DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

QUADERNS DivalData

Quaderns dirigits a delegats,
responsables i especialistes en protecció
de dades personals

Quadern nº 31 | Gener 2023

Privacitat i serveis cloud en el sector públic

Í N D E X

Privacitat i serveis cloud en el sector públic

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades y Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure't a la nostra publicació accedeix al següent

enllaç

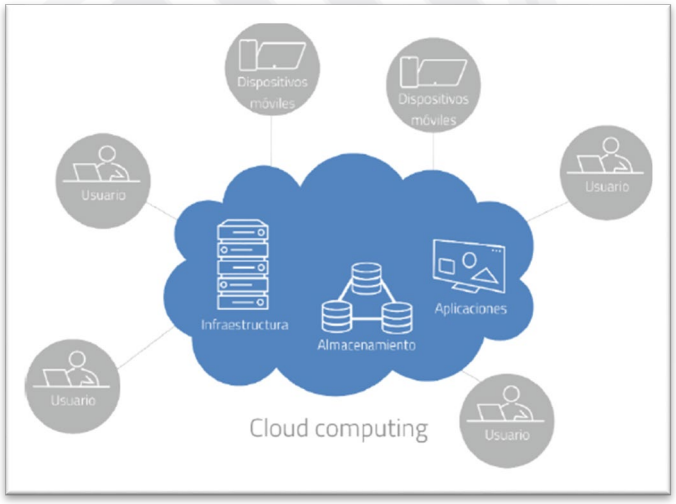
"La principal novetat que van introduir aquestes normes va ser la d'apostar per una Administració Pública, íntegrament electrònica, amb "paper zero" i interconnectada".

INTRODUCCIÓ

Des de fa alguns anys les organitzacions han vingut adaptant-se als continus canvis que s'han produït en la societat, així com als grans avanços tecnològics que hui dia ens permeten accedir a qualsevol tipus de servei, de manera ràpida i senzilla a través d'Internet.

En concret, les administracions públiques han patit una autèntica revolució des de l'entrada en vigor de la Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, i la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic. La principal novetat que van introduir aquestes normes va ser la d'apostar per una Administració Pública, íntegrament electrònica, amb "paper zero" i interconnectada, per a així facilitar les relacions electròniques dels ciutadans i les empreses amb l'Administració.

Arran de l'entrada en vigor d'aquestes normes, tota la documentació, continga o no dades personals, va passar a digitalitzar-se de manera massiva, la qual cosa va provocar que els expedients ja no es conservaren únicament en els espais de treball, com a escriptoris o prestatgeries, sinó que van passar a entorns web mitjançant la computació en núvol o cloud computing amb tots els avantatges i inconvenients que aquest servei puga comportar.



CLOUD COMPUTING

El *cloud computing* o computació en núvol és una nova forma de prestació dels serveis de tractament de la informació.

Aquesta solució permet a l'organització optimitzar l'assignació i el cost dels recursos associats a les seues necessitats de tractament d'informació.

