DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

QUADERNS DivalData

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

Quadern nº 33 | Març 2023

GESTIÓ DE PROVEÏDORS EN EL SECTOR PÚBLIC: DEURE DE DILIGÈNCIA IN VIGILANT

Í N D E X

GESTIÓ DE PROVEÏDORS EN EL SECTOR PÚBLIC: DEURE DE DILIGÈNCIA IN VIGILANT

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

Dpto. de Protecció de Dades i 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

INTRODUCCIÓ

L'art. 24. 1. Reglament (UE) 2016/679 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (d'ara en avant, RGPD) exigeix que el responsable aplique mesures tècniques i organitzatives apropiades i que les revise i actualitze quan siga necessari, al seu torn en l'art. 28.1 li indica al responsable que triarà un proveïdor/encarregat que puga aplicar mesures tècniques i organitzatives suficients.

El Considerant 81 RGPD resulta summament esclaridor en assenyalar que el responsable (…) ha de recórrer únicament a encarregats que oferisquen suficients garanties, en particular pel que fa a coneixements especialitzats, fiabilitat i recursos, de cara a l'aplicació de mesures tècniques i organitzatives que complisquen els requisits del present Reglament, inclosa la seguretat del tractament (…).

Per això, la Diputació de València, d'acord amb el que es preveu en l'art. 28 RGPD, serà responsable que el seu proveïdor/encarregat del tractament (en els tractaments que per compte del responsable realitze) complisca amb el RGPD. En aquest sentit, Les "Directrius per a l'elaboració de contractes entre responsables i encarregats de tractament" elaborades per l'Agència Espanyola de Protecció de Dades (d'ara en avant AEPD) l'Agència Basca de Proteccion de Dades (d'ara en avant, AVPD) i l'Agència Catalana de Proteccion de Dades (d'ara en avant APDCAT) assenyalen que, el RGPD estableix una obligació de diligència deguda en l'elecció dels encarregats de tractament que han d'aplicar tots els responsables, contractant únicament encarregats que estiguen en condicions complir amb el RGPD. I això, implica la necessitat de valorar si els encarregats amb els quals s'hagen contractat o es vagen a contractar operacions de tractament, ofereixen garanties de compliment del RGPD.

"RGPD estableix una obligació de diligència deguda en l'elecció dels encarregats de tractament que han d'aplicar tots els responsables, contractant únicament encarregats que estiguen en condicions complir amb el RGPD"

DILIGÈNCIA EN LA SELECCIÓ DE PROVEÏDORS

L'actuació diligent a l'hora de triar proveïdor/encarregat de tractament, no ha de ser només tasca de la Diputació, sinó per extensió dels seus propis encarregats o subencargados; han de demostrar i acreditar que efectivament compleixen amb la normativa aplicable.

En aquest sentit, a fi de poder demostrar compliment, el propi RGPD ens dona algunes pautes o indicacions, del que en determinats àmbits resulta obligatori tant per a responsables com per a encarregats, a saber:

a) Adopció i implantació de determinades mesures com: seudonimización, minimització/reducció de tractaments, transparència, supervisió de tractaments, promoció de desenvolupament i fabricació de productes amb una privacitat per defecte, etc. (C. 78 RGPD).

b) Revisió i actualització de mesures o controls que garantisquen la seguretat del tractament (C.81 i art. 24.1 RGPD), prèviament determinats i/o exigit al proveïdor

c)) Comptar amb un Registre d'activitats de tractament (C. 82)

d) Adoptar les garanties adequades en els casos d'estar davant una transferència internacional de dades (decisió de la comissió, clàusules contractuals tipus, etc. (C.108)

Sense ànim d'exhaustivitat, l'incompliment de l'obligació de diligència deguda i, per tant, l'absència de control en matèria de privacitat en l'elecció d'un proveïdor podria donar lloc a diferents tipus de responsabilitat.

Els responsables assumeixen el nivell més alt nivell de responsabilitat: han de complir i demostrar el compliment del RGPD i també són responsables del compliment del seu proveïdor/encarregat. D'acord amb l'art. 4.7) RGPD el responsable és "la persona física o jurídica, autoritat pública, servei o un altre

"A fi de poder demostrar compliment, el propi RGPD ens dona algunes pautes o indicacions, del que en determinats àmbits resulta obligatori tant per a responsables com per a encarregats, a saber:

a) Adopció i implantació de determinades mesures com: seudonimización, minimització/reducció de tractaments, transparència, supervisió de tractaments, promoció de desenvolupament i fabricació de productes amb una privacitat per defecte, etc. (C. 78 RGPD)."

organisme que, només o juntament amb uns altres, determine els fins i mitjans del tractament.

