EEE, ja sigui amb destinació a un altre responsable del tractament, que decidirà sobre la finalitat, el contingut i l'ús del tractament, o a un encarregat del tractament, que les tractarà a compte del responsable.

> Des de finals de l'any 2015 les transferències internacionals de dades de caràcter personal han tingut una rellevància pública després de les revelacions incloses en el denominat cas Snowden i, sobretot, amb la sentència del Tribunal de Justícia de la Unió

Europea, que va invalidar la Decisió de port segur de la Comissió Europea, que considerava que les entitats dels Estats Units adherides a aquest sistema adoptat per la Comissió europea l'any 2000 no proporcionaven un nivell adequat de protecció. El port segur va ser substituït pel denominat Acord de l'escut de privacitat (Privacy Shield) com a sistema de garanties per poder transmetre dades a les entitats establertes als Estats Units d'Amèrica que hagin optat per adherir-se al sistema de garanties per a les transferències internacionals incloses en aquest marc.

L'RGPD estableix en la regulació que només es poden transmetre dades als països, els territoris, els sectors o els organismes internacionals respecte dels quals la Comissió Europea ha considerat que disposen d'un nivell adequat de protecció o, en un altre cas, si s'aporten garanties suficients o es donen algunes de les circumstàncies previstes com a excepcions, i sempre que s'observin els altres requisits de l'RGPD esmentat.

LA PRIMERA QÜESTIÓ QUE CAL DESTACAR ÉS QUE L'RGPD ESTABLEIX sense cap dubte que l'exportador de dades pot ser tant un responsable com un encarregat del tractament.

Així mateix, s'amplia el ventall d'instruments en què es poden incloure i aportar les garanties adequades per protegir els drets dels afectats a conseqüència de la transferència de dades. Així, s'hi incorporen els codis de conducta i els mecanismes de certificació com a instruments que poden aportar aquestes garanties, a més de les normes corporatives vinculants (conegudes per les seves sigles en anglès, BCR) per als grups multinacionals. Aquesta gamma més àmplia d'instruments hauria de facilitar la tasca dels exportadors en disposar d'un major ventall d'instruments entre els quals triar.

PERÒ ON SÓN MÉS EVIDENTS LES NOVETATS QUE INTRODUEIX L'RGPD ÉS EN EL RÈGIM D'AUTORITZACIÓ I NOTIFICACIÓ PRÈVIA DE LES TRANSFERÈNCIES INTERNACIONALS, que queden reduïdes a molt pocs supòsits.

En el marc de l'RGPD, amb caràcter general, les transferències es poden dur a terme sense necessitat d'autorització prèvia, llevat que les garanties s'aportin a través d'un contracte entre el responsable o l'encarregat del tractament, l'encarregat o el destinatari de les dades personals en el tercer país o l'organització internacional, o d'un acord administratiu entre autoritats públiques, supòsits en què és necessari que existeixi l'autorització de l'autoritat de control, tal com assenyala l'article 46.3 de l'RGPD.

En l'àmbit nacional aquesta matèria ha estat regulada pels articles 40-43 de la LOPDGDD, dels quals deriva el règim jurídic següent:

- L'Agència Espanyola de Protecció de Dades i les autoritats autonòmiques de protecció de dades poden adoptar, de conformitat amb el que disposa l'article 46.2.*c)* del Reglament (UE) 2016/679, clàusules contractuals tipus per fer transferències internacionals de dades, que s'han de sotmetre prèviament al dictamen del Comitè Europeu de Protecció de Dades previst en l'article 64 del Reglament esmentat.

➢ L'Agència Espanyola de Protecció de Dades i les autoritats autonòmiques de protecció de dades poden aprovar normes corporatives vinculants d'acord amb el que preveu l'article 47 del Reglament (UE) 2016/679.

