

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 22 | Abril 2022

LA PROTECCIÓ DE DADES EN LES RELACIONS LABORALS



Í N D E X



LA PROTECCIÓ DE DADES EN LES RELACIONS LABORALS

	Pàgina
Introducció	2
Aspectes generals	3
Base de licitud	4
Drets de protecció de dades	5
Sistemes interns de denúncies	7
Protecció de la privacitat de les víctimes d'assetjament i violència de gènere	8
Material complementari i notícies	10



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

Departament 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](#)



***“ES RECONeix EL DRET A LA INTIMITAT
EN L'ÚS DE DISPOSITIUS DIGITALS I
ENFRONT DE L'ÚS DE DISPOSITIUS DE
VIDEOVIGILÀNCIA I GEOLOCALITZACIÓ,
AIXÍ COM A LA DESCONNEXIÓ DIGITAL”.***

INTRODUCCIÓ

Les entitats públiques i privades requereixen tractar dades personals de l'àrea de recursos humans necessaris per a dur a terme la seua activitat. El tractament de dades d'empleats públics ha de garantir els principis i requisits legals establits per la normativa de protecció de dades vigent.

En particular, la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals (d'ara en avant, “LOPDGDD”) estableix diverses disposicions aplicables a l'àmbit del sector públic, especialment respecte a aquelles finalitats dirigides a controlar el compliment de les obligacions del personal públic i garantir la integritat dels dispositius portàtils destinats a l'exercici de les seues funcions.

La LOPDGDD modifica el text refós de la Llei de l'Estatut Bàsic de l'Empleat públic (d'ara en avant, “EBEP”) reconeixent el dret de l'empleat públic a la intimitat en l'ús de dispositius digitals posats a la seua disposició i enfront de l'ús de dispositius de videovigilància i geolocalització, així com a la desconnexió digital en els termes establits en la legislació vigent en matèria de protecció de dades personals i garantia dels drets digitals.

L'Agència Espanyola de Protecció de Dades va publicar la Guia relativa a la “Protecció de dades en les relacions laborals” destinada a proporcionar una orientació de caràcter pràctic, no vinculant, que facilite als responsables i encarregats el compliment de la legislació.

En aquest document s'analitzaran els principals aspectes tractats en la Guia de protecció de dades en les relacions laborals, des de la perspectiva enfocada en la seua aplicació en el sector públic.



***“EL TRACTAMENT DE DADES DELS
RECURSOS HUMANS POT ABASTAR UN
AMPLI VENTALL DE DADES
PERSONALS, INCLOSES CATEGORIES
ESPECIALS DE DADES”.***

ASPECTES GENERALS

D'acord amb el que es disposa en l'article 4.1 del Reglament General de Protecció de Dades (d'ara en avant, "RGPD") es considera dada de caràcter personal:

“Tota informació relativa a una persona física identificada o identificable”.

Com s'avançava a la introducció, el tractament de dades dels recursos humans, siguen referents al sector públic o al privat, ha de garantir la privacitat i el compliment de la normativa de protecció de dades vigent. En particular, el tractament pot abastar un ampli ventall de dades personals, incloses categories especials de dades.

L'article 9.1 de l'RGPD estableix amb caràcter general la prohibició de tractar categories especials de dades. No obstant això, en el seu segon apartat, estableix una relació de supòsits en virtut dels quals s'habilita als Responsables a tractar aquesta categoria de dades personals.

Una de les excepcions a la qual fa referència l'Agència Espanyola de Protecció de Dades en la Guia de protecció de dades en les relacions laborals és l'establida en l'article 9.2.b) RGPD, quant el tractament:

“És necessari per al compliment d'obligacions i l'exercici de drets específics del responsable del tractament o de l'interessat en l'àmbit del Dret laboral i de la seguretat i protecció social...”

Exemples de categories especials de dades

Informació relativa la situació de discapacitat de la persona treballadora a l'efecte de reduccions o bonificacions de quotes a la Seguretat Social.

Sistema de fitxatge per al control horari basat en el reconeixement facial/empremta dactilar (dades biomètriques).



BASE DE LICITUD

El tractament de dades personals exigeix que el responsable del tractament compte amb una “base jurídica” que el legitime per a aquest tractament concret.

