Versió 11.11.2019

L'encarregat del tractament en el Reglament General de Protecció de Dades (RGPD)

Aquest document, elaborat inicialment per l'Autoritat Catalana de Protecció de Dades en col·laboració amb l'Agència Espanyola de Protecció de Dades i l'Agència Basca de Protecció de Dades, té com a objectiu identificar els punts clau a tenir en compte en el moment d'establir la relació entre el responsable del tractament i l'encarregat del tractament, així com identificar les qüestions que afecten de manera directa la gestió de la relació entre tots dos.

Ha estat actualitzat amb les modificacions incorporades per la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

Així mateix pretén oferir orientacions, a manera de recomanació, per confeccionar el document que ha de regular aquesta relació.

1.- Què és un encarregat del tractament i quina és la seva funció principal?

L'encarregat del tractament és la persona física o jurídica, autoritat pública, servei o organisme que presta al responsable un servei que comporta el tractament de dades personals per compte d'aquest.

Els tipus d'encarregat del tractament i les formes de regular-ne la relació poden ser tan variades com els tipus de serveis que poden suposar accés a dades personals. Així, podem trobar serveis que tenen com a objecte principal el tractament de dades personals (per exemple, una empresa o entitat pública que ofereix un servei d'allotjament d'informació en els seus servidors) i uns altres que tracten dades personals només com a conseqüència de l'activitat que presten per compte del responsable del tractament (per exemple, el gestor d'un servei públic municipal).

Tot i que la definició pot semblar clara, a la pràctica es donen multitud de situacions en què pot ser difícil delimitar quan ens trobem davant d'un encarregat i quan davant d'un responsable del tractament. Per facilitar aquesta distinció, hem de tenir en compte que correspon al responsable decidir sobre la finalitat i els usos de la informació, mentre que l'encarregat del tractament ha de complir les instruccions de qui li encomana un determinat servei, en relació amb el tractament de les dades personals a les quals té accés com a conseqüència de la prestació d'aquest servei.

Quan s'aplica la Llei 9/2017, de 8 de novembre, de contractes del sector públic (LCSP), cal tenir en compte que aquesta llei preveu (disposició addicional 25a) que si la contractació implica l'accés del contractista a dades de caràcter personal del tractament de les quals n'és responsable l'entitat contractant, el contractista té la consideració d'encarregat del tractament. En aquests casos, el règim establert en l'RGPD també s'aplica.

Si l'encarregat estableix relacions amb les persones afectades en el seu propi nom i sense que consti que actua per compte del responsable del tractament, se'l considerarà responsable del tractament, encara que s'hagi formalitzat un contracte d'encàrrec del tractament o un altre acte jurídic amb el contingut de l'article 28.3 RGPD. Aquesta previsió no és d'aplicació però als encàrrecs del tractament fets en el marc de la legislació de contractes del sector públic.

També se'l considerarà responsable del tractament si utilitza les dades per a les seves pròpies finalitats.

2.- Quins tractaments pot dur a terme un encarregat sobre les dades que li han estat encomanades?

L'encarregat pot efectuar tots els tractaments, automatitzats o no, que el responsable del tractament li encomani formalment. La definició de tractament ens permet concretar-los, atenent al cicle de vida de la informació: recollida, registre, organització, estructuració, conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per a transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

En tot cas, en l'acord que s'adopti han de quedar clarament delimitats.

3.- Quin nivell de decisió pot assumir un encarregat del tractament?

L'encarregat del tractament pot adoptar qualsevol decisió organitzativa i operacional necessària per prestar el servei que té contractat. En cap cas pot variar les finalitats i els usos de les dades, ni pot utilitzar-les per a les seves pròpies finalitats.

Les decisions que adopta han de respectar les instruccions del responsable del tractament.

4.- El responsable del tractament pot triar qualsevol encarregat del tractament?

El responsable del tractament ha de triar un encarregat del tractament que ofereixi garanties suficients respecte de la implantació i el manteniment de les mesures tècniques i organitzatives apropiades, d'acord amb el que estableix l'RGPD, i que

garanteixi la protecció dels drets de les persones afectades. Per tant, hi ha un deure de diligència a l'hora d'escollir l'encarregat.