➢ Les transferències internacionals de dades a països o organitzacions internacionals que no compten amb la decisió d'adequació aprovada per la Comissió o que no s'emparin en alguna de les garanties previstes en l'article anterior i en l'article 46.2 del Reglament (UE) 2016/679, requereixen una autorització prèvia de l'Agència Espanyola de Protecció de Dades o, si escau, de les autoritats autonòmiques de protecció de dades, la qual pot atorgar-se en els supòsits següents:

a) Quan la transferència pretén fonamentar-se en l'aportació de garanties adequades amb fonament en clàusules contractuals que no corresponen a les clàusules tipus previstes en l'article 46.2, lletres *c)* i *d)*, del Reglament (UE) 2016/679.
b) Quan la transferència la du a terme algun dels responsables o encarregats a què es refereix l'article 77.1 d'aquesta Llei orgànica i es fon en disposicions incorporades a acords internacionals no normatius amb altres autoritats o organismes públics de tercers estats, que incorporin drets efectius i exigibles per als afectats, incloent-hi els memoràndums d'entesa.

El procediment tindrà una durada màxima de sis mesos.

➢ Els responsables del tractament han d'informar l'Agència Espanyola de Protecció de Dades o, si escau, les autoritats autonòmiques de protecció de dades de qualsevol transferència internacional de dades que pretenguin dur a terme sobre la base de la seva necessitat per a fins relacionats amb interessos legítims imperiosos perseguits per aquells i la concurrència de la resta dels requisits prevists en el darrer paràgraf de l'article 49.1 del Reglament (UE) 2016/679. Així mateix, han d'informar els afectats de la transferència i dels interessos legítims imperiosos perseguits. Aquesta informació ha de facilitar-se abans de fer la transferència. El que disposa aquest article no és aplicable a les activitats que duen a terme les autoritats públiques en l'exercici dels seus poders públics, d'acord amb l'article 49.3 del Reglament (UE) 2016/679.

4.4.2. Transferències basades en una decisió d'adequació

L'RGPD assenyala en el considerant 102 que

> «[...] Els estats membres poden formalitzar acords internacionals que impliquin la transferència de dades personals a tercers països o organitzacions internacionals sempre que aquests acords no afectin aquest Reglament ni cap altra disposició del dret de la Unió i incloguin un nivell adequat de protecció dels drets fonamentals dels interessats.»

Fins ara, la Comissió Europea ha considerat que ofereixen un nivell adequat de protecció els països i els territoris següents:

- Suïssa, l'Argentina, Guernsey, Man, Jersey, illes Fèroe, Andorra, Israel, l'Uruguai i Nova Zelanda.

- El Canadà (només quan a l'entitat destinatària hi sigui aplicable el «Personal Information and Electronic Documents Act»).

- Els Estats Units (només quan l'entitat destinatària de les dades estigui certificada en l'esquema de l'escut de privacitat).

La decisió dictada recentment en l'assumpte Schrems II pel Tribunal de Justícia de la Unió Europea ha invalidat el sistema de l'escut de privacitat. El Comitè Europeu de Protecció de Dades ha publicat unes «Preguntes freqüents sobre la sentència del Tribunal de Justícia de la Unió Europea en l'assumpte C-311/18— Comissària de Protecció de Dades vs Facebook Irlanda i Maximillian Schrems», que ofereixen informació rellevant en aquesta matèria.

4.4.3. Transferències mitjançant les garanties adequades

De conformitat amb el considerant 108 de l'RGPD

> «Si no hi ha una decisió per la qual es constati l'adequació de la protecció de les dades, el responsable o l'encarregat del tractament han de prendre mesures per compensar la falta de protecció de dades en un tercer país mitjançant garanties adequades per a l'interessat. Aquestes garanties adequades poden consistir en el recurs a normes corporatives vinculants, a clàusules tipus de protecció de dades adoptades per la Comissió o per una autoritat de control, o a clàusules contractuals autoritzades per una autoritat de control. Les garanties han d'assegurar l'observança dels requisits de protecció de dades i drets dels interessats adequats al tractament dins la Unió, incloent-hi la disponibilitat per part dels interessats de drets exigibles i d'accions legals efectives, cosa que inclou el dret a obtenir una reparació administrativa o judicial efectiva i a reclamar una indemnització, a la Unió o en un tercer país. En particular, han de referir-se al compliment dels principis generals relatius al tractament de les dades personals i els principis de la protecció de dades des del disseny i per defecte. Les transferències també poden fer-les autoritats o entitats públiques amb entitats o autoritats públiques de tercers països o amb organitzacions internacionals amb competències o funcions corresponents, igualment sobre la base de disposicions incorporades a acords administratius, com un memoràndum d'entesa, que reconeguin drets exigibles i efectius als interessats. Si les garanties figuren en acords

