



Guia bàsica en protecció de dades de caràcter personal



Índex

1 | 18

Introducció

2 | 18

Bloc I - Qüestions generals

3 | 18

1. Normativa de protecció de dades

4 | 18

2. Què es defineix com a dada personal?

5 | 18

3. Qui és qui en protecció de dades?

6 | 18

Bloc II - Obligacions rellevants de la Diputació, en qualitat de responsable del tractament de dades de caràcter personal

7 | 18

1. Registre d'Activitats de Tractament (R.A.T.)

8 | 18

2. Deure d'informar del tractament dades

9 | 18

3. Encàrrecs de tractament de dades personals

10 | 18

4. Adopció de mesures de seguretat

11 | 18

5. Anàlisi de Riscos i Avaluacions d'Impacte en Protecció de Dades

12 | 18

6. Incident en la seguretat de dades personals

13 | 18

7. Drets en protecció de dades

14 | 18

8. Videovigilància

15 | 18

Bloc III - Bones pràctiques en el tractament de les dades per part de les persones usuàries del sistema d'informació

16 | 18

1. Bones pràctiques en el tractament automatitzat (informàtic) de dades personals

17 | 18

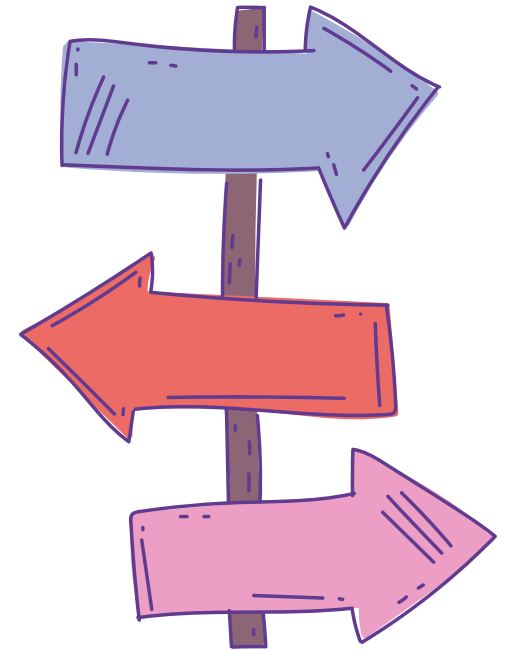
2. Bones pràctiques en el tractament no automatitzat (paper) de dades personals

18 | 18

En aquesta **guia, amb un caràcter succint, clar i senzill**, s'aborden les **qüestions elementals** que, el personal de la Diputació, haguera de conèixer en relació a l'**aplicació de la legislació en protecció de dades de caràcter personal**.

Aquesta guia es divideix en **3 grans blocs**, que tracten la següent temàtica:

- I.** En el primer bloc, s'indiquen les **principals normes reguladores, l'objecte i abast** d'aquestes. Així com, s'assenyalen els **conceptes bàsics** en protecció de dades, quant a què es defineix com a dada de caràcter personal, tipologia de dades personals i, a més, es presenten les diferents figures involucrades en la protecció de dades a nivell de la Diputació.
- II.** En el segon bloc, es relacionen i es desgranen, sense exhaustivitat, **les obligacions rellevants que, la Diputació, ha de complir**.
- III.** Finalment, el tercer bloc assenyala aquells **aspectes més rellevants que, el personal de la Diputació, ha de tindre en compte en el tractament, informàtic o en paper, de dades personals**.

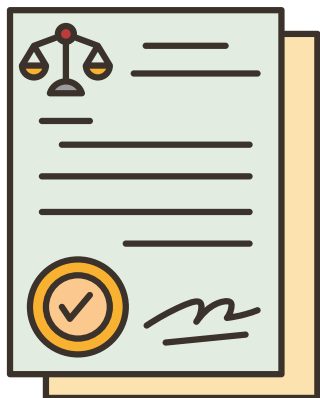




Bloc I

Qüestions generals

1. Normativa de protecció de dades



1. Dret fonamental. Protecció de dades de persones físiques.

La protecció de dades concernents a persones físiques és un **dret fonamental**.

