

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 36 | Juny 2023

**PROTECCIÓ DE DADES DE LES PERSONES INFORMANTS SOBRE
INFRACCIONS NORMATIVES I DE LLUITA CONTRA LA CORRUPCIÓ**



Í N D E X



PROTECCIÓ DE DADES DE LES PERSONES INFORMANTS SOBRE INFRACCIONS NORMATIVES I DE LLUITA CONTRA LA CORRUPCIÓ

	Pàgina
Introducció.	2
Àmbit d'aplicació de la llei de protecció dels informants.	4
Principals característiques del sistema intern d'informació.	6
Obligacions de l'Administració pública, responsable del tractament de les dades personals dels informants.	8
Canal extern d'informació A.A.I.	10
El paper del Delegat de Protecció de Dades.	12
Notícies i material complementari.	14



Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interès 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

[enlace](#)



INTRODUCCIÓ

Amb l'aprovació de la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informen sobre infraccions normatives i de lluita contra la corrupció es transposa, això és, s'incorpora al Dret espanyol la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre de 2019.

La norma europea permet als Estats eximir de la implantació del canal intern als municipis de menys de 10.000 habitants o entitats del sector públic de menys de 50 treballadors. No obstant això, la Llei 2/2023, en enunciar l'àmbit d'aplicació en el seu article 13, ha prescindit d'aquesta opció.

“Amb l'aprovació de la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informen sobre infraccions normatives i de lluita contra la corrupció es transposa, això és, s'incorpora al Dret espanyol la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre de 2019”.



A través del sistema intern d'informació, es podrà informar davant una hipotètica infracció de legislació o normativa, referida, entre altres, a:

- Contractació pública.
- Serveis, productes i mitjans financers i prevenció del blanqueig de capitals i el finançament del terrorisme.
- Seguretat del transport
- Protecció del medi ambient.
- Cadena alimentària, i en particular en la seguretat dels aliments i els pinsos, així com de la sanitat, la protecció i el benestar dels animals.
- Protecció dels usuaris o consumidors.



“La citada directiva regula aspectes mínims que havien d'abastar els diferents llits d'informació a través dels quals una persona coneixedora d'una infracció del dret de la Unió Europea pugua donar a conèixer l'existència de la mateixa en un entorn laboral”.

- Protecció de la intimitat i les dades personals.
- Seguretat de les xarxes i els sistemes d'informació.

En el present quadern, en primer lloc, s'indica quin és l'àmbit personal d'aplicació, així com que entitats del sector públic estan obligades a crear un sistema intern d'informació. A continuació, es mostren els principals requisits o característiques que ha de reunir el sistema d'informació; col·loquialment conegut com a canal de denúncies o *whistleblowing*.

D'altra banda, se citen les principals actuacions, de conformitat amb la legislació en protecció de dades de caràcter personal, que hauran de dur a terme els ens públics, com a responsables del tractament de les dades personals dels informants, així com de la resta de persones involucrades en la comunicació efectuada per aquests.

A més de tals canals interns, exigeix la Directiva la determinació d'altres canals d'informació, denominats «externs», amb la finalitat d'oferir als ciutadans una comunicació amb una autoritat pública especialitzada, la qual cosa els pot generar més confiança en dissipar el seu temor a patir alguna represàlia en el seu entorn.

Finalment, s'indica el paper del Delegat de Protecció de Dades en relació amb els tractaments de dades personals dutes a terme a través del Sistema intern d'informació o canal de denúncies intern.



“La Llei protegeix les persones físiques informants, que treballen en el sector públic i que hagen obtingut informació sobre infraccions en un context laboral”.

ÀMBIT D'APLICACIÓ DE LA LLEI DE PROTECCIÓ DELS INFORMANTS

1. Àmbit d'aplicació personal.

Aquesta Llei s'aplicarà a les persones físiques informants, que treballen en el sector privat o públic i que hagen obtingut informació sobre infraccions en un context laboral o professional, comprenent en tot cas:

- a) les persones que tinguen la condició d'empleats públics o treballadors per compte d'altri;
- b) els autònoms;
- c) els accionistes, partíps i persones pertanyents a l'òrgan d'administració, direcció o supervisió d'una empresa, inclosos els membres no executius;
- d) qualsevol persona que treballa per a o sota la supervisió i la direcció de contractistes, subcontractistes i proveïdors.