El considerant 81 de l'RGPD disposa que l'encarregat del tractament ha d'oferir garanties suficients pel que fa a coneixements especialitzats, fiabilitat i recursos, amb vista a l'aplicació de mesures tècniques i organitzatives que compleixin els requisits del Reglament, inclosa la seguretat del tractament.

Per demostrar que l'encarregat ofereix garanties suficients, l'RGPD preveu que l'adhesió a codis de conducta o la possessió d'un certificat de protecció de dades serveixen com a mecanismes de prova.

5.- Com s'han de regular les relacions entre el responsable i l'encarregat del tractament?

La regulació de la relació entre el responsable i l'encarregat del tractament s'ha d'establir a través d'un contracte o d'un acte jurídic similar que els vinculi. El contracte o l'acte jurídic ha de constar per escrit, inclòs en format electrònic.

La possibilitat de regular aquesta relació a través d'un acte jurídic unilateral del responsable del tractament és una de les novetats que preveu l'RGPD. En qualsevol cas, ha de ser un acte jurídic que estableixi i defineixi la posició de l'encarregat del tractament, sempre que aquest acte vinculi jurídicament l'encarregat del tractament. Aquest seria el cas, per exemple, d'una resolució administrativa que consti notificada a l'encarregat del tractament.

L'article 33.5 de l'LOPDGDD estableix que en l'àmbit del sector públic poden atribuir-se les competències pròpies d'un encarregat del tractament a un determinat òrgan de l'Administració o a organismes autònoms vinculats o dependents mitjançant l'adopció d'una norma reguladora de les seves competències, que haurà d'incorporar el contingut exigit per l'article 28.3 de l'RGPD.

En qualsevol cas, tant si es tracta d'un acord com d'un altre acte jurídic, el contingut ha de reunir els requisits establerts en l'RGPD, als quals es fa referència més endavant.

El contingut de l'acte o de l'acord es pot basar en clàusules tipus establertes per la Comissió Europea o per l'autoritat de control, inclòs quan formin part d'una certificació atorgada al responsable o a l'encarregat del tractament.

Els models de clàusules que s'inclouen a l'annex 1 d'aquest document no tenen la consideració de clàusules tipus a l'efecte de l'article 28.8 de l'RGPD, sinó que simplement són un model orientatiu perquè els diferents responsables puguin adaptar-lo a les necessitats derivades de la seva pròpia organització.

6.- Qui és responsable dels tractaments duts a terme per l'encarregat?

El responsable del tractament no perd aquesta consideració en cap cas. Per tant, continua sent responsable que les dades personals es tractin correctament i de la garantia dels drets de les persones afectades. El responsable té una obligació d'especial diligència en l'elecció i la supervisió de l'encarregat.

7.-L'RGPD només s'aplica als encarregats establerts al territori de la Unió Europea?

No, el Reglament s'aplica al tractament de dades personals en el context de les activitats d'un establiment de l'encarregat a la Unió, independentment de si el tractament té lloc a la Unió o no.

D'altra banda, l'RGPD també s'aplica al tractament de dades personals d'interessats que resideixen a la Unió, efectuat per un encarregat no establert en la Unió, quan les activitats de tractament estan relacionades amb:

a) L'oferta de béns o serveis als esmentats interessats a la Unió, independentment de si se'ls requereix pagament o no.

b) El control del seu comportament, en la mesura que tingui lloc a la Unió.

8.- Hi ha un règim especial per contractar un encarregat que no estigui establert al territori de la Unió Europea o que efectuï el tractament fora del territori de la Unió?

La comunicació de dades personals, en el marc d'un acord d'encarregat del tractament, a un país que no formi part de la Unió es regeix per la regulació establerta en el Reglament per a les transferències internacionals.

La transferència a un tercer país no pot suposar en cap cas una reducció del nivell de protecció de les persones que estableix el Reglament. Aquest principi també s'aplica en les transferències posteriors de dades personals, des del tercer país a un altre tercer país o a una organització internacional.

Per a la transferència de dades a països que no garanteixen un nivell de protecció adequat, el responsable ha d'acreditar que l'encarregat del tractament està en disposició d'oferir garanties adequades. En tot cas, ha de garantir que els interessats compten amb drets exigibles i accions legals efectives.

9.- ¿Si s'externalitza les funcions del delegat de protecció de dades a un tercer, aquest té la consideració d'encarregat del tractament?