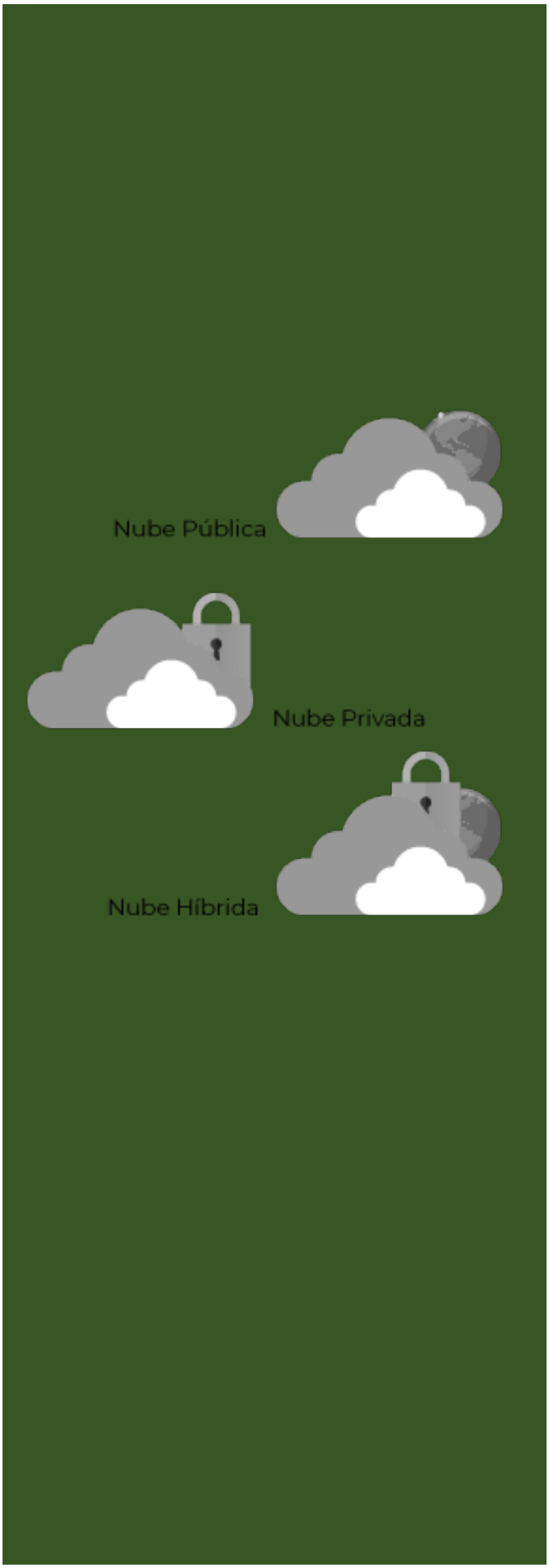
L'organització no té necessitat de realitzar inversions en infraestructura sinó que utilitza la que posa a la seua disposició el prestador del servei, garantint que no es generen situacions de falta o excés de recursos, així com el sobrecost associat a aquestes situacions.

En un entorn de *cloud computing* la gestió de la informació està de manera virtual en mans de l'organització que contracta els serveis del núvol, que la tracta a través d'Internet accedint a solucions de bases de dades, correu electrònic, o qualsevol tipus d'aplicacions d'acord amb les seues necessitats.

El proveïdor del servei pot trobar-se en, pràcticament, qualsevol lloc del món i el seu objectiu últim serà proporcionar els serveis optimitzant els seus propis recursos a través de, per exemple, pràctiques de deslocalització, compartició de recursos i mobilitat o realitzant subcontractacions addicionals.

Això últim és el que la fa realment diferent, ja que permet l'ús de recursos de maquinari, programari, emmagatzematge, serveis i comunicacions que es troben distribuïts geogràficament i als quals s'accedeix a través de xarxes públiques, de manera dinàmica, quan es necessita, mentre es necessita i abonant una tarifa (quan no és gratuïta) sobre el que es consumeix; és a dir, proporcionant a les organitzacions un servei de tecnologies d'informació sota demanda.

"El proveïdor del servei pot trobar-se en, pràcticament, qualsevol lloc del món i el seu objectiu últim serà proporcionar els serveis optimitzant els seus propis recursos."



TIPUS DE 'CLOUD COMPUTING'

No tots els serveis i proveïdors de *cloud computing* són iguals, ni ho són les possibles relacions que s'estableixen entre clients i proveïdors. Els núvols es poden classificar de moltes formes atesos diversos criteris:

NÚVOL PÚBLIC: parlem d'un servei de Núvol Públic quan el proveïdor de serveis de cloud proporciona els seus recursos de manera oberta a entitats heterogènies, sense més relació entre si que haver tancat un contracte amb el mateix proveïdor de servei. Existeixen diverses i nombroses solucions en Núvol Públic i presten els seus serveis des de particulars a grans organitzacions, ja que qualsevol pot contractar amb ells.