També s'aplicarà als informants que comuniquen o revelen públicament informació sobre infraccions obtinguda en el marc d'una relació laboral o estatutària ja finalitzada, voluntaris, becaris, treballadors en períodes de formació amb independència que perceben o no una remuneració, així com a aquells la relació laboral dels quals encara no haja començat, en els casos en què la informació sobre infraccions haja sigut obtinguda durant el procés de selecció o de negociació precontractual.

2. Entitats obligades en el sector públic.

D'altra banda, la Llei disposa que totes les entitats que integren el sector públic estaran obligades a disposar d'un Sistema intern d'informació en els termes que marca la llei, com ara:



“Totes les entitats que integren el sector públic estaran obligades a disposar d'un Sistema intern d'informació”.

a) L'Administració General de l'Estat, les Administracions de les comunitats autònomes, ciutats amb Estatut d'Autonomia i les **entitats que integren l'Administració Local**.

b) Els **organismes i entitats públiques vinculades o dependents d'alguna Administració pública**, així com aquelles **altres associacions i corporacions** en les quals participen Administracions i organismes públics.

Aquestes entitats seran responsables del tractament de dades de caràcter personal de les persones informants.



PRINCIPALS CARÀCTERÍSTIQUES DEL SISTEMA INTERN D'INFORMACIÓ

La Llei conté unes disposicions generals sobre les característiques o requisits que haurà de complir el canal de denúncies intern, que s'aplicaran tant a sector públic com privat. Entre aquestes, a continuació, se citen les principals:

1. S'imposa l'obligació de realitzar consulta prèvia amb els sindicats i representació legal dels treballadors (empleats públics), als qui se'ls reserva per tant un paper rellevant en la configuració del canal (article 5.1.)

2. L'òrgan d'administració o de govern tindrà la condició de responsable del tractament de les dades personals que siguen objecte de tractament durant les denúncies (article 5.1)

3. En el seu article 5.2.b) la llei imposa que el sistema garantisca la confidencialitat de la identitat de l'informant i de qualsevol tercer esmentat en la comunicació i de les actuacions que es desenvolupen en la gestió i tramitació d'aquesta, la protecció de dades, impedit l'accés de personal no autoritzat. Aquelles persones a les quals es referisquen els fets relatats en la comunicació, efectuada per l'informant, han de comptar amb una singular protecció davant el risc que la informació, fins i tot amb aparent aparença de veracitat, haja sigut manipulada, siga falsa o responga a motivacions que el Dret no pot emparar. Aquestes persones mantenen tots els seus drets de tutela judicial i defensa, d'accés a l'expedient, de confidencialitat i reserva d'identitat i la presumpció d'innocència

4. S'ha de permetre la presentació de comunicacions per escrit o verbalment, o de totes dues maneres (article 5.2.c).

5. En el cas d'existir diferents canals interns de denúncia, aquests hauran d'integrar-se i estar disponibles de manera unificada en la pàgina principal de l'espai web de l'entitat, en una secció separada i fàcilment identificable. A més, el canal de

“L'òrgan d'administració o de govern tindrà la condició de responsable del tractament de les dades personals que siguen objecte de tractament durant les denúncies”.



“La llei imposa que el sistema garantisca la confidencialitat de la identitat de l'informant i de qualsevol tercer esmentat en la comunicació i de les actuacions que es desenvolupen en la gestió i tramitació d'aquesta, la protecció de dades, impedit l'accés de personal no autoritzat.”.

denúncies i el seu funcionament han de ser transparents, obligant a publicar informació de manera clara i fàcilment accessible sobre l'ús de tot canal intern d'informació que hagen implantat, així com sobre els principis essencials del procediment de gestió (article 5.2.d).

6. Han de ser **independents i estar diferenciats de la resta de sistemes d'informació** d'altres entitats o organismes (article 5.2.f).

7. Ha d'existir un **procediment de gestió** de les informacions rebudes (article 5.2.i).

8. Els **canals** de comunicació han de ser **clars, públics i de fàcil accés** a empleats i tercers que desitgen interposar una comunicació.



“L'Administració pública, en qualitat de responsable del tractament, haurà d'adoptar les mesures necessàries per a preservar la identitat i garantir la confidencialitat de les dades corresponents a les persones afectades per la informació subministrada, especialment la de la persona que haguera posat els fets en coneixement de l'entitat, en cas que s'haguera identificat”.

OBLIGACIONS DE L'ADMINISTRACIÓ PÚBLICA, RESPONSABLE DEL TRACTAMENT DE LES DADES PERSONALS DELS INFORMANTS

Sense entrar, de manera exhaustiva i detallada, en totes les actuacions que ha d'escometre l'Administració pública, com a responsable del tractament de les dades personals dels informants i altres persones involucrades, a continuació, s'indiquen les més rellevants:

- 1. L'Administració pública ha de dissenyar, establir i gestionar d'una forma segura el sistema intern d'informació.** De manera que, aquest sistema garantisca la confidencialitat de la identitat de l'informant i de qualsevol tercer esmentat en la comunicació, i de les actuacions que es desenvolupen en la gestió i tramitació d'aquesta, així com la protecció de dades, impedit l'accés de personal no autoritzat.
- 2. L'Administració pública, en qualitat de responsable del tractament, haurà d'adoptar les mesures necessàries per a preservar la identitat i garantir la confidencialitat** de les dades corresponents a les persones afectades per la informació subministrada, especialment la de la persona que haguera posat els fets en coneixement de l'entitat, en cas que s'haguera identificat.

Això suposa l'adopció de **mesures de seguretat, tècniques i organitzatives**, en el sistema d'informació. D'acord amb la Disposició addicional primera de la LOPDGDD, les mesures de seguretat seran conforma al Reial decret 311/2022, de 3 de maig, pel qual es regula l'**Esquema Nacional de Seguretat (ENS)**.

- 3. No obstant això, abans d'adoptar les mesures, atés que, per la naturalesa com pel context, suposa un tractament de dades de caràcter personal d'alt risc per als drets i llibertats de les persones físiques informants, de conformitat amb l'article 35 RGPD, l'Administració pública, en qualitat de responsable del tractament, haurà de realitzar una Avaluació d'Impacte en Protecció de Dades (EIPD).**



“En el cas que es contracte un tercer extern per a la gestió i manteniment del sistema d'informació, l'Administració pública haurà de formalitzar l'encàrrec de tractament de dades personals. Aquest tercer tindrà l'obligació, a preveure a Pliego o contracte, d'adoptar les mesures de seguretat de l'Esquema Nacional de Seguretat”.

4. En el cas que es contracte un tercer extern, per a la gestió i manteniment del sistema d'informació, l'Administració pública haurà de formalitzar, de conformitat amb l'article 28 RGPD i article 33 LOPDGDD, **l'encàrrec de tractament de dades personals**. Aquest tercer, en qualitat d'encarregat de tractament, tindrà l'obligació, a preveure a Pliego o contracte, d'adoptar les mesures de seguretat de l'Esquema Nacional de Seguretat.

5. Les **dades personals** de qui formule la comunicació i dels empleats i tercers **hauran de conservar-se** en el sistema de denúncies únicament durant el **temps imprescindible** per a decidir sobre la procedència d'iniciar una investigació sobre els fets denunciats.

6. En tot cas, transcorreguts 3 mesos des de la introducció de les dades, haurà de procedir-se a la seua supressió del sistema de denúncies, llevat que la finalitat de la conservació siga deixar evidència del funcionament del model de prevenció de la comissió de delictes per la persona jurídica. Les denúncies a les quals no s'haja donat curs solament podran constar de forma anonimitzada. Transcorregut el termini esmentat en el paràgraf anterior, les dades podran continuar sent tractats, per l'òrgan al qual corresponga, conforme a l'apartat 2 d'aquest article, la investigació dels fets denunciats, no conservant-se en el propi sistema d'informació de denúncies internes.

7. La identitat de l'informant només podrà ser comunicada a l'Autoritat judicial, al Ministeri Fiscal o a l'autoritat administrativa competent en el marc d'una investigació penal, disciplinària o sancionadora.



“Tota persona física podrà informar també davant l'Autoritat Independent de Protecció de l'Informant (A.A.I.). En l'àmbit de la Comunitat Valenciana, addicionalment (però no en substitució del canal de la A.A.I.), podrà utilitzar-se la bústia externa de denúncies de l'Agència Valenciana Antifrau”.

CANAL EXTERN D'INFORMACIÓ A.A.I.

El sistema intern d'informació ha de ser **complementat amb un canal extern**, és a dir, amb la possibilitat que qui conega el fet susceptible de ser comunicat conformement a aquesta norma pugui acudir a una autoritat pública que, amb totes les garanties, tinga constància del fet informat i procedisca a investigar-lo i, si escau, pugui col·laborar amb el Ministeri Fiscal quan aprecie que el fet objecte de la comunicació és constitutiu de delicte.

D'aquesta manera, tota persona física **podrà informar davant l'Autoritat Independent de Protecció de l'Informant, A.A.I., o davant les autoritats o òrgans autonòmics** corresponents, de la comissió de qualsevol accions o omissions incloses en l'àmbit d'aplicació d'aquesta llei, ja siga directament o prèvia comunicació a través del corresponent canal intern.

La informació **es podrà realitzar per escrit, a través de correu postal o a través de qualsevol mig electrònic** habilitat a aquest efecte dirigit al canal extern d'informacions de la A.A.I., o verbalment, per via telefònica o a través de sistema de missatgeria de veu. A sol·licitud de l'informant, també podrà presentar-se mitjançant una reunió presencial, dins del termini màxim de set dies. En els casos de comunicació verbal s'advertirà a l'informant que la comunicació serà gravada i se l'informarà del tractament de les seues dades d'acord amb l'article 13 RGPD i 11 LOPDGDD.

En l'àmbit de la Comunitat Valenciana, addicionalment (però no en substitució del canal de la A.A.I.), podrà utilitzar-se la bústia externa de denúncies de l'Agència Valenciana Antifrau i, en tot cas, s'utilitzarà per a comunicar irregularitats contràries a la integritat pública o potencialment constitutives de frau o corrupció d'àmbit autonòmic (incloent tot tipus d'irregularitats per a protegir tota classe de fons públics). Així, a l'efecte de pràctiques contràries a la integritat, frau i corrupció sobre fons públics podrà designar-se com a tal, a l'empara de la Llei 1/2022, de Transparència i Bon Govern de la Comunitat Valenciana, la bústia externa de denúncies de l'Agència Valenciana Antifrau.



*“Al seu torn, conviu amb altres canals de denúncies externs com l'habilitat pel SNCA (*Infofraude), per a la comunicació d'informació sobre frauds o irregularitats que afecten fons europeus, el qual disposa d'un apartat específic relatiu al Mecanisme de Recuperació i Resiliència”.*

Al seu torn, conviu amb altres canals de denúncies externs com l'habilitat pel SNCA (*Infofraude), per a la comunicació d'informació sobre frauds o irregularitats que afecten fons europeus, el qual disposa d'un apartat específic relatiu al Mecanisme de Recuperació i Resiliència, tenint en compte el que es disposa en la Comunicació 1/2017, de 6 d'abril, sobre la forma en la qual poden procedir les persones que tinguen coneixement de fets que puguen ser constitutius de frau o irregularitat en relació amb projectes o operacions finançats totalment o parcialment amb càrrec a fons procedents de la Unió Europea.



***“El Delegat de Protecció de Dades
tindrà accés a les dades personals
continguts en el Sistema intern
d'informació, dins de l'àmbit de les
seues competències i funcions,
exclusivament”.***

EL PAPER DEL DELEGAT DE PROTECCIÓ DE DADES

L'article 24 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (**LOPDGDD**) estableix únicament els requisits que han de tindre els sistemes d'informació de denúncies internes, a fi de garantir la privacitat dels denunciants. No obstant això, res ens diu sobre el nomenament i designació de persona per a l'acompliment de Delegat de Protecció de Dades (DPD) en les entitats obligades a la creació dels sistemes interns d'informació.

Doncs bé, el Preàmbul de la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informen sobre infraccions normatives i de lluita contra la corrupció, ens diu que *“D'altra banda, s'exigeix que les entitats obligades a disposar d'un Sistema intern d'informació, els tercers externs que en el seu cas el gestionen i l'Autoritat Independent de Protecció de Dades, A.A.I. així com les que en el seu cas es constituïsquen, compten amb un delegat de protecció de dades”*.

No obstant això, aquesta obligació no s'ha inclòs en l'articulat vigent de la Llei 2/2023. Únicament, l'article 34 d'aquesta Llei, ens diu que *“D'acord amb el que disposa l'article 37.1.a) del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, l'Autoritat Independent de Protecció de l'Informant, A.A.I., i les autoritats independents que en el seu cas es constituïsquen, hauran de nomenar un delegat de protecció de dades”*.

Abans de l'aprovació de la vigent Llei, el Projecte de Llei incloïa, en el seu article 34, una referència expressa a l'obligació per part de les entitats de nomenar un Delegat de Protecció de Dades, que implicava que totes les entitats privades de més de 50 persones treballadores hagueren de disposar d'un DPD. No obstant això, tal com s'ha recollit en l'articulat finalment aprovat, la Llei obliga únicament a l'Autoritat Independent de Protecció de l'Informant (A.A.I.), i les autoritats independents que en el seu cas es



“Com els subjectes de l'article 77.1 LOPDGDD (això és, en termes generals, l'Administració pública) està obligada a nomenar i designar un DPD, no tindrà la necessitat de nomenar un altre DPD, a l'efecte de l'assessorament i supervisió d'aquest sistema d'informació.”.

constituïsquen a nomenar un DPD; fet que resulta contradictori amb el que es disposa en el Preàmbul. No obstant això, al no incloure, de manera expressa, aquesta obligació en l'articulat vigent de la Llei s'interpreta que s'ha eliminat l'obligació de designar un DPD, de manera general, per a totes aquelles entitats que hagen de disposar d'un Sistema Intern d'informació.

En tot cas, cal dir que, com els subjectes de l'article 77.1 LOPDGDD (això és, en termes generals, **l'Administració pública**) **està obligada a nomenar i designar un DPD, no tindrà la necessitat de nomenar un altre DPD, a l'efecte de l'assessorament i supervisió d'aquest sistema d'informació.**

Aclarit això, **el paper del DPD serà també l'assessorament i supervisió**, com si d'una altra activitat de tractament de dades de caràcter personal es tractara. Si bé, de conformitat amb l'article 32 d'aquesta Llei 2/2023, el DPD també **té accés a les dades personals continguts en el sistema intern d'informació; limitat a l'àmbit de les seues competències i funcions.**



MATERIAL COMPLEMENTARI

- Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informen sobre infraccions normatives i de lluita contra la corrupció. Consulta la Llei en [aquest enllaç](#).
- Directiva (UE) 2019/1937 del Parlament Europeu i del Consell de 23 d'octubre de 2019 relativa a la protecció de les persones que informen sobre infraccions del Dret de la Unió. Consulta la Directiva en [aquest enllaç](#).
- Publicació de l'AEPD sobre "Privacitat en sistemes de denúncia o 'whistleblowing'". Consulta la Publicació en [aquest enllaç](#).

NOTÍCIES

- **El Butlletí Oficial de l'Estat (BOE) ha publicat una modificació de la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD).**
Després de diversos anys des de l'aplicació del Reglament General de Protecció de Dades (RGPD) i l'entrada en vigor de la Llei orgànica, s'han dut a terme modificacions tant en la tramitació d'alguns procediments de l'Agència Espanyola de Protecció de Dades (AEPD) com en el seu Estatut. Consulta la Publicació en [aquest enllaç](#).
- **L'Agència Espanyola de Protecció de Dades (AEPD) ha publicat, en col·laboració amb l'Associació Espanyola per al Foment de la Seguretat de la Informació (ISMS Fòrum) i l'Associació Professional Espanyola de Privacitat (APEP), la guia Orientacions per a la supervisió de sistemes criptogràfics com a mesura de seguretat en protecció de dades.**
El document recull que el xifratge serà una mesura adequada de seguretat per a la protecció de dades sempre que la seua implementació s'ajuste a les característiques i impacte del tractament en els drets i llibertats dels afectats. Consulta la Publicació en [aquest enllaç](#).