Sí, l'RGPD preveu que el delegat de protecció de dades ha de poder accedir a les dades que es tractin. Per tant, s'haurà formalitzar un encàrrec del tractament.

10.- Cal informar els interessats de la contractació d'un encarregat del tractament?

L'LOPDGDD no considera l'accés de l'encarregat del tractament com una comunicació de dades, si s'han complert els requisits establerts per l'RGPD. Per això, no seria exigible incloure informació sobre l'existència i, si escau, la identitat dels encarregats del tractament entre la informació sobre les comunicacions que cal facilitar a les persones interessades. Tot i això, en determinades circumstàncies (atenent, per exemple, a la naturalesa del tractament, a les dades tractades, a l'existència de tractament de la informació als sistemes de l'encarregat, especialment si això implica una transferència a tercers països, o per altres circumstàncies concurrents) pot ser convenient que es doni informació, com a mínim, sobre l'existència d'encarregats del tractament, per a una major transparència en el tractament de les dades personals. La informació sobre la identitat dels encarregats pot oferir-se per mitjans electrònics a través d'un web, de manera que permeti la seva actualització immediata.

11.- Quin és el contingut mínim d'un acord o acte d'encàrrec del tractament?

Com a mínim cal establir l'objecte, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i les categories d'interessats, així com les obligacions i els drets del responsable.

En particular, l'acord o acte ha de contenir:

A.- Les instruccions del responsable del tractament

Cal documentar de manera precisa les instruccions respecte de l'encàrrec realitzat. Cal identificar de forma clara i concreta quins són els tractaments de dades que ha de dur a terme l'encarregat del tractament, atenent al tipus de servei prestat i a la manera de prestar-lo. És especialment necessari determinar de forma clara les comunicacions a tercers que el responsable encomana a l'encarregat o que es deriven del servei prestat.

La subjecció a les instruccions del responsable s'ha de produir, igualment, en el cas de les transferències internacionals de dades que es produeixen com a conseqüència de la prestació del servei. Si el dret de la Unió o d'un estat membre obliga legalment l'encarregat del tractament a transferir dades a un tercer país, cal que n'informi el responsable abans de dur a terme el tractament, tret que aquest dret ho prohibeixi per raons importants d'interès públic.

Si l'encarregat del tractament considera que alguna de les instruccions infringeix l'RGPD, l'LOPDGDD o qualsevol altra disposició en matèria de protecció de dades de la Unió o dels estats membres, l'encarregat n'ha d'informar immediatament el responsable.

B.- El deure de confidencialitat

Cal establir la forma en què l'encarregat del tractament garantirà que les persones autoritzades per tractar dades personals s'han compromès, de forma expressa, a respectar la confidencialitat o que, si escau, estan subjectes a una obligació de confidencialitat de naturalesa estatutària.

El compliment d'aquesta obligació ha de quedar documentat i a disposició del responsable del tractament.

C.- Les mesures de seguretat

L'acord ha d'establir l'obligació de l'encarregat d'adoptar totes les mesures de seguretat necessàries, de conformitat amb el que estableix l'article 32 de l'RGPD.

Correspon al responsable del tractament fer l'avaluació de riscos per determinar les mesures de seguretat apropiades per garantir la seguretat de la informació tractada i els drets de les persones afectades. Així mateix, l'encarregat també ha d'avaluar els possibles riscos derivats del tractament, tenint en compte els mitjans emprats (tecnologies, recursos etc.) i altres circumstàncies que puguin incidir en la seguretat, como per exemple que l'encarregat dugui a terme altres tractaments.

A partir d'aquí, les mesures de seguretat concretes es poden determinar amb una llista exhaustiva o amb una remissió a un estàndard o marc nacional o internacional reconegut. En l'àmbit del sector públic, aquestes mesures de seguretat hauran d'ajustar-se a l'Esquema Nacional de Seguretat.

Així, tenint en compte l'estat de la tècnica, els costos d'aplicació i la naturalesa, l'abast, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat variables per als drets i les llibertats de les persones físiques, el responsable i l'encarregat del tractament han d'establir les mesures tècniques i organitzatives apropiades per garantir el nivell de seguretat adequat al risc existent que, si escau, poden incloure, entre d'altres:

a) La seudonimització i el xifrat de dades personals.

b) La capacitat de garantir la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i els serveis de tractament.

c) La capacitat de restaurar la disponibilitat i l'accés a les dades personals de forma ràpida, en cas d'incident físic o tècnic.

d) Un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives que garanteixen la seguretat del tractament.