NÚVOL PRIVAT: en l'altre extrem podem parlar de Núvol Privat, que la trobem quan una entitat realitza la gestió i administració dels seus serveis en el núvol per a les parts que la formen, sense que en la mateixa puguen participar entitats externes i mantenint el control sobre ella. Un Núvol Privat no necessàriament s'implementa per la mateixa entitat que la utilitza, sinó que pot contractar-se a un tercer que actuarà sota la seua supervisió i en funció de les seues necessitats.

Les entitats que opten pels Núvols Privats són aquelles que són complexes i necessiten centralitzar els recursos informàtics i, alhora, oferir flexibilitat en la disponibilitat d'aquests, per exemple, administracions públiques i grans organitzacions.

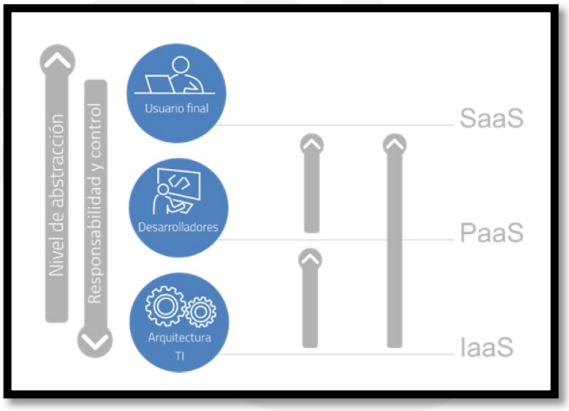
ALTRES MODELS: entre tots dos models es troben solucions intermèdies que prendran diferents noms, com poden ser els Núvols Híbrids, en les quals determinats serveis s'ofereixen de manera pública i altres de manera privada; els Núvols Comunitaris, quan aquests serveis són compartits en una comunitat tancada; o els Núvols Privats Virtuals, quan sobre Núvols Públics s'implementen garanties addicionals de seguretat.

"Els proveïdors del núvol proporcionen accés a recursos informàtics a través de la xarxa, i ofereixen una sèrie de serveis addicionals de valor afegit que acostaran l'oferta del proveïdor a les necessitats del seu client. En funció del complet que siga aqueix valor afegit podem dir que tenim una solució d'Infraestructura com a Servei, Plataforma com a Servei o Software com a Servei."

MODALITATS DEL SERVEI

Ara bé, s'ofereixen una sèrie de categories de servei que es detallen a continuació:

- **IAAS (Infrastructure as a Service):** s'encarrega d'entregar una infraestructura a l'usuari, proporcionant recursos de processament i emmagatzematge a través de la xarxa, sense cap altre valor afegit. El proveïdor s'encarrega de l'administració de la infraestructura i el client té el control sobre els sistemes operatius, emmagatzematge i aplicacions desplegades, així com el control dels components de xarxa.
- **PAAS (Platform as a Service):** s'encarrega d'entregar una plataforma a l'organització client. El client no administra ni controla la infraestructura, però té el control sobre les aplicacions instal·lades i la seua configuració, i pot fins i tot instal·lar noves aplicacions.
  Es proporcionen eines i utilitats per a desenvolupar aplicacions sobre el núvol com a bases de dades o entorns de programació en les quals l'usuari pot desenvolupar les seues pròpies solucions.
- **SAAS (Software as a Service):** podem parlar d'un Núvol de *Software* quan l'usuari troba en el núvol les eines finals amb les quals pot implementar directament els processos de la seua organització: una aplicació de comptabilitat, de correu electrònic, un *worlkflow*, un programa per a la gestió d'expedients, etc.