> administratius que no siguin jurídicament vinculants, s'ha de recollir l'autorització de l'autoritat de control competent.»

Així, en l'article 46 es relacionen les garanties adequades que poden ser aportades sense que es requereixi cap autorització expressa d'una autoritat de control:

- un instrument jurídicament vinculant i exigible entre les autoritats o organismes públics;
- normes corporatives vinculants;
- clàusules tipus de protecció de dades adoptades per la Comissió;
- clàusules tipus de protecció de dades adoptades per una autoritat de control i aprovades per la Comissió;
- un codi de conducta aprovat de conformitat amb l'article 40, juntament amb compromisos vinculants i exigibles del responsable o l'encarregat del tractament en el tercer país d'aplicar garanties adequades, incloent-hi les relatives als drets dels interessats;
- un mecanisme de certificació aprovat de conformitat amb l'article 42, juntament amb compromisos vinculants i exigibles del responsable o l'encarregat del tractament en el tercer país d'aplicar garanties adequades, incloent-hi les relatives als drets dels interessats.

Per la seva banda, l'AEPD també ha contribuït a facilitar la tasca d'aportar garanties, elaborant el 2012 un conjunt de clàusules estàndards, sobre la base de les que va establir la Comissió en la Decisió 2010/87/UE, per a les transferències internacionals fetes entre un encarregat del tractament com a exportador i un subencarregat importador de les dades.

Les garanties s'estableixen a favor dels interessats, motiu pel qual les clàusules són exigibles no només pels signants del contracte, sinó també pels interessats, en particular quan siguin perjudicats per l'incompliment del contracte. Per això, tots els models contenen una clàusula, denominada de tercer beneficiari, per la qual els interessats poden exigir el compliment del contracte, malgrat que no en siguin part.

4.4.4. Normes corporatives vinculants (BCR)

L'RGPD assenyala, en el considerant 110, en relació amb les BCR, que:

> «Qualsevol grup empresarial o unió d'empreses dedicades a una activitat econòmica conjunta ha de tenir la possibilitat d'invocar normes corporatives vinculants autoritzades per a les seves transferències internacionals de la Unió a organitzacions dins el mateix grup empresarial o unió d'empreses dedicades a una activitat econòmica conjunta, sempre que aquestes normes corporatives incorporin tots els

> principis essencials i drets aplicables per tal d'oferir garanties adequades per a les transferències o categories de transferències de dades de caràcter personal.»

En aquest sentit, en l'RGPD es defineixen les BCR com

> «les polítiques de protecció de dades personals assumides per un responsable o un encarregat del tractament establert en el territori d'un estat membre per a transferències o un conjunt de transferències de dades personals a un responsable o un encarregat en un o més països tercers, dins un grup empresarial o una unió d'empreses dedicades a una activitat econòmica conjunta» (article 4 apartat 20).

Per ser aprovades per l'autoritat de control competent, l'RGPD estableix una sèrie de requisits que s'han plasmat en diversos documents elaborats pel denominat Grup de l'Article 29, substituït pel Comitè Europeu de Protecció de Dades a partir del 25 de maig de 2018.