L'adhesió a codis de conducta o la possessió d'una certificació són elements que serveixen per demostrar el compliment dels requisits indicats anteriorment.

El responsable i l'encarregat del tractament han de prendre mesures per garantir que qualsevol persona que actua sota la seva autoritat, i té accés a dades personals, només pot tractar-les seguint instruccions del responsable, tret que hi estigui obligada en virtut del dret de la Unió o dels estats membres.

D.- El règim de la subcontractació

L'acord ha d'establir el règim de subcontractació. L'RGPD exigeix que, quan el servei encomanat comporta que un tercer tracti les dades personals, per recórrer a un altre encarregat (subencarregat) per desenvolupar aquest servei l'encarregat del tractament ha de tenir l'autorització prèvia per escrit del responsable del tractament.

Aquesta autorització pot ser específica (identificació de l'entitat concreta) o general (només autoritzant la subcontractació, però sense concretar l'entitat).

Si l'autorització és de caràcter general, l'encarregat ha d'informar el responsable de la incorporació d'un subencarregat o de la substitució per altres subencarregats; d'aquesta manera, dóna al responsable l'oportunitat d'oposar-se a aquests canvis.

Pot ser útil que l'acord o l'acte estableixi la forma (que, en tot cas, ha de constar per escrit) i el termini perquè el responsable manifesti la seva oposició.

En tot cas, el subencarregat del tractament ha d'estar subjecte a les mateixes condicions (instruccions, obligacions, mesures de seguretat…) i en la mateixa forma (acord per escrit o acte jurídic vinculant) que l'encarregat del tractament, en relació amb el tractament adequat de les dades personals i la garantia dels drets de les persones afectades. Si el subencarregat les incompleix, l'encarregat inicial continua sent plenament responsable del compliment de les obligacions del subencarregat davant del responsable del tractament.

Quan s'aplica la legislació de contractes del sector públic, també cal tenir en compte les disposicions específiques previstes en aquesta llei.

E.- Els drets dels interessats

S’ha d’establir la forma en què l'encarregat del tractament ha d’assistir el responsable, en el compliment de l'obligació de respondre les sol·licituds d'exercici dels drets dels interessats establerts en el capítol III de l’RGPD:

- Accés a dades personals
- Rectificació
- Supressió (dret a l'oblit)
- Limitació del tractament
- Portabilitat de dades
- Oposició
- A no ser objecte de decisions individualitzades automatitzades (inclosa l'elaboració de perfils)

L'acord ha d'establir de forma clara si correspon a l'encarregat del tractament atendre i donar resposta a les sol·licituds d'aquests drets, o bé establir expressament que la seva única obligació és comunicar al responsable del tractament que s'ha exercit un dret.

En el primer supòsit, l'acord ha d'establir la forma i els terminis per atendre o, si escau, donar resposta a les sol·licituds d'exercici de drets. En el segon supòsit, cal establir la forma i el termini en què la sol·licitud i, si escau, la informació corresponent a l'exercici del dret s'ha de comunicar al responsable del tractament.

Quant al dret d'informació de les persones afectades, es tracta d'un dret no subjecte a sol·licitud i, per tant, estrictament no li seria aplicable l’obligació d’assistir el responsable en la seva obligació de respondre. Tot i això, en els casos en què l'encarregat ha de recollir les dades és recomanable que l'acord o acte jurídic estableixi la forma i el moment en què s’ha de donar el dret d'informació.

F.- Col·laboració en el compliment de les obligacions del responsable

Cal establir la forma en què l'encarregat ha d’ajudar el responsable a garantir el compliment de les obligacions relatives a l'aplicació de les mesures de seguretat corresponents, la notificació de violacions de dades a les autoritats de protecció de dades, la comunicació de violacions de dades als interessats, la realització de les avaluacions d'impacte relativa la protecció de dades i, si escau, la realització de consultes prèvies.

El compliment d'aquesta obligació queda supeditat a la naturalesa del tractament efectuat i a la informació que estigui a disposició de l'encarregat.

El responsable pot delegar en l'encarregat el compliment d'aquestes obligacions.