Un dels majors riscos per a les administracions públiques a l'hora de contractar aquest servei en el núvol és la pèrdua de control i les traves que poden trobar-se quan pretenen demanar la portabilitat*

- ***Portabilitat: que les dades d'un contractista que estan en els servidors del proveïdor de cloud puguen traslladar-se a un altre proveïdor (o a sistemes locals) a elecció del contractista i sense pèrdua de dades ni de servei.***

- ***No s'ha de confondre amb el dret a la portabilitat de les dades que poden exercir els interessats conformement a l'art. 20 del RGPD.***

COMPLIMENT BASAT EN EL RISC

L'ús de serveis de computació en núvol ofereix un gran nombre d'avantatges però presenta també, per les seues característiques, uns riscos específics que han d'afrontar-se amb una adequada elecció del prestador.

- **Falta de transparència i control.** El client transfereix el control al proveïdor de serveis.
- **Ubicació de les dades.** És necessari acordar amb el proveïdor perquè el processament de les dades estiga subjecte al marc legal del país.
- **Compliment normatiu.** Seguretat i integritat de les dades.
- **Aïllament de dades.** El client transfereix el control al proveïdor de serveis.
- **Portabilitat i viabilitat a llarg termini.** Implicacions en la migració de dades.
- **Accés d'usuaris amb privilegis.** Acordat amb el proveïdor per a usuaris de suport.
- **Recuperació.** Política de recuperació de dades en cas de desastre.
- **Monitoratge.** El monitoratge i vigilància són activitats molt dependents dels mecanismes oferits pel proveïdor de serveis.

Per a identificar els riscos de la forma més senzilla possible s'ha de tindre en compte els aspectes que ja hem analitzat, des del tipus de computació en núvol que es contracta fins al tipus de servei que ens presta el proveïdor.

Tal com s'ha esmentat, en aquest procés de computació en núvol, la informació passa a estar en format virtual accessible des d'una web. Això comporta una sèrie de riscos, que s'han de tindre en compte per a implementar mesures de seguretat que garanteix la seguretat de la informació.

En les administracions públiques es tracten infinitat de dades personals pel que resulta d'aplicació el **REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades** i pel qual es deroga la Directiva 95/46/CE (d'ara en avant, "RGPD").

L'article 32 del RGPD estableix que tenint en compte l'estat de la tècnica, els costos d'aplicació, i la naturalesa, l'abast, el context i els fins del tractament, així com riscos

- ***El client que contracta serveis de cloud computing continua sent responsable del tractament de les dades personals. Encara que els contracte amb una gran companyia multinacional la responsabilitat no es desplaça al prestador del servei, ni tan sols incorporant una clàusula en el contracte amb aquesta finalitat.***

- ***I que ofereix la contractació de cloud computing és un prestador de serveis que en la llei de protecció de dades té la qualificació d''encarregat del tractament'.***

de probabilitat i gravetat variables per als drets i llibertats de les persones físiques, el responsable i l'encarregat del tractament aplicaran mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc.

El problema que tots coneixem és que malgrat exigir que s'implementen mesures de seguretat no existeix un catàleg de mesures a implementar per a complir amb el RGPD.

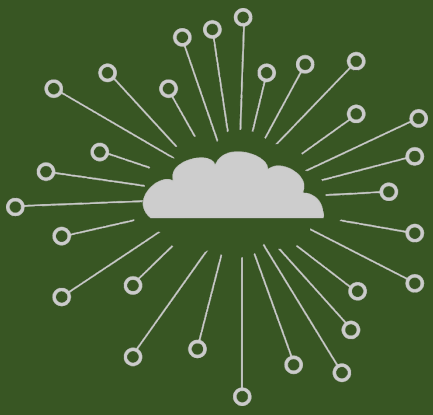
Per a resoldre aquest assumpte, l'habitual és acudir a la **Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals** (d'ara en avant, "LOPDGDD"), en concret, a la disposició addicional primera sobre mesures de seguretat en l'àmbit del sector públic, on es determina que les administracions públiques han d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguen de les previstes en l'Esquema Nacional de Seguretat, així com impulsar un grau d'implementació de mesures equivalents en les empreses o fundacions vinculades als mateixos subjectes al Dret privat.