Aquests requisits s'enumeren en l'article 47 de l'RGPD, que exigeix de les BCR que:

- siguin jurídicament vinculants i s'apliquin i siguin complertes per tots els membres corresponents del grup empresarial o de la unió d'empreses dedicades a una activitat econòmica conjunta, incloent-hi els seus empleats;

- confereixin expressament als interessats drets exigibles en relació amb el tractament de les seves dades personals; i

- compleixin i incloguin, com a mínim els requisits i elements següents:

a) l'estructura i les dades de contacte del grup empresarial o de la unió d'empreses dedicades a una activitat econòmica conjunta i de cadascun dels seus membres;
b) les transferències o conjunts de transferències de dades, incloent-hi les categories de dades personals, el tipus de tractaments i els seus fins, el tipus d'interessats afectats i el nom del tercer o els tercers països en qüestió;
c) el seu caràcter jurídicament vinculant, tant internament com externa;
d) l'aplicació dels principis generals en matèria de protecció de dades, en particular la limitació de la finalitat, la minimització de les dades, els períodes de conservació limitats, la qualitat de les dades, la protecció de les dades des del disseny i per defecte, la base del tractament, el tractament de categories especials de dades personals, les mesures encaminades a garantir la seguretat de les dades i els requisits respecte a les transferències ulteriors a organismes no vinculats per les normes corporatives vinculants;
e) els drets dels interessats en relació amb el tractament i els mitjans per exercir-los, en particular el dret a no ser objecte de decisions basades exclusivament en un tractament automatitzat, incloent-hi l'elaboració de perfils de conformitat amb el que disposa l'article 22, el dret a presentar una reclamació davant l'autoritat de control competent i davant els tribunals competents dels estats membres de conformitat amb l'article 79, i el dret a obtenir una reparació i, quan escaigui, una indemnització per violació de les normes corporatives vinculants;
f) l'acceptació per part del responsable o de l'encarregat del tractament establerts en el territori d'un estat membre de la responsabilitat per qualsevol violació de les normes corporatives vinculants per part de qualsevol membre no establert en la Unió; el responsable o l'encarregat només serà exonerat, totalment o parcialment, d'aquesta responsabilitat si demostra que l'acte que va originar els danys i perjudicis no és imputable a aquest membre;

g) la manera com es facilita als interessats la informació sobre les BCR, en particular pel que fa a les disposicions establertes en les lletres *d)*, *e)* i *f)* d'aquest apartat, a més dels articles 13 i 14 relatius a la informació que cal facilitar als interessats;
h) les funcions de tot delegat de protecció de dades designat, o de qualsevol altra persona o entitat encarregada de la supervisió del compliment de les normes corporatives vinculants dins el grup empresarial o de la unió d'empreses dedicades a una activitat econòmica conjunta, així com de la supervisió de la formació i de la tramitació de les reclamacions;
i) els procediments de reclamació;
j) els mecanismes establerts dins el grup empresarial o de la unió d'empreses dedicades a una activitat econòmica conjunta per garantir la verificació del compliment de les normes corporatives vinculants. Aquests mecanismes inclouen auditories de protecció de dades i mètodes per garantir accions correctives per protegir els drets de l'interessat. Els resultats d'aquesta verificació haurien de comunicar-se a la persona o l'entitat a què es refereix la lletra *h)* i al consell d'administració de l'empresa que controla un grup empresarial, o de la unió d'empreses dedicades a una activitat econòmica conjunta, i posar-se a disposició de l'autoritat de control competent que ho sol·liciti;
k) els mecanismes establerts per comunicar i registrar les modificacions introduïdes en les normes i per notificar aquestes modificacions a l'autoritat de control;
l) el mecanisme de cooperació amb l'autoritat de control per garantir el compliment per part de qualsevol membre del grup empresarial o de la unió d'empreses dedicades a una activitat econòmica conjunta, en particular posant a disposició de l'autoritat de control els resultats de les verificacions de les mesures establertes en la lletra *j)*;
m) els mecanismes per informar l'autoritat de control competent de qualsevol requisit jurídic d'aplicació en un país tercer a un membre del grup empresarial o de la unió d'empreses dedicades a una activitat econòmica conjunta, que probablement tenen un efecte advers sobre les garanties establertes en les normes corporatives vinculants, i
n) la formació en protecció de dades pertinent per al personal que té accés permanent o habitual a dades personals.