En les relacions laborals, la base jurídica principal és l'execució del contracte de treball (article 6.1.b RGPD). No obstant això, en referència al consentiment com a base de licitud en l'àmbit que ens ocupa, l'AEPD estableix a la Guia de Protecció de Dades i Relacions Laborals, que el consentiment de l'interessat no és vàlid quan es proporciona en un context de “desequilibri clar entre l'interessat i el responsable del tractament”. En l'àmbit públic, aquesta impossibilitat es reflecteix principal i clarament en la relació professional que vincula al personal laboral amb l'entitat pública:

Article 19 Llei 4/2021, de 16 d'abril, de la Funció Pública Valenciana

“És personal laboral qui [...] està vinculat a qualsevol de les administracions públiques, organismes públics, consorcis o universitats públiques, mitjançant una relació professional caracteritzada per les notes d'alienitat, dependència, voluntarietat i retribució.

«És molt poc probable que el consentiment constituïska una base jurídica per al tractament de dades en el treball, llevat que els treballadors puguem negar-se sense conseqüències adverses [...]. Excepte en situacions excepcionals, els empresaris hauran de basar-se en un altre fonament jurídic diferent del consentiment, com la necessitat de tractar les dades per al seu interès legítim.

No obstant això, un interès legítim en si mateix no és suficient per a prevaldre sobre els drets i llibertats dels treballadors».

(Dictamen 2/2017 sobre el tractament de dades en el treball del Grup de Treball de l'Article 29).

“EL CONSENTIMENT DE L'INTERESSAT NO ÉS VÀLID QUAN ES PROPORCIONA EN UN CONTEXT DE DESEQUILIBRI CLAR ENTRE L'INTERESSAT I EL RESPONSABLE DEL TRACTAMENT”.



***“LA LIMITACIÓ DEL TRACTAMENT ES
BASA EN EL MARCAT DE LES DADES DE
CARÀCTER PERSONAL CONSERVATS
AMB LA FINALITAT DE LIMITAR EL SEU
TRACTAMENT EN EL FUTUR”.***

DRETS DE PROTECCIÓ DE DADES

Les persones treballadores, en tant són interessats en el tractament de les seues dades personals, poden exercir els següents drets enfront del responsable del tractament:

DRET D'ACCÉS (ART. 15 RGPD)

Independentment de la informació que se li haja proporcionat sobre el tractament, la persona treballadora té dret a obtindre la confirmació que s'està produint un tractament de dades i, en el seu cas, com s'està produint el mateix.

Així mateix, poden sol·licitar una còpia de les dades personals que estan sent objecte del tractament.

DRET DE RECTIFICACIÓ (ART. 16 RGPD)

Les persones treballadores tenen la possibilitat d'exigir la rectificació de les dades inexactes que estiguen sent objecte de tractament, així com completar aquella informació de caràcter personal que resulte incompleta.

DRET DE SUPRESSIÓ (ART.17 RGPD)

Les persones treballadores tenen la possibilitat d'exigir la supressió de les dades personals objecte del tractament en determinades situacions, com ara: quan les dades personals no siguen necessàries o la base de licitud siga el consentiment i aquest haja sigut retirat.

DRET A LA LIMITACIÓ DEL TRACTAMENT (ART. 18)

D'acord amb el que es disposa en l'article 4.3 de l'RGPD la limitació del tractament es basa en “el marcat de les dades de caràcter personal conservats amb la finalitat de limitar el seu tractament en el futur”. És un dret de les persones treballadores quan es donen les circumstàncies establides en l'RGPD.



***“ES RECONeix COM A DRET
INDIVIDUAL DELS EMPLEATS PÚBLICS
EL DRET A LA INTIMITAT EN L'ÚS DELS
DISPOSITIUS DIGITALS I EL DRET A LA
DESCONNEXIÓ DIGITAL”.***

DRET A LA PORTABILITAT DE LES DADES (ART.20 RGPD)

Quan la base de licitud del tractament siga el consentiment o l'execució d'un contracte, la persona treballadora té dret a obtindre les seues dades personals en un format estructurat, d'ús comú i lectura mecànica, i a transmetre'ls a un altre responsable del tractament sense que ho impedisca el responsable al qual li'ls haguera facilitats.

DRET D'OPOSICIÓ (ART. 21 RGPD)

Si la base de licitud és la satisfacció d'interessos legítims perseguits pel responsable o per un tercer o una missió realitzada en interès públic, les persones treballadores podran exercir el dret d'oposició, llevat que s'acrediten motius legítims que prevalguen sobre els interessos, drets i llibertats de les persones treballadores o per a la formulació, l'exercici o la defensa de reclamacions.

A més dels drets esmentats cal destacar la modificació de l'EBEP amb l'entrada en vigor de la disposició final catorzena de la LOPDGDD. Amb aquesta modificació es reconeix com a dret individual dels empleats públics el dret a la intimitat en l'ús de dispositius digitals posats a la seua disposició i enfront de l'ús de dispositius de videovigilància i geolocalització, així com el dret a la desconnexió digital en els termes establits en la legislació vigent.

Sobre la base del que s'estableix en l'article 88 LOPDGDD, el dret a la desconnexió digital té per objectiu garantir, fora del temps de treball legal o convencionalment establert, el respecte del seu temps de descans, permisos i vacances, així com de la seua intimitat personal i familiar.



“LA IMPLEMENTACIÓ DE SISTEMES DE DENÚNCIES INTERNES PROVÉ DE L'EXISTÈNCIA D'UN INTERÉS PÚBLIC ”

SISTEMES INTERNES DE DENÚNCIES O “WHISTLEBLOWING”

És habitual en la pràctica configurar els sistemes interns de denúncies o “*whistleblowing*” mitjançant la creació de bústies internes. A través d'aquests canals les persones treballadores posen de manifest la comissió d'actes o conductes contràries a la llei.

Referent a la base de licitud d'aquests sistemes, la pròpia LOPDGDD estableix que la licitud del tractament relatiu a la implementació de sistemes de denúncies internes prové de l'existència d'un interès públic, en els termes establits en l'article 6.1.e) de l'RGPD. A més, la transposició a Espanya de la Directiva (UE) 2019/1937 pot implicar una obligació legal.

L'article 24.5 de la LOPDGDD estableix que els principis que es recullen en els seus apartats 1-4 seran aplicables als sistemes de denúncies internes que pogueren crear-se en les Administracions Públiques. En particular, els requisits que ha de reunir un sistema d'informació de denúncies internes són els següents:

- Els empleats i tercers hauran de ser informats sobre l'existència del sistema.
- S'haurà de limitar l'accés a les dades contingudes en el sistema al personal estrictament necessari.
- Hauran d'adoptar-se les mesures necessàries per a preservar la identitat i garantir la confidencialitat de les dades personals contingudes en el sistema, especialment els referits a la persona denunciant dels fets.
- La LOPDGDD permet sistemes de denúncies internes “anònimes”.
- Ha de regir el principi de limitació del termini de conservació de les dades personals. En tot cas, transcorreguts tres mesos de la introducció de les dades, haurà de procedir-se a la seua supressió.

Les denúncies a les quals no s'haja donat curs solament podran constar de forma anonimitzada, sense que resulte d'aplicació l'obligació de bloqueig establida en l'article 32 de la LOPDGDD.



PROTECCIÓ DE LA PRIVACITAT DE LES VÍCTIMES D'ASSETJAMENT I VIOLÈNCIA DE GÈNERE

La informació de caràcter personal de les víctimes d'assetjament en el treball i de les dones supervivents a la violència de gènere tenen, amb caràcter general, la consideració de categories especials de dades personals, per la qual cosa s'exigeix al responsable del tractament una protecció reforçada (Informe AEPD 149 – 2019).

En els supòsits d'assetjament en aquest àmbit, en les seues diferents modalitats, el responsable del tractament haurà d'adoptar mesures oportunes respecte de l'assetjador i de la persona assetjada. Entre aquestes mesures s'inclou l'obligació de protegir les dades personals.

La posada en marxa de procediments sancionadors enfront de l'assetjador no requereix del consentiment de la persona assetjada. La base de licitud en aquest cas es troba en el compliment d'una obligació legal (art. 6.1.c) de l'RGPD). D'una banda, en el sector privat, l'empresa és garant de la salut i seguretat en el treball conforme als articles 4.2.d) de l'Estatut dels treballadors i 14 de la Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals (LPRL). D'altra banda, en el sector públic, regeix el que s'estableix en l'EBEP:

- Els funcionaris públics i el personal laboral queden subjectes al règim disciplinari establert en el TÍTOL VII EBEP i a les normes que les lleis de Funció Pública dicten en desenvolupament de l'EBEP. (ART. 93.1 EBEP).
- Les Administracions Públiques corregiran disciplinàriament les infraccions del personal al seu servei, sense perjudici de la responsabilitat patrimonial o penal que poguera derivar-se de tals infraccions. (Art.94.1 EBEP).

Si l'acte o conducta fora constitutiu de delictes públics, tot testimoni del mateix està obligat a posar-ho en coneixement de la Justícia, de la mateixa manera que si es tractara d'altres delictes, inclosos els lleus, que es cometien en l'àmbit de la violència de gènere.

***“LA POSADA EN MARXA DE
PROCEDIMENTS SANCIONADORS
ENFRONT DE L'ASSETJADOR NO
REQUEREIX DEL CONSENTIMENT DE LA
PERSONA ASSETJADA. LA BASE DE
LICITUD EN AQUEST CAS SERIA EL
COMPLIMENT D'UNA OBLIGACIÓ
LEGAL”.***



***“FINALITZAT EL PROCEDIMENT
SANCIONADOR, LES DADES HAN DE
ROMANDRE BLOQUEJADES DURANT
EL PERÍODE DE PRESCRIPCIÓ DE LA
SANCIO, O EN TANT PUGUEN SER
UTILITZADES EN UN PROCEDIMENT
JUDICIAL”.***

S'ha de garantir la confidencialitat de la informació tractada i la identitat de la víctima solament serà revelada davant persones amb interès en el procediment, no sent en cap cas admissible una publicitat massiva o indiscriminada sense consentiment de la víctima, ni tampoc l'accés a les dades de persones no legitimades. Per a garantir la confidencialitat resulta convenient assignar un codi identificatiu tant de la persona suposadament assetjada com la suposadament assetjadora, a fi de preservar la identitat d'aquestes.

Una vegada finalitzat el procediment sancionador, les dades han de romandre bloquejades durant el període de prescripció de la sanció, o en tant puguen ser utilitzades en un procediment judicial.

El bloqueig de les dades, tal com estableix l'article 32.2 de la LOPDGDD, consisteix en la identificació i reserva d'aquestes, adoptant mesures tècniques i organitzatives, per a impedir el seu tractament, incloent la seua visualització, excepte per a la posada a disposició de les dades als jutges i tribunals, el Ministeri Fiscal o les Administracions Públiques competents, en particular de les autoritats de protecció de dades, per a l'exigència de possibles responsabilitats derivades del tractament i només pel termini de prescripció d'aquestes.

Una vegada finalitzat el termini de prescripció s'haurà de procedir a la destrucció de les dades.



MATERIAL COMPLEMENTARI

- 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 [aquest enllaç](#).
- Dictamen 2/2017, sobre el tractament de dades en el treball (GT29). Consulta [aquest enllaç](#).
- Guia: "Protecció de dades en les relacions laborals" (AEPD). Consulta [aquest enllaç](#).
- Recomanacions de l'AEPD sobre la Protecció de Dades com a garantia en les polítiques de prevenció de l'assetjament. Consulta [aquest enllaç](#).
- Guia: "Protecció de dades i prevenció de delictes". Consulta [aquest enllaç](#).

NOTICIES

- **L'AEPD imposa una sanció de prevenció a un Ajuntament per haver-hi infringit el deure d'informar els seus empleats respecte al tractament de l'empremta dactilar.** L'AEPD recorda que la implantació d'un sistema de control horari basat en la petjada per part de l'ocupador ha de ser informada als empleats de manera clara, completa, concisa i, a més, fent referència a les bases legals i informació requerida per l'article 13 de l'RGPD. Així mateix, l'AEPD determina que l'empremta dactilar ha de ser classificada com a dada biomètrica. Consulta la resolució en [aquest enllaç](#).
- **L'AEPD resol una consulta relativa a l'anàlisi de la qualitat de les dades d'una víctima de violència de gènere com a mereixedors d'especial protecció, per a dispensar-los o no, la protecció que s'estableix en l'article 9 de l'RGPD.** L'AEPD conclou que no estem davant dades personals ordinàries, no ha d'obviar-se que són dades sensibles que requereixen major protecció. Si bé l'AEPD considera que les categories especials de dades han de considerar-se com a "numerus clausus", s'han de tractar d'acord amb l'eficàcia i abast d'un dret fonamental en relació amb l'especial consideració que el legislador i, en el seu cas, els poders públics, atorguen al col·lectiu de víctimes de violència de gènere. Consulta en [aquest enllaç](#).
- **L'AEPD resol una consulta remesa per l'Associació Espanyola de Compliance (ASCOM) relativa al període de conservació de les dades personals recaptades a través dels canals de denúncies interns.** L'AEPD fa esment a l'article 24 de la LOPDGDD que estableix el termini de 3 mesos des de la introducció de les dades en el sistema de denúncies. A més, puntualitza que en el cas que la denúncia pugui considerar-se fundada i done lloc a una concreta investigació, no implica que hagen de suprimir-se dels sistemes de l'entitat, sinó que únicament procedirà la seua supressió del concret sistema d'informació de denúncies internes, passant a integrar-se en els sistemes propis de l'òrgan de compliment o, en el seu cas, del que tinga al seu càrrec la gestió de personal. Consulta en [aquest enllaç](#).