En els casos en els quals el tercer preste un servei en règim de concessió, encàrrec de gestió o contracte, com pot ser la computació en núvol, les mesures de seguretat es correspondran amb les de l'Administració pública d'origen i s'ajustaran a l'Esquema Nacional de Seguretat.

A l'hora de contractar un servei de computació en el núvol s'han de tindre en compte els riscos per a drets i llibertats dels titulars de les dades personals. En administracions públiques recobra major importància el següent:

1. Establir mesures per a complir amb el Capítol V del RGPD sobre les transferències internacional de dades.
2. Signar contracte d'encarregat amb el proveïdor per a garantir que s'implementen les mesures de seguretat necessàries.
3. Facilitar informació al ciutadà sobre on s'emmagatzemen les seues dades i la cessió a terceres parts.
4. Realitzar anàlisi de riscos tenint en compte les amenaces a la qual les dades s'exposen per tindre'ls allotjats en el núvol.

"Per al cas que ens ocupa ens centrarem en les mesures del Marc Operacional, en concret la nova incorporada al catàleg sobre serveis en el núvol (op.nub)."



ESQUEMA NACIONAL DE SEGURETAT

El mes de maig passat va entrar en vigor el **Reial decret 311/2022**, de 3 de maig, pel qual es regula el nou Esquema Nacional de Seguretat (d'ara en avant, "ENS") i que substitueix a l'anterior Reial decret 3/2010, de 8 de gener, pel qual es regula l'ENS en l'àmbit de l'Administració Electrònica.

Entre les **novetats** que porta amb si aquesta nova versió de l'ENS, cal destacar el següent:

- **Incorporació de la figura del perfil de compliment**: l'objectiu és aconseguir una adaptació a l'ENS més eficaç i eficient, racionalitzant recursos requerits sense menyscapte de la protecció perseguida i exigible.
  Es tracta d'enumerar un conjunt de mesures de seguretat, compreses o no l'en Annex II de l'ENS que, a conseqüència de la preceptiva anàlisi de riscos, resulten d'aplicació a una entitat o sector d'activitat concreta i per a una determinada categoria de seguretat.
  Es persegueix introduir la capacitat d'ajustar els requisits de l'ENS a necessitats específiques, entre altres, a determinats àmbits tecnològics com el servei en núvol.

- **Nou sistema de codificació dels requisits de les mesures de seguretat**: l'objectiu és facilitar de manera proporcionada la seguretat dels sistemes d'informació, la seua implantació i la seua auditoria.
  S'han codificat els requisits de mesures i s'han organitzat de la següent forma:
  1. Requisits base.
  2. Possibles reforços de Seguretat (R) alineats amb el nivell de seguretat perseguit, que se sumen als requisits base de la mesura, però que no sempre són incrementals entre si; de manera que en uns certs casos, es pot triar entre aplica un reforç o un altre.

Decàleg de recomanacions per a la utilització de serveis en el núvol:

1. Determinar la categoria del sistema (BÀSICA, MITJANA o ALTA) que suportarà la solució en el núvol, segons l'ANNEX I del nou ENS.
2. Elaborar la declaració d'aplicabilitat, segons l'ANNEX II del nou ENS.
3. Realitzar una anàlisi de riscos, per a identificar requisits addicionals de seguretat, que es reflectiran en la declaració d'aplicabilitat.
4. Acollir-se a un Perfil de Compliment Específic (en cas que siga aplicable).
5. Establir les condicions contractuals, amb caràcter previ a la contractació, en els plecs i/o peticions d'oferta.
6. En les condicions contractuals, a més de les relatives al compliment de requisits legals, detallar aspectes relatius al servei, la seua infraestructura, el dimensionament, els registres d'activitat, la gestió d'incidents, còpies de seguretat, etc. i establir condicions relatives a la finalització del servei.
7. Supervisar el compliment, per part del CSP, dels requisits legals establits en les condicions de contractació.
8. Realitzar un seguiment periòdic del compliment dels Acords de Nivell de Servei (SLA), establits amb el CSP.
9. Planificar revisions periòdiques de la informació, que el CSP proporciona a través de diversos mecanismes, com per exemple els registres d'activitat, la capacitat, l'emmagatzematge, etc.
10. Elabora una normativa de seguretat específica per als usuaris del núvol.