4.4.5. Excepcions per a situacions específiques

Addicionalment, es consideren una sèrie d'excepcions als supòsits generals per a la transferència internacional de dades. AIXÍ, S'INDICA EN EL CONSIDERANT 111 DE L'RGPD QUE

> «S'ha d'establir la possibilitat de fer transferències en determinades circumstàncies, d'intervenir per al consentiment explícit de l'interessat, si la transferència és ocasional i necessària en relació amb un contracte o una reclamació, independentment de si es tracta d'un procediment judicial o un procediment administratiu o extrajudicial, incloent-hi els procediments davant organismes reguladors. També s'ha d'establir la possibilitat de fer transferències quan ho requereixin raons importants d'interès públic establertes pel dret de la Unió o dels estats membres, o quan la transferència es faci a partir d'un registre establert per llei i es destini a consulta pel públic o per persones que en tenguin un interès legítim. En aquest darrer cas, la transferència no ha d'afectar la totalitat de les dades personals o de les categories de dades incloses en el registre i, quan el registre estigui destinat a ser consultat per persones que en tenguin un interès legítim, la transferència només ha de fer-se a petició d'aquestes persones o, si aquestes en seran les destinatàries, tenint plenament en compte els interessos i els drets fonamentals de l'interessat.»

I segons el considerant 112:

> «Aquestes excepcions han d'aplicar-se en particular a les transferències de dades requerides i necessàries per raons importants d'interès públic, per exemple en cas d'intercanvis internacionals de dades entre autoritats en l'àmbit de la competència, administracions fiscals o duaneres, entre autoritats de supervisió financera, entre serveis competents en matèria de seguretat social o de sanitat pública, per exemple en cas contactes destinats a localitzar malalties contagioses o per reduir i/o eliminar el dopatge en l'esport. La transferència de dades personals també ha de considerar-se lícita en cas que sigui necessària per protegir un interès essencial i vital de l'interessat o d'una altra persona, incloent-hi la integritat física o la vida, si l'interessat no està en condicions de donar-hi el consentiment. Si no hi ha una decisió d'adequació, el dret de la Unió o dels estats membres pot limitar expressament, per raons importants d'interès públic, la transferència de categories específiques de dades a un tercer país o a una organització internacional. Els estats membres han de notificar aquestes disposicions a la Comissió. Pot considerar-se necessària, per una raó important d'interès públic o per ser d'interès vital per a l'interessat, qualsevol transferència a una organització internacional humanitària de dades personals d'un interessat que no tengui capacitat física o jurídica per donar-hi el consentiment, per tal de dur complir una comesa basada en les Convencions de Ginebra o de conformar-se al dret internacional humanitari aplicable en cas de conflictes armats.»

Atès que es consideren excepcions al règim general, l'RGPD, com ja el va fer el Grup de l'article 29 en el seu document WP 114,[2] aclareix el règim restrictiu de l'ús d'aquestes excepcions, per la qual cosa, de conformitat amb el considerant 113:

> «Les transferències que poden qualificar-se de no repetitives i que només es refereixen a un nombre limitat d'interessats també han de ser possibles en cas que serveixin per interessos legítims imperiosos del responsable del tractament, si no hi prevalen sobre els interessos o els drets i les llibertats de l'interessat i el responsable ha avaluat totes les circumstàncies concurrents en la transferència de dades. El responsable ha de prestar especial atenció a la naturalesa de les dades personals, la finalitat i la durada de l'operació o les operacions de tractament propostes i la situació al país d'origen, el tercer país i el país de destinació final i oferir garanties apropiades per protegir els drets fonamentals i les llibertats de les persones físiques respecte al tractament de les seves dades personals. Aquestes transferències només han de ser possibles en casos aïllats, quan cap dels altres motius per a la transferència no hi són aplicables. Les expectatives legítimes de la societat en un augment del coneixement s'han de tenir en compte per a fins d'investigació científica o històrica o fins estadístics. El responsable ha d'informar de la transferència l'autoritat de control i l'interessat.»

2 WP 114 Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995. Podeu consultar-lo en l'adreça següent https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf