DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de Protecció de Dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí Núm. 4| Octubre 2020

LES DEU INFRACCIONS MÉS HABITUALS EN PROTECCIÓ DE DADES EN LES ENTITATS LOCALS

DIPUTACIÓ DE VALÈNCIA
Protecció de Dades i Seguretat de la Informació

Í N D E X

LES DEU INFRACCIONS MÉS HABITUALS EN PROTECCIÓ DE DADES EN LES ENTITATS LOCALS

	Pàgina
INFRACCIONS CONSIDERADES MOLT GREUS	2
INFRACCIONS CONSIDERADES GREUS	3
INFRACCIONS CONSIDERADES LLEUS	3
EXERCICI DE DRETS	4
VIDEOVIGILÀNCIA	5
DEURE D'INFORMACIÓ	5
OBTENCIÓ DEL CONSENTIMENT	6
PUBLICACIÓ DE LES ACTES DE LA JUNTA DEL GOVERN LOCAL	6
PUBLICACIÓ DE DADES PERSONALS EN PROCESSOS SELECTIUS	7
CORREUS ELECTRÒNICS SENSE CÒPIA OCULTA	7
PUBLICACIÓ DE RESOLUCIONS JUDICIALS	8
SEGURETAT DEL TRACTAMENT I NOTIFICACIÓ DE VIOLACIONS DE SEGURETAT	8
NOMENAMENT DEL DELEGAT DE PROTECCIÓ DE DADES	9
MATERIAL COMPLEMENTARI	10
NOTÍCIES D'ACTUALITAT	10

Vos invitem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Estes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

Correu electrònic: dpdssi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedix al següent enllaç

LES DEU INFRACCIONS MÉS HABITUALS EN PROTECCIÓ DE DADES EN LES ENTITATS LOCALS

Una de les novetats que va portar amb si el 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 i pel qual es deroga la Directiva 95/46/CE (RGPD) va ser l'enduriment del règim sancionador, que va incrementar notablement la quantia de les sancions per l'incompliment del que es preveu en la normativa de protecció de dades.

La Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD) va desenvolupar el sistema de sancions del RGPD, categoritzant les infraccions en molt greus, greus i lleus. Alguns dels actes sancionables de cadascun dels tres nivells són:

- Vulneració de principis i garanties.
- Tractament de dades sense base de licitud.
- Incompliment dels requisits exigits per a la validesa del consentiment.
- Utilització de dades per a finalitats incompatibles amb la de recollida.
- Tractament de categories especials de dades sense que concórrega una de les circumstàncies previstes.
- Tractament de dades relatives a condemnes i infraccions penals o mesures de seguretat connexes, o infraccions i sancions administratives fora dels supòsits permesos.
- L'omissió del deure d'informar l'afectat sobre el tractament de les seues dades.
- La vulneració del deure de confidencialitat.
- L'impediment o l'obstaculització o la no atenció reiterada de l'exercici de drets.
- La transferència internacional de dades sense concórrer garanties, requisits o excepcions.
- L'incompliment de l'obligació de bloqueig de les dades.

INFRACCIONS CONSIDERADES GREUES

- El tractament de dades personals d'un **menor d'edat sense recaptar el seu consentiment**, quan tinga capacitat per a això, o el del titular de la seua pàtria potestat o tutela.
- La falta d'adopció d'aquelles mesures tècniques i organitzatives que resulten apropiades per a aplicar de manera efectiva els principis **de protecció de dades des del disseny**.
- La falta d'adopció de les mesures tècniques i organitzatives apropiades per a garantir que, **per defecte**, només es tractaran les **dades personals necessàries** per a cadascun de les finalitats específiques del tractament.
- La falta d'adopció d'aquelles mesures tècniques i organitzatives que resulten apropiades per a garantir **un nivell de seguretat adequat al risc** del tractament.
- La contractació pel responsable del tractament **d'un encarregat de tractament que no oferisca les garanties suficients**.
- Encarregar el **tractament de dades a un tercer sense la prèvia formalització d'un contracte** o un altre acte jurídic en els termes del RGPD.
- No disposar del **registre d'activitats de tractament.**
- L'incompliment de **l'obligació de designar un delegat de protecció de dades** quan siga exigible el seu nomenament.

INFRACCIONS CONSIDERADES LLEUS

- L'incompliment del **principi de transparència** de la informació o el dret d'informació de l'afectat per **no facilitar tota la informació exigida**.
- **No atendre les sol·licituds d'exercici dels drets**.
- Disposar d'un **registre d'activitats de tractament que no incorpore tota la informació exigida**.
- La **notificació incompleta, tardana o defectuosa a l'autoritat** de protecció de dades de la informació relacionada amb una **violació de seguretat** de les dades personals.
- L'incompliment de l'obligació de **documentar qualsevol violació de seguretat**.
- L'incompliment del **deure de comunicació a l'afectat d'una violació de la seguretat** de les dades que comporte un alt risc per als drets i llibertats dels afectats.
- **No publicar les dades de contacte del delegat de protecció de dades, o no comunicar-los a l'autoritat de protecció de dades.**

En l'àmbit de l'Administració Pública, el RGPD permet als Estats establir les seues pròpies normes per a regular el règim sancionador d'aquestes. En el cas d'Espanya, la LOPDGDD contempla per a aquestes la sanció de prevenció, acompanyada de les mesures que procedisca adoptar perquè cesse la conducta o es corregisquen els efectes de la infracció. Així mateix, ha de tindre's en compte el mal reputacional que la sanció causaria a l'entitat.

"EL RÈGIM SANCIONADOR APLICABLE A les ADMINISTRACIONS PÚBLIQUES CONTEMPLA PER A AQUESTES LA SANCIÓ DE PREVENCIÓ, QUE ANIRÀ ACOMPANYADA DE LES MESURES QUE PROCEDISCA ADOPTAR PERQUÈ CESSAMENT LA CONDUCTA O ES CORREGISQUEN ELS EFECTES DE LA INFRACCIÓ. AIXÍ MATEIX, HA DE TINDRE'S EN COMPTE EL MAL REPUTACIONAL QUE LA SANCIÓ CAUSARIA A L'ENTITAT"

A continuació, farem un repàs a les infraccions més habituals en protecció de dades en les Entitats Locals:

EXERCICI DE DRETS

El dret fonamental a la protecció de dades reconeix als interessats la facultat de controlar les seues dades personals i la capacitat per a disposar i decidir sobre els mateixos. Entre els drets que la Llei atorga als interessats en relació amb les seues dades personals estan els drets d'accés, rectificació, supressió, oposició, dret a la limitació del tractament, portabilitat de les dades i a no ser objecte de decisions basades únicament en el tractament automatitzat de les seues dades.

Les sol·licituds han de ser sempre ateses sense demora i en el termini màxim d'un mes. Si el Responsable del Tractament no dona curs a la sol·licitud de l'interessat, l'ha d'informar sense demora injustificada, i a tot tardar al mes de la recepció de la sol·licitud, de les raons per les quals no ha actuat, així com de la possibilitat de presentar una reclamació davant una autoritat de control i recórrer als tribunals.

Aquest constitueix un dels aspectes més importants de la legislació relativa a la protecció de dades de caràcter personal, atès que un mal coneixement o mala gestió del procediment d'exercici de drets sol ser l'avantsala d'un procediment sancionador.

De fet, la indeguda atenció a les sol·licituds dels ciutadans en l'exercici dels drets que estableix el RGPD és, en la pràctica, una de les infraccions més habituals en l'àmbit de les Entitats Locals. Especialment, destaca la indeguda atenció dels drets d'accés i supressió, seguits pel dret d'oposició i el de rectificació.

En la Resolució núm. R/00171/2020, l'Agència Espanyola de Protecció de Dades (AEPD) va sancionar a una Entitat Local per no haver sigut degudament atès un dret de supressió. En concret, el reclamant va sol·licitar l'eliminació de les seues dades personals d'en enllaç de la web municipal. Si bé l'Entitat Local reclamada va mostrar la seua voluntat d'atendre el dret, no el va fer efectiu.

En la Resolució núm. R/00180/2020 de l'AEPD, per part seua, l'Entitat Local va ser sancionada per no donar la resposta legalment exigible a la sol·licitud de supressió exercida pel reclamant.

VIDEOVIGILÀNCIA

La imatge d'una persona, en la mesura que identifique o puga identificar a aquesta, constitueix una dada de caràcter personal que pot ser objecte de tractament per a diverses finalitats, sent comuna la de garantir la seguretat de persones, béns i instal·lacions municipals.

Aquests tractaments de dades hauran de complir amb el que es disposa en l'art. 22 LOPDGDD, que disposa entre altres coses, que els tractaments de dades personals amb finalitats de vigilància a través de sistemes de càmeres o càmeres de vídeo, el deure d'informació pot complir-se mitjançant la col·locació, en les zones videovigilades, d'un distintiu informatiu situat en lloc prou visible, tant en espais oberts com tancats, i servint-se d'impresos en els quals es detalle la informació prevista, que el responsable haurà de posar a la disposició dels interessats.

D'altra banda, només podran captar-se imatges de la via pública en la mesura en què resulte imprescindible per a preservar la seguretat de les persones i béns, així com de les seues instal·lacions.

Són nombroses les sancions que imposa l'AEPD per no complir amb les previsions de l'art. 22 LOPDGDD.

En el Procediment Núm.: PS/00384/2019, si bé les imatges de les cambres que instal·la l'Entitat Local es limiten a la zona d'accés a les instal·lacions, considerant-se les mateixes proporcionades amb la finalitat de control d'accés a unes instal·lacions esportives, se sanciona a l'entitat perquè el sistema no disposava inicialment de cartell informatiu, ni de formulari informatiu adaptat a la normativa en vigor.

DEBER D'INFORMACIÓ

L'art. 13, apartats 1 i 2, del RGPD, estableix la informació que ha de facilitar-se a l'interessat en el moment de la recollida de les seues dades: identitat i dades de contacte del responsable, dades de contacte del Delegat de Protecció de Dades (DPD), finalitats del tractament, base jurídica, destinataris, intenció de realitzar transferències internacionals, termini de conservació, existència de drets, dret a presentar una reclamació davant l'autoritat de control, etc.

No obstant això, les Entitats Locals no sempre la faciliten o ho fan de manera incompleta, la qual cosa constitueix una infracció en matèria de protecció de dades.

En el Procediment núm. PS/00347/2019, se sanciona a una Entitat Local per vulneració de l'art. 13 del RGPD, respecte de la falta d'informació que es va proporcionar als treballadors i funcionaris de l'Ajuntament quan es van obtindre les seues dades personals per a l'elaboració de la relació de llocs de treball (RLPT).

OBTENCIÓ DEL CONSENTIMENT

En relació amb el consentiment per a tractar dades de caràcter personal, el legislador europeu ha concebut aquest com una causa més de licitud o legitimació per a realitzar el tractament de dades. Ara bé, el consentiment ha de complir amb les condicions requerides pel RGPD. Entre aquestes condicions, es troba la de l'art. 7.2 RGPD que estableix que, si el consentiment de l'interessat es dona en el context d'una declaració escrita que també es referisca a altres assumptes, la sol·licitud de consentiment s'ha de presentar de tal forma que es distingisca clarament dels altres assumptes, de manera intel·ligible i de fàcil accés i utilitzant un llenguatge clar i senzill.

No obstant això, davant l'absència d'una altra base en la qual legitimar el tractament de les dades, les Entitats Locals no sempre sol·liciten el consentiment, o obtenen un consentiment que no compleix amb les condicions exigides pel RGPD.

En la Resolució R/03041/2017, l'AEPD va sancionar a una Entitat Local per crear un grup de WhatsApp en el qual va incorporar 255 números de telèfon de veïns del municipi per a facilitar la comunicació amb aquests, això a pesar que aquests no havien atorgat el seu consentiment per a aquest tractament.