ANÀLISI DE LES DISPOSICIONS

Com esmentàvem anteriorment del considerant 81 del Reglament, es desprenen dues qüestions a tindre en consideració; d'una banda, que els responsables del tractament han de ser diligents a l'hora de triar als seus encarregats i; per un altre, que els encarregats del tractament, amb caràcter previ a la seua contractació, han d'oferir als responsables les garanties que resulten adequades al nivell de risc identificat, facilitant les evidències que permeten acreditar el compliment d'aquestes.

Quant a l'anterior, el considerant del Reglament, estableix que l'adhesió de l'encarregat a un codi de conducta o a un mecanisme de certificació aprovats per les autoritats de control competents pot servir d'element per a demostrar el compliment de les obligacions per part del responsable.

"l'adhesió de l'encarregat a un codi de conducta o a un mecanisme de certificació aprovats per les autoritats de control competents pot servir d'element per a demostrar el compliment de les obligacions per part del responsable".

En l'actualitat, ni les autoritats de control competents ni el Comité Europeu de Protecció de Dades, han desenvolupat els esquemes de certificació o aprovats suficients codis de conducta, perquè les garanties enunciades puguen ser aplicades o tingudes en consideració pels responsables a l'hora de seleccionar als seus encarregats.

Entre els mecanismes que els responsables poden implementar en les seues organitzacions o els responsables podran optar, bé per desenvolupar i implementar polítiques i processos interns que els permeten dur a terme l'avaluació i selecció de proveïdors de manera objectiva i evidenciable, o bé, contractar els serveis d'un tercer de confiança que haja desenvolupat uns criteris d'avaluació propis.

Quant a la primera opció, és necessari que les polítiques i procediments interns siguen conegudes per totes les persones que participen en el procés de selecció, incloses les unitats contractants, sent imprescindible la formació i conscienciació contínua d'aquestes persones sobre la matèria.

En aquest sentit, resulta recomanable que els criteris establits pel responsable per a la selecció d'encarregats del tractament, per exemple, en el moment de publicar una licitació, siguen coneguts amb caràcter previ per aquests, de cara al fet que els tinguen en compte a l'hora de realitzar les seues ofertes als responsables o participar en les licitacions publicades per aquells.

QUÈ HEM DE TINDRE EN COMPTE?

El procés d'homologació de les garanties d'aquests proveïdors, haurà de ser transversal a totes les unitats implicades en la selecció de proveïdors, però a més ha de tindre la capacitat o entitat suficient per a determinar si finalment procedeix o no, iniciar la contractació d'aquest.

"És important conéixer l'escenari davant el qual ens trobem de cara a la identificació i classificació de futurs proveïdors, de manera que això ens ajude a dur a terme una posterior avaluació exhaustiva i eficient".

És important conéixer l'escenari davant el qual ens trobem de cara a la identificació i classificació de futurs proveïdors, de manera que això ens ajude a dur a terme una posterior avaluació exhaustiva i eficient.

Els següents passos, a tindre en compte cronològicament, ens ajudaren a obtindre el resultat desitjat:

1. Identificació de tots els proveïdors que vagen a tractar dades personals per compte de la nostra organització:

2. Anàlisi respecte a la tipologia de les dades que seran tractats.

3. Anàlisi de la situació contractual.

4. Preparació de l'avaluació i requisits de compliment normatiu.

El procés d'homologació ha d'incloure l'avaluació de l'organització i governança de la privacitat del proveïdor, verificant i revisant l'existència de criteris relatius a protecció de dades i altres aspectes del govern i compliment de la normativa com, per exemple:

- La possible adhesió a codis de conducta.
- La possessió d'un certificat de protecció de dades.
- En el seu cas, el nomenament de DPO i el seu registre davant l'autoritat de control competent.
- La realització o no de Transferències Internacionals de Dades, i en tal case l'existència de garanties adequades per a dur-la a terme d'acord amb la regulació.
- La gestió d'un Registre d'Activitats de Tractament.
- La implementació de polítiques internes relatives al tractament de dades personals (exercicis de drets, comunicació d'incidents de seguretat, gestió de personal etc.).
- L'existència de possibles subcontractacions (subencarregats del tractament i els corresponents acords de protecció de dades amb tercers).
- L'existència d'antigues sancions a l'encarregat del tractament en matèria de protecció de dades.
- L'existència de sentències condemnatòries i/o procediments judicials oberts en matèria de protecció de dades respecte de l'encarregat del tractament.

"El procés d'homologació ha d'incloure l'avaluació de l'organització i governança de la privacitat del proveïdor, verificant i revisant l'existència de criteris relatius a protecció de dades i altres aspectes del govern i compliment de la normativa".