El **tractament automatitzat (informàtic) o no automatitzat (paper) de dades de persones físiques (no jurídiques) ha de ser protegit** per les entitats, públiques o privades, responsables o encarregades d'aquest tractament.

La legislació contempla un conjunt de principis i normes encaminades a **garantir els drets de les persones sobre el control de la seua informació personal** (= drets d'accés, rectificació, supressió, limitació, oposició, portabilitat) i sobre la confidencialitat, integritat i disponibilitat d'aquesta, a conferir, mitjançant l'adopció de **mesures de seguretat**, tècniques i organitzatives, per part de l'entitat, responsable o encarregada del tractament de les dades de caràcter personal.

La Diputació en tractar dades de de persones físiques està subjecta a les obligacions i responsabilitats d'aquesta normativa.



2. Principals normes reguladores.

Generals

- 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 (Reglament general de protecció de dades o **RGPD**).
- Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (**LOPDGDD**).

Específiques de la Diputació

- **Reglament** pel qual es regula la política de seguretat i de la protecció de dades de caràcter personal en aquesta corporació [BOPB *Nº127 5/7/2022].
- **Normativa** de Protecció de Dades de Caràcter Personal [Decret núm. 15874, de 27 de desembre de 2022, del President de la Diputació].
- **Procediments** de protecció de dades de caràcter personal [Decret núm. 15875, de 27 de desembre de 2022, del President de la Diputació].

2. Què es defineix com a dada personal?

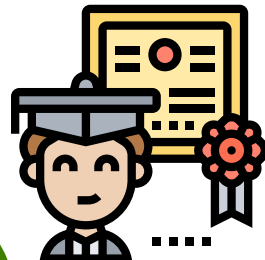
1. Definició.



Dada de caràcter personal és **tota informació concernent a una persona física** (no jurídica), **identificada o identificable**.

Exemples

Nom i cognoms; DNI/Passaport; Signatura; Domicili; Correu electrònic; Telèfon.; Edat; Sexe; Nacionalitat; Imatge/Veu; Dades bancàries; Titulació.



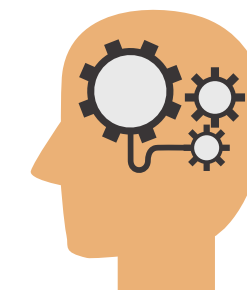
2. Tipologia de dades.

- **Dades identificatives** [entre altres, Nom i Cognoms; DNI/NIE/Passaport; Núm. S. S.; Adreça; Telèfon; Imatge; Veu; Marca Física; Signatura; empremta digital; Signatura electrònica].
- **Dades d'infraccions o sancions administratives i dades de naturalesa penal.**
- **Dades de característiques personals** [ens altres, Estat civil; Edat; Sexe; Data de naixement; Nacionalitat].
- **Dades de circumstàncies socials** [ens altres, Aficions i estil de vida; Pertinença a clubs, associacions; Llicències, permisos, autoritzacions].
- **Dades acadèmiques i professionals** [entre altres, Titulacions; Experiència professional; Pertinença a col·legis o associacions professionals]
- **Dades detall d'ocupació** [ens altres, Cos/Escala; Categoria/grau; Historial treballador]
- **Dades d'informació comercial** [entre altres, Activitats i negocis; Llicències comercials]
- **Dades economicofinanceres i d'assegurances** [entre altres, Dades bancàries; Rendes; Inversions, Béns patrimonials; Crèdits; Pensions; Nòmina; Deduccions impositives/imposades; Assegurances; Hipoteques; Subsidis].
- **Dades de transaccions** [Béns i serveis subministrats per l'afectat; Béns i serveis rebuts per l'afectat; Transaccions financeres; Compensacions/indemnitzacions].