MESURA DE SEGURETAT

Per al cas que ens ocupa ens centrarem en les mesures del Marc Operacional, en concret la de serveis en el núvol (op.nub):

Requisits:

- **[op.nub.1.1]** Els sistemes que subministren un servei en el núvol a organismes del sector públic hauran de complir amb el conjunt de mesures de seguretat en funció del model de servei en el núvol que presten: SaaS, PaaS i IaaS.
- **[op.nub.1.2]** Quan s'utilitzen serveis en el núvol subministrats per tercers, els sistemes d'informació que els suporten hauran de ser conformes amb l'ENS o complir amb les mesures desenvolupades en una guia CCN-STIC que inclourà, entre altres, requisits relatius a:

1. Auditoria de proves de penetració (pentesting).
2. Transparència.
3. Xifratge i gestió de claus.
4. Jurisdicció de les dades.

Reforç R1 - Serveis certificats

- **[op.nub.1.r1.1]** Quan s'utilitzen serveis en el núvol subministrats per tercers, aquests hauran d'estar certificats sota una metodologia de certificació reconeguda per l'Organisme de Certificació de l'Esquema Nacional d'Avaluació i Certificació de Seguretat de les Tecnologies de la Informació.[op.nub.1.r1.2] Si el servei en el núvol és un servei de seguretat haurà de complir amb els requisits establits en [op.pl.5].

Reforç R2 - Guies de Configuració de Seguretat Específiques.

- **[op.nub.1.r2.1]** La configuració de seguretat dels sistemes que proporcionen aquests serveis haurà de realitzar-se segons la corresponent guia CCN-STIC de Configuració de Seguretat Específica, orientades tant a l'usuari com al proveïdor.

MATERIAL COMPLEMENTARI

- Esquema Nacional de Seguretat. Consulta aquest enllaç.
- Guia cloud clients AEPD. Consulta aquest enllaç.
- Guia de seguretat Cloud CCN. Consulta aquest enllaç.

  Guia orientacions per a prestadors de serveis de Cloud Computing. Consulta aquest enllaç.

NOTÍCIES

- **L'AEPD imposa sanció de prevenció per infracció de l'article 32 RGPD "seguretat del tractament".** El reclamant exposa que es va imposar sense consentiment l'ús d'uns comptes personals de correu electrònic, allotjat en la plataforma GOOGLE SUITE. En la pàgina 19 s'aclareix que El Cloud "*és un disc dur virtual on guardar i compartir carpetes i arxius que permet l'edició ofimàtica de manera col·laborativa*". De la informació traslladada, l'AEPD considera que la reclamada ha infringit l'article 32 RGPD, relatiu a la seguretat del tractament. Consulta la Resolució en aquest enllaç.

- **L'AEPD imposa sanció de prevenció per infracció de diversos articles del RGPD i de la LOPDGDD.** L'AEPD, després de les notícies que van aparéixer en els mitjans de comunicació sobre la implantació d'una app de rastreig de possibles infectats de COVID-19. En la resolució queda patent que les dades del sistema RADAR COVID eren emmagatzemats en els servidors d'AWS situats en la zona geogràfica d'Irlanda. Aporten el document "Arquitectura AWS Cloud: Definició de Serveis". No obstant això, l'AEPD considera – entre altres infraccions descrites en el document – la infracció de l'article 28 RGPD, per entendre que no estava degudament articulada la relació entre responsable i encarregat del tractament. Consulta la Resolució en aquest enllaç.