CONSIDERACION DEL ENS

D'altra banda, cal tindre en consideració que aquesta obligació de diligència deguda també és exigida, més enllà de la normativa general RGPD i estàndards d'aplicació, per a la Diputació, ha de complir amb l'aplicació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica (d'ara en avant, ENS).

Veiem per tant, que quant a la gestió de terceres parts en relacions mercantils de prestació de serveis que implique accés a dades personals o a informació confidencial en general d'una organització, la relació Responsable de la Informació proveïdor de serveis està inclosa en molts estàndards i legislació que obliga a un control diligent per part del Responsable i que inclou una sèrie d'obligacions de control i diligència en les diferents fases de la relació: pre, contractual i postcontractual, més enllà del RGPD. En el cas de l'ENS s'inclou entre els seus requisits mínims l'obligació de l'AAPP de verificar que tot producte que adquirisca o contracte complisca amb tots els requisits de l'ENS, havent de valorar-se positivament les certificacions quant a seguretat que aportació.

A més, les mesures de seguretat obligatòries per a tota la informació tractada un apartat de Serveis Externs.

Atés que qualsevol proveïdor de les AAPP espanyoles està obligat a complir amb l'ENS, incloure entre les obligacions internes a complir les de diligència i gestió de terceres parts, seguint les directrius de l'ENS, pot simplificar processos interns i donar llum a tasques i mesures a implantar en el procés de diligència en la gestió de tercers.

Asi, s'exposa en l'Annex II, Mesures de Seguretat de l'ENS, més concretament en les mesures del marc operacional referents als Serveis Externs, “Gestion Diària” on s'estableix que per a la gestió diària del sistema, s'establiran els següents punts;

– Un sistema rutinari per a mesurar el compliment de les obligacions de servei, incloent-hi el procediment per a neutralitzar qualsevol desviació fora del marge de tolerància acordada

– El mecanisme i els procediments de coordinació per a dur a terme les tasques de manteniment dels sistemes

“Atés que qualsevol proveïdor de les AAPP espanyoles està obligat a complir amb l'ENS, incloure entre les obligacions internes a complir les de diligència i gestió de terceres parts, seguint les directrius de l'ENS, pot simplificar processos interns i donar llum a tasques i mesures a implantar en el procés de diligència en la gestió de tercers”.

compresos en l'acord, que contemplaran els supòsits d'incidents i desastres

Tindre en compte que aquests últims punts seran aplicable sempre que estiguem davant sistemes de categoria MITJANA, tal com disposa la norma.

.

"Com a justificació a l'exclusió del consentiment com a base de licitud, al·ludeix a la posició de desequilibri entre el ciutadà com a interessat i l'Administració com a Responsable del tractament, la qual cosa fa que no es puga comptar amb un consentiment vàlid al no basar-se en una "manifestació de voluntat lliure".

MATERIAL COMPLEMENTARI

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, («RGPD») relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades. Consulta aquest enllaç.
- Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica. Consulta aquest enllaç.
- Guia "Directrius per a l'elaboració de contractes entre responsables i encarregats del tractament". Consulta aquest enllaç.

  Guia de Computing Cloud per a entitats que contracten serveis. Consulta aquest enllaç.

NOTÍCIES

- **La Comissió Europea prohibeix al seu personal usar TikTok "per a protegir les seues dades i augmentar la seua ciberseguretat"**

  El Parlament Europeu ha acabat per sumar-se a les altres dues grans institucions europees i ha vetat l'ús de TikTok en els seus dispositius a eurodiputats i empleats. La Comissió Europea i el Consell de la UE van adoptar aquesta decisió la setmana passada per als seus funcionaris i cinc dies després els ha seguit l'Eurocambra. L'aplicació xinesa s'ha convertit en els últims temps en font de sospites a Occident per "la protecció de dades i la recollida de dades per a terceres parts", segons pot llegir-se en el missatge que han rebut els parlamentaris.

  A la llista de Governs que veten l'ús d'aquest programa informàtic en els dispositius electrònics utilitzats pels seus empleats es va sumar aquest dilluns Canadà: "La decisió d'eliminar i bloquejar TikTok dels dispositius mòbils de les administracions públiques s'adopta per precaució, en particular per la inquietud que suscita el règim jurídic que regeix la informació recopilada dels dispositius, i està d'acord amb el plantejament dels nostres socis internacionals. En un dispositiu mòbil, els mètodes de recopilació de dades de TikTok proporcionen un accés considerable al contingut del telèfon", apunta el comunicat amb el qual es va donar a conéixer la decisió.". Consulta la notícia en aquest enllaç.