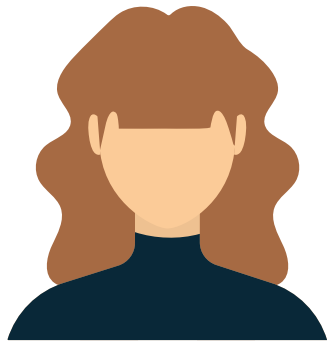
3. Dades de categoria especial.

Es tracta d'aquells que pertanyen a l'**esfera o halo més íntim de la persona**. Es consideren més **sensibles** i, és per això que, mereixen especial protecció.

- Dades relatives a la salut, física o psíquica
- Opinions polítiques.
- Convicció religiosa o filosòfica.
- Afiliació sindical.
- Origen ètnic o racial.
- Dades genètiques.
- Dades biomètriques dirigides a identificar de manera unívoca a una persona física (ex. empremta dactilar, reconeixement facial).
- Vida o orientació sexual.



3. Qui és qui en protecció de dades?



1. Interessat o Interessada

Persona física, titular de les dades personals.

En l'àmbit de la Diputació, es tracten dades de diversos col·lectius o grups de persones físiques, titulars de dades personals (Ex. ciutadans, càrrecs i empleats públics, proveïdors, candidats o aspirants en oferta pública d'ocupació).



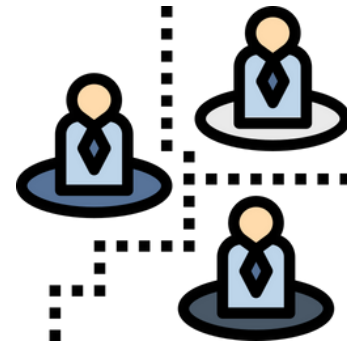
2. Responsable del Tractament (RT)

Persona física o jurídica, autoritat pública, servei o organisme que **determina els fins i mitjans del tractament que es realitza.**

En el nostre àmbit, la condició de RT s'atribueix a la persona jurídica pública, Diputació provincial de València. No s'atribueix a càrrec o empleat públic, de manera individual i/o nominativa.

La Diputació és el subjecte obligat i és el que respon davant l'autoritat de control, Agència Espanyola de Protecció de Dades.

No obstant això, els CGT assumeixen les obligacions de complir amb la normativa interna en protecció de dades.



3. Centre Gestor del Tractament (CGT)

Unitat administrativa de la Diputació **responsable del fitxer o tractament** de dades corresponent.

La seua determinació es basarà en la **vinculació que aquestes unitats tinguen amb l'activitat de tractament:**

- Presta el servei o té la competència per a la qual cosa es tracten les dades.
- Decideix sobre la creació, finalitat i/o tipus de dades o l'ús d'aquests.
- Principal o major usuària de les dades.



4. Usuari o Usuaria

Càrrec, empleada o empleat públic de la Diputació **que,** en l'acompliment de les funcions i tasques, accedeix o **tracta dades de caràcter personal**, a nivell informàtic i/o en paper.



5. Encarregat del Tractament (ET)

Persona física o jurídica, autoritat, servei o organisme que **tracta les dades per compte del Responsable del tractament (Diputació).**

En l'àmbit de la Diputació, la condició de ET s'atribueix als tercers, adjudicataris, contractistes o concessionaris, la prestació de servei dels quals comporte un accés o tractament de dades de caràcter personal, dels quals és responsable del tractament la Diputació. (Ex. Empresa subministre programari).

Al seu torn, la Diputació és ET respecte dels Ajuntaments (Ex. Gestió i recaptació de tributs locals).



6. Delegat o Delegada de Protecció de Dades (DPD)

Persona física o jurídica, pública o privada, **d'obligat nomenament** i designació en l'Administració pública.

La figura del DPD pot ser designada a nivell **intern**, com és el cas de la Diputació. O, en el seu cas, designar a una persona, física o jurídica, **externa**.