Per part seua, en el Procediment PS/00382/2019, si bé l'Entitat Local reclamada va sol·licitar el consentiment per a la participació en activitats lúdiques organitzades pel municipi per a menors i la publicació d'imatges d'aquests, va ser sancionada per obtindre el consentiment per a totes les activitats en general, havent de recollir-se per a cadascuna d'elles.

PUBLICACIÓ DE LES ACTES DE LA JUNTA DE GOVERN LOCAL

La Llei 7/1985, de 2 d'abril, Reguladora de les Bases de Règim Local estableix en el seu article 70.1 que les sessions del Ple de les Corporacions Locals són públiques, excepte en aquells assumptes que puguen afectar el dret fonamental dels ciutadans a què es refereix l'article 18.1 de la Constitució, quan així s'acorde per majoria absoluta i també, que les sessions de la Junta de Govern Local no són públiques. D'altra banda, l'apartat 2 del referit article 70 estableix que els acords que adopten les corporacions locals es publicaran o notificaran en la forma prevista per llei.

L'article 88.1 del RD 2568/1986, de 28 de novembre, del Reglament d'Organització, Funcionament i Règim Jurídic de les Entitats Locals, estableix el caràcter públic de les sessions del Ple, amb la possibilitat de celebrar a porta tancada el debat i votació d'aquells assumptes que puguen afectar el dret fonamental dels ciutadans a què es refereix l'article 18 de la Constitució, quan així s'acorde per majoria absoluta. Al seu torn, l'article 229 del RD 2568/1986 estableix que les Corporacions donaran publicitat resumida del contingut de les sessions plenàries i de tots els acords del Ple i de les Comissions de Govern, així com de les resolucions de l'Alcalde.

La conclusió és que les Entitats Locals poden publicar de forma resumida el contingut de les sessions i acords del Ple i les Comissions, però sense incloure més dades dels que siguen adequats, pertinents i no excessius en relació amb la finalitat pretesa, la qual cosa no sempre compleixen les Entitats Locals, publicant el contingut íntegre de les Actes de la Junta de Govern Local.

En la Resolució R/00387/2018, l'AEPD va sancionar a una Entitat Local per publicar en la seua pàgina web el contingut íntegre de l'Acta de la Sessió Ordinària celebrada per la Junta de Govern Local, en la qual es feia referència a una sol·licitud de devolució d'una donació realitzada per la reclamant, la qual cosa suposa una indeguda divulgació de les seues dades de caràcter personal.

PUBLICACIÓ DE DADES PERSONALS EN PROCESSOS SELECTIUS

En els procediments selectius, el principi de publicitat i transparència es torna en essencial, com a garantidor del principi d'igualtat, encara que per a assegurar el compliment del principi de publicitat la Llei no especifica cap mitjà concret, podent existir casos en els quals la forma de publicació per la qual s'ha optat puga considerar-se excessiva. La proporcionalitat i adequació del tractament han d'estar conformes amb el principi de transparència per als participants en el procés, i no resulta necessari per a això exposar les dades en obert per a qualsevol persona no participant en el procés. Una manera satisfactòria de complir l'objectiu seria preveure un sistema en el qual tots els participants puguen accedir a la informació, ja que es tracta de concurrència competitiva, però aquesta informació no ha de ser accessible a tercers no participants en el procés, afectant la transparència exclusivament als admesos o exclosos. Per tant, ni el torn pel qual es presenten els candidats ni el nom i cognoms en el lloc al qual opten és necessari que siga accessible per persones que no participen en el procés.

No obstant això, no en poques ocasions ens trobem que les Entitats Locals fan públiques, en obert, en les seues pàgines webs o fins i tot en les seues Xarxes Socials, les llistes d'admesos i exclosos en procediments de concurrència competitiva, la qual cosa comporta la imposició de sancions per part de les autoritats de control.

En el Procediment núm. AP/00046/2018, l'AEPD va sancionar a una Entitat Local per publicar en la seua pàgina web i en les seues xarxes socials la llista del personal seleccionat en el marc d'un Pla de Cooperació Local, inclosos el nom i cognoms dels aspirants lligats a la seua condició de discapacitat.

CORREUS ELECTRÒNICS SENSE CÒPIA OCULTA

L'enviament de correus electrònics ha d'atendre també les obligacions recollides en la normativa vigent de protecció de dades, en particular quant a preservar la confidencialitat i dades personals concernents als destinataris dels missatges. Referent a això, es considera precís el recurs a una modalitat d'enviament que ofereixen els programes de correu electrònic disponibles en el mercat, la qual permet detallar les adreces electròniques dels destinataris múltiples en un camp específic de l'encapçalat del missatge: el camp CCO (amb còpia oculta), en lloc de l'habitual CC.

En la Resolució R/01625/2018, l'AEPD va sancionar a una Entitat Local per remetre a 12 destinataris el llistat final del curs de "Operacions auxiliars de muntatge de xarxes elèctriques", amb les adreces de correu electrònic de tots els destinataris visibles per a tots ells.

PUBLICACIÓ DE RESOLUCIONS JUDICIALS

El principi de publicitat de les actuacions judicials es troba consagrat, quant a les sentències, pels articles 205.6, 232, 235, 235 bis, 235 ter i 266 de la Llei orgànica del Poder Judicial. La publicitat a la qual es refereixen aquests preceptes té per objecte assegurar el ple desenvolupament del dret de les parts a obtindre la tutela efectiva dels jutges i Tribunals en l'exercici dels seus drets, sense que en cap manera puga produir-se'ls indefensió, consagrat per l'article 24.1 de la Constitució. La col·lisió entre la publicitat de les sentències i el dret a la intimitat de les persones ja ha sigut analitzada per l'AEPD, que sobre la base del que es disposa pel Consell General del Poder Judicial, ha entés que en el tractament i difusió de les resolucions judicials s'ha de procurar la supressió de les dades d'identificació per a assegurar en tot moment la protecció de l'honor i intimitat personal i familiar.

És per això que, les resolucions judicials dels procediments en els quals les Entitats Locals siguen part no poden ser difoses íntegrament en Taulons en les dependències de l'entitat, ni en la seua pàgina web.

En la Resolució núm. R/00036/2018 es va sancionar a una Entitat Local per col·locar una nota informativa amb totes les dades de la sentència judicial en la qual es condemnava a un veí en un plet contra l'Ajuntament, en tres taulers d'anuncis del municipi, i en la pàgina de Facebook de la localitat.

SEGURETAT DEL TRACTAMENT I NOTIFICACIÓ DE VIOLACIONS DE SEGURETAT

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 riscos de probabilitat i gravetat variables per als drets i llibertats de les persones físiques, les Entitats Locals han d'aplicar mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat als riscos. A més, en cas de violació de la seguretat de les dades personals, han de notificar a l'autoritat de control competent sense dilació indeguda i, a tot tardar, 72 hores després que haja tingut constància d'ella, llevat que siga improbable que aquesta violació de la seguretat constituïsca un risc per als drets i les llibertats de les persones físiques. Així mateix, quan siga probable que la violació de la seguretat de les dades personals comporte un alt risc per als drets i llibertats de les persones físiques, l'Entitat Local ho haurà de comunicar també a l'interessat sense dilació indeguda.

No obstant això, les Entitats Locals no sempre apliquen les mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc i, en cas d'incident de seguretat, no sempre ho gestionen correctament.

En el Procediment núm. PS/00463/2019, l'AEPD sanciona a una Entitat local per mostrar en la seua Seu Electrònica 23 certificats de diversa índole relacionats amb el padró on apareixen dades personals dels components de la família del reclamant i dels interessats d'altres 22 certificats signats el mateix dia, perquè tots els certificats signats el mateix dia tenien el mateix CSV. A més, tampoc va donar compliment a l'obligació de notificar-ho a l'autoritat de control, així com als possibles afectats per l'incident sense dilacions indegudes una vegada va tindre el coneixement d'això.

NOMENAMENT DEL DELEGAT DE PROTECCIÓ DE DADES

En el marc del RGPD la figura del DPD ha emergit gràcies, principalment, a la seua exigibilitat en diferents suposats; i també gràcies a que és una de les mesures que componen un dels principals principis del RGPD: la responsabilitat activa.

Un dels supòsits d'obligada designació es dona quan el tractament el duga a terme una autoritat o organisme públic, la qual cosa implica que totes les Entitats Locals hagen de designar un DPD.

Si bé no és una de les infraccions més habituals en l'àmbit local, és una conducta que l'AEPD comença a sancionar.

En el Procediment PS/00001/2020, l'AEPD va sancionar a una Entitat Local per mancar de Delegat de Protecció de Dades.

MATERIAL COMPLEMENTARI

- Resolució AEPD Núm.: R/00171/2020 (exercici de drets)
- Resolució AEPD Núm.: R/00180/2020 (exercici de drets)
- Resolució AEPD Procediment Núm.: PS/00384/2019 (videovigilància)
- Resolució AEPD Procediment Núm.: PS/00347/2019 (deure d'informació)
- Resolució AEPD Procediment Núm. AP/00023/2017 (consentiment)
- Resolució AEPD Procediment Núm.: PS/00382/2019 (consentiment)
- Resolució AEPD Núm. R/00387/2018 (Actes Junta de Govern Local)
- Resolució AEPD Procediment Núm. AP/00046/2018 (Procediments selectius)
- Resolució AEPD Procediment Núm. AP/00037/2017 (còpia oculta)
- Resolució AEPD Procediment Núm.: PS/00463/2019 (publicació de resolucions judicials)
- Resolució AEPD Procediment Núm.: PS/00001/2020 (DPD)

NOTÌCIES

- **Es publica el Reial decret llei 28/2020, de 22 de setembre, de treball a distància**. En el seu capítol IV, el Reial decret llei es refereix de manera específica a les facultats d'organització, direcció i control empresarial en el treball a distància, incloent la protecció de dades i seguretat de la informació, el compliment per la persona treballadora de les seues obligacions i deures laborals i les instruccions necessàries per a preservar a l'empresa enfront de possibles bretxes de seguretat. Consulta la norma en aquest enllaç.
- **Es publica la Llei orgànica 1/2020, de 16 de setembre, sobre la utilització de les dades del Registre de Noms de Passatgers per a la prevenció, detecció, investigació i enjudiciament de delictes de terrorisme i delictes greus.** Aquesta inclou una sèrie de disposicions en matèria de protecció de dades, entre les quals figuren l'obligació de conservació de la documentació relativa als sistemes i procediments de tractament; l'obligació de registre de les operacions de recollida, consulta, transferència i supressió de les dades, així com l'obligació de comunicar a l'interessat i a l'autoritat nacional de control qualsevol violació de les dades personals que done lloc a un elevat risc per a la protecció dels mateixos o afecte negativament la intimitat de l'interessat. Consulta la norma en aquest enllaç.
- **L'AEPD publica recomanacions per a minimitzar els riscos per a la privacitat en la navegació per Internet.** La nota repassa algunes de les tècniques més utilitzades per pàgines web i serveis d'internet per a fer seguiment dels llocs web que visiten els usuaris. L'Agència inclou un apartat de recomanacions bàsiques dirigides a usuaris amb un nivell de coneixements mitjà, com la importància de valorar la privacitat com una característica desitjable en triar un navegador i les aplicacions que s'instal·len; evitar la instal·lació d'aplicacions innecessàries en el navegador; activar, en el seu cas, la protecció anti-rastreig o seguiment en el navegador, o configurar-lo per a bloquejar les cookies de tercers, o almenys bloquejar-les si es navega en manera privada, entre altres. Així mateix, recull recomanacions per a usuaris avançats. Consulta la Nota en aquest enllaç.