G.- El destí de les dades al finalitzar la prestació

Cal preveure si, una vegada finalitzada la prestació dels serveis de tractament, l'encarregat del tractament ha de procedir a la supressió o a la devolució de les dades personals i de qualsevol còpia existent, ja sigui al responsable o a un altre encarregat designat pel responsable.

L'acord ha d'establir de forma clara quina de les dues opcions ha triat el responsable, així com la forma i el termini en què s'ha de complir. No procedirà la destrucció quan hi hagi una previsió legal que obligui a la seva conservació.

No procedirà la destrucció de les dades quan hi hagi una previsió legal que obligui a la seva conservació, supòsit en què caldrà retornar-les al responsable. Correspon al responsable garantir-ne la conservació mentre persisteixi aquesta obligació.

No obstant això, l'encarregat pot conservar-ne una còpia amb les dades bloquejades mentre es puguin derivar responsabilitats de l'execució de la prestació.

H.- La col·laboració amb el responsable per demostrar el compliment

Cal establir l'obligació de l'encarregat de posar a disposició del responsable tota la informació necessària per demostrar que compleix les obligacions establertes en aquest article, així com l'obligació de permetre i contribuir a les auditories, incloses inspeccions, que efectuï el responsable o un altre auditor autoritzat pel responsable.

I.- Contingut addicional

Per als encàrrecs del tractament sotmesos a la legislació de contractes del sector públic, cal tenir en compte, a més, que al plec de clàusules hi ha de constar (art. 122.2 LCSP):

a) La finalitat per a la qual es cediran les dades al contractista.

b) L'obligació del contractista de sotmetre's en tot cas a la normativa nacional i de la Unió Europea en matèria de protecció de dades, sense perjudici del que estableix l'últim paràgraf de l'apartat 1 de l'article 202.

c) L'obligació de l'empresa adjudicatària de presentar abans de la formalització del contracte una declaració en la que posi de manifest on estaran ubicats els servidors i des d'on es prestaran els serveis associats als mateixos.

d) L'obligació de comunicar qualsevol canvi que es produeixi, al llarg de la vida del contracte, de la informació facilitada a la declaració a què es refereix la lletra c) anterior.

e) L'obligació dels licitadors d'indicar en la seva oferta, si tenen previst subcontractar els servidors o els serveis associats als mateixos, el nom o el perfil empresarial, definit per referència a les condicions de solvència professional o tècnica, dels subcontractistes a qui es vagi a encomanar la seva realització.

12.- S'han d'adaptar a l'RGPD els contractes d'encàrrec formalitzats abans de l'aplicació de l'RGPD?

Els contractes d'encàrrec formalitzats abans de la plena aplicabilitat de l'RGPD (25 de maig de 2018) s'han d'adaptar per respectar el que estableix l'article 28 RGPD. Tot i que moltes de les obligacions derivades del règim establert a l'RGPD ja estan recollides a la normativa espanyola, cal modificar els contractes existents perquè les seves clàusules reflecteixin tots els continguts del Reglament, tenint en compte que les remissions genèriques a l'article de l'RGPD que els regula no són vàlides.

D'acord amb la Disposició transitòria cinquena de l'LOPDGDD, els contractes i acords d'encàrrec del tractament establerts abans de 25 de maig de 2018 mantenen la seva vigència fins la data de venciment assenyalada en els mateixos.

Quan es tracti d'encàrrecs amb durada indefinida, mantenen la vigència fins el 25 de maig de 2022.

En qualsevol cas, durant la vigència del contracte o acord, qualsevol de les parts pot exigir a l'altra la modificació del contracte per adaptar-la al que estableix l'article 28 de l'RGPD.

13.- Es poden considerar encarregades del tractament els qui, malgrat l'existència d'un acord o acte jurídic d'encàrrec del tractament, estableixen relacions amb les persones afectades en nom propi?

D'acord amb l'article 33.1 LOPDGDD, si l'encarregat del tractament estableix relacions amb les persones afectades en nom propi i sense que consti que actua per compte d'un altre, no tindrà la consideració d'encarregat del tractament, malgrat que existeixi un contracte o acte jurídic d'encàrrec del tractament.

Aquesta previsió no és d'aplicació als encàrrecs del tractament que es facin en el marc de la legislació de contractes del sector públic. En aquest cas el contractista tindrà la consideració d'encarregat del tractament en qualsevol cas, i l'administració adjudicatària tindrà la condició de responsable del tractament.