El DPD és una figura que actua amb independència i respon al més alt nivell jeràrquic.

Les principals funcions del DPD són la de **supervisar i assessorar en el compliment de la normativa**. Al seu torn, s'ocupa de la interlocució amb l'autoritat de control, Agència Espanyola de *Proteccion de Dades, així com amb els titulars de dades.

Pots contactar amb el nostre DPD: **pdp@dival.es**.



Bloc II

Obligacions rellevants de la Diputació, en qualitat de responsable del tractament de dades de caràcter personal

1. Registre d'Activitats de Tractament



1. És l'**inventari de les activitats de tractament de dades de caràcter personal**, que s'efectuen, en qualitat de responsable o encarregat, per part dels diferents òrgans o unitats administratives de la Diputació, en l'acompliment de les funcions o competències atribuïdes. En el R.A.T. consten, entre altres: (i) la finalitat o ús de les dades (ii) la base jurídica de licitud (iii) tipologia de dades (iv) categoria d'interessats (v) terminis de conservació (vi) cessionaris o destinataris de les dades (vii) dades de contacte del Delegat de Protecció de Dades.

2. La Diputació té un **Registre d'Activitats del Tractament (R.A.T.)**:

- En qualitat de **RESPONSABLE**: inventari d'activitats de tractament de dades personals, de les quals decideix per si, la Diputació, l'ús, els fins i els mitjans del tractament.
- En qualitat d'**ENCARREGAT**: activitats de tractament que efectua per compte d'una altra entitat pública. Ex. gestió tributària per compte dels Ajuntaments.

3. La Diputació ha de posar a la disposició del públic per mitjans electrònics, el R.A.T., en qualitat de responsable i d'encarregat del tractament. La Diputació té **publicat** els R.A.T. en:

www.dival.es/content/registre-activitats-de-tractament





1. En què consisteix?

La Diputació ha d'**informar** els interessats [persones físiques titulars de dades] **sobre el tractament de les dades personals.**

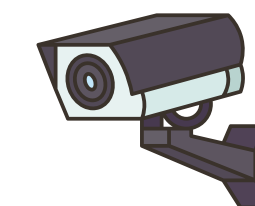
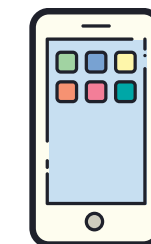
L'interessat té el **dret a ser informat** de manera prèvia, concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill.

2. Deure d'informar del tractament dades

2. Canals o mitjans de recollida, on haurem d'informar l'interessat:

3. De què hem d'informar?

- Dades identificant Responsable de tractament (Diputació) i el contacte amb el Delegat de Protecció de Dades (pdp@dival.es).
- Fins i base jurídica del tractament.
- Termini de conservació o, criteris utilitzats per a determinar aquest termini.
- En el seu cas, destinataris o categories de destinataris.
- En el seu cas, transferències internacionals.
- Drets dels interessats.
- Dret a presentar reclamació davant l'Agència Espanyola de Protecció de Dades.



4. Com informar?

En funció del canal de recollida de dades, haurem d'adoptar la manera d'informar més adequat. Encara que tinguem limitacions, en tot cas, sempre haurà de transmetre's una informació, de caràcter bàsic i després completar tota la informació en un altre espai. Així, s'admet la informació per capes:

1ª Capa: Informació bàsica.

- Identitat del responsable del tractament (= Diputació de València).
- Descripció senzilla dels fins del tractament.
- Referència a l'exercici de drets en protecció de dades.

2ª Capa: Informació completa.

S'inclou tota la informació preceptiva indicada en l'apartat anterior. A aquest efecte, es tracta, per exemple, d'informar en el revers d'un imprés; locució telefònica; indicar una adreça web (Política Privacitat); un codi QR; cartell zona videovigilada.

3. Encàrrecs de tractament de dades personals



1. Qui és l'Encarregat del Tractament (ET)?

Persona física o jurídica, autoritat, servei o organisme que **tracta les dades per compte del Responsable del tractament (Diputació)**.

En l'àmbit de la Diputació, la condició de ET s'atribueix als tercers, adjudicataris, contractistes o concessionaris, la prestació de servei dels quals comporte un accés o tractament de dades de caràcter personal, dels quals és responsable del tractament la Diputació. (Ex. Empresa subministre programari).

Al seu torn, la Diputació és ET respecte dels Ajuntaments (Ex. Gestió i recaptació de tributs locals).

2. Com s'articulen els encàrrecs de tractament? En **actes jurídics o contractes** (si escau, acords o convenis) entre la Diputació i el tercer, ET. En matèria de contractació, a través dels **Plecs** (PCPA i/o PPT).

3. Què es contempla en l'encàrrec de tractament?

- Objecte, la duració, la naturalesa i la finalitat del tractament, el tipus de dades personals i categories d'interessats.
- Les persones autoritzades per a tractar les dades personals estan subjectes al **deure de confidencialitat**.
- Prendrà totes les **mesures de seguretat** necessàries per a la protecció de les dades. En concret, seran conforme a l'Esquema Nacional de Seguretat (ENS).
- **Assistir** a la Diputació, en el seu cas, en l'obligació de respondre sol·licituds d'exercici de dret en protecció de dades.
- A elecció de la Diputació, **suprimirà o retornarà totes les dades** personals una vegada finalitze la prestació dels serveis de tractament.
- Permetrà i contribuirà a la realització d'**auditories**, incloses **inspeccions**, per part de la Diputació o tercer contractat a aquest efecte.
- Ha de transmetre's **idèntiques obligacions i responsabilitats** als tercers, en el seu cas, **subcontractats**.

4. Què més es contempla en un encàrrec de tractament? D'acord amb la legislació de contractació del sector públic, el licitador haurà d'aportar una **declaració responsable** en el qual indique **on estan situats els servidors** i els serveis associats a aquests, utilitzats, en el seu cas, per a albergar les dades personals.

Tinga's en compte que dades relatives a **censos electorals, de població, fiscals o tributaris, i d'usuaris del servei de salut** no poden albergar-se en països fora de l'Espai Econòmic Europeu o que no tinguen decisió d'adequació de la Comissió Europea.

Pots consultar el **Repositori documental de protecció de dades** de la Diputació ací:

www.dival.es/intranet/node/42701



4. Adopció de mesures de seguretat

1. Esquema Nacional de Seguretat

La protecció de les dades de caràcter personal, tractats per la Diputació, serà conforme a les **mesures de seguretat** previstes pel Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (**ENS**).

2. Mesures de protecció

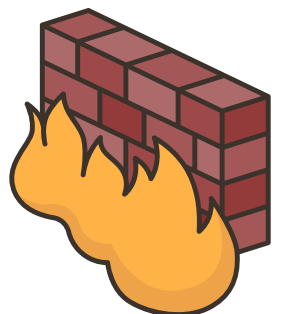
A part de mesures de caràcter organitzatiu i operacional, la Diputació **ha d'adoptar mesures tècniques de seguretat per a la protecció:**



De les instal·lacions i infraestructures (Ex. Portar una relació de persones autoritzades i un sistema de control d'accés que verifiqui la identitat i, en el seu cas, l'autorització).



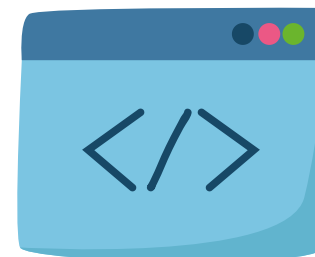
Dels equips (Ex. Bloqueig automàtic de l'equip informàtic davant un temps d'inactivitat).



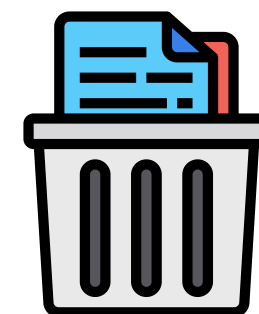
De les comunicacions (Ex. Instal·lació d'un tallafocs que separe la xarxa interna de l'exterior. Tot el trànsit de comunicacions amb l'exterior estarà sotmés als tallafocs).



De la informació (Ex. Realitzar còpies de seguretat que permeten recuperar dades perdudes accidentalment o a causa d'un ciberatac).



De les aplicacions informàtiques (Ex. Durant les proves de desenvolupament o producció de l'aplicació es tractarà de no usar dades reals, sinó dades fictícies).



Dels suports d'informació (Ex. Esborrat o destrucció segura dels suports extraïbles (electrònics i no electrònics) que vagen a ser reutilitzats).

5. Anàlisi de Riscos i Avaluacions d'Impacte en Protecció de Dades

1. Anàlisi de Riscos

Totes les activitats de tractament de dades personals **impliquen un risc** per a les persones les dades de les quals són tractats i, en particular, per als seus **drets i llibertats**.

En funció dels riscos detectats, s'hauran d'adoptar les **mesures de seguretat** oportunes per a evitar o mitigar aquests.



2. Avaluacions d'Impacte en Protecció de Dades (AIPD)

La Diputació haurà de realitzar una AIPD quan siga probable que un tipus de tractament de dades personals comporte un **ALT RISC per als drets i llibertats de les persones físiques**.

Exemples de supòsits en els quals s'haguera de dur a terme una AIPD, prèviament a efectuar el tractament de les dades de les persones:



- Utilització de reconeixement facial per a controlar l'accés a les instal·lacions.



- Implantació d'un Sistema intern d'informació per a garantir la protecció de les persones que informen sobre infraccions normatives, en compliment 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.

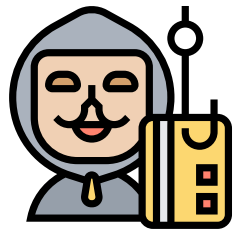
6. Incident en la seguretat de dades personals

1. Què es considera incident en protecció de dades?

L'«**incident**», en aquest context, és qualsevol anomalia que afecte o poguera afectar la seguretat de les dades personals, a nivell informàtic o en paper.

Es considera «**violació de seguretat**» totes aquelles violacions o bretxes de la seguretat que ocasionen la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservats o tractats d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades. Afecta a la confidencialitat, integritat o disponibilitat de les dades personals.

Exemples



Ciberincident per Suplantació d'identitat (Phishing)



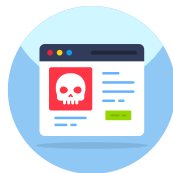
Ciberincident per infecció de virus informàtic



Ciberincident per dispositiu xifrat / segrest de dades (Ex. Ransomware)



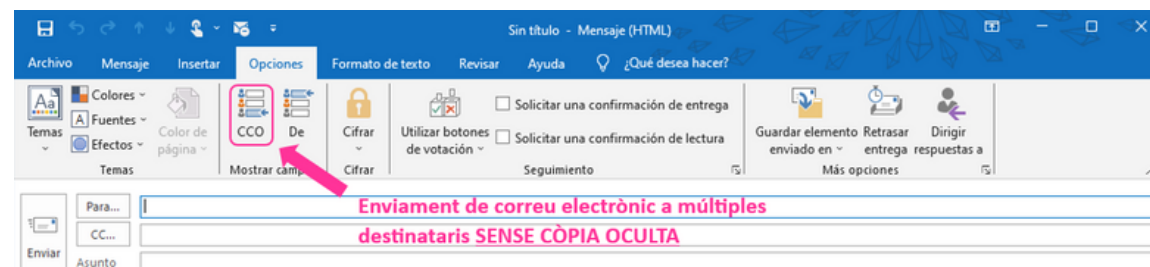
Bloqueig o accés no autoritzat a sistema informàtic



Incendi o inundació d'arxiu



Desfer-se de documents confidencials o amb dades personals sense prèvia destrucció



2. Què hem de fer quan patim o tenim constància d'un incident?



proactivanet



Comunicar-ho de manera immediata al **Servei d'Informàtica**, a través del sistema automatitzat de notificació d'incidències: www.incidencias.dival.es/. Aquest valorarà si es considera un esdeveniment de seguretat a reportar.

Informació a comunicar: data i hora de detecció; persona que ha detectat; descripció breu del succés; sistema, aplicació, arxiu afectats.

En tot cas, siga un incident o bretxa de seguretat, que afecte dades personals, es comunicarà, immediatament, al Delegat de Protecció de Dades pdp@dival.es

3. Què ha de fer la Diputació?

Independentment de les notificacions internes que s'hagen de produir per a gestionar un incident de seguretat, en cas de bretxa o violació, la **Diputació**, sota l'assessorament del **Delegat de Protecció de Dades**, deurà:

1. Notificar a l'Agència Espanyola de Protecció de Dades (AEPD), quan:

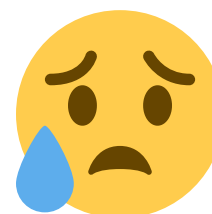
- Risc per als drets i les llibertats de les persones.
- 72 hores després d'haver tingut constància de la bretxa o violació. És per això que ha de comunicar-se amb màxima diligència al Responsable i DPD.

2. Comunicar als **Afectats**, quan:

- Alt risc per als seus drets i llibertats.
- Sense dilació indeguda.

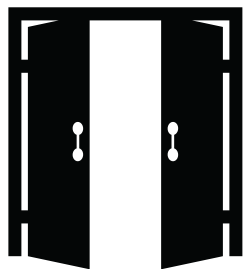


AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



7. Drets en protecció de dades

Accés



La persona titular de les dades pot sol·licitar a la Diputació **saber informació sobre el tractament**, ens altres: quines categories o tipus de dades es tracten; finalitat del tractament; destinataris; d'on s'han obtingut les dades. Ha de distingir-se d'altres drets d'accés (ex.): en qualitat interessat en procediment administratiu; accés informació pública; accés en qualitat d'Edil; a història clínica.

Rectificació



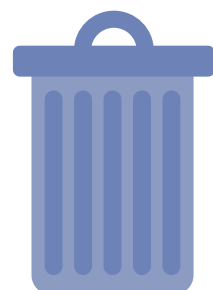
La persona titular de les dades pot sol·licitar a la Diputació la **correcció de les seues dades o es completen**, si són **inexactes o incomplets**.

Oposició



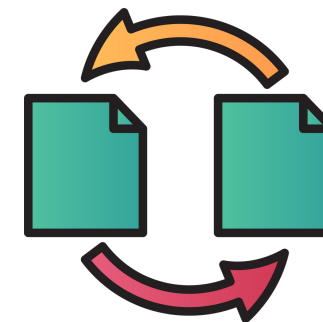
La persona titular de les dades pot sol·licitar a la Diputació l'**oposició al tractament de les seues dades** per motius relacionats amb la seua situació particular.

Supresió



La persona titular de les dades pot sol·licitar a la Diputació l'**eliminació o esborrat de les seues dades** quan: ja no són necessaris; retirada del consentiment; tractament il·lícit; per obligació legal.

Portabilitat



La persona titular de les dades pot sol·licitar **rebre les seues dades** en un format estructurat, d'ús comú i lectura mecànica, per a transmetre'ls a una altra entitat.

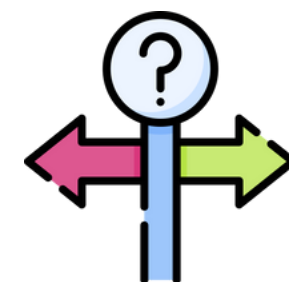
Aquest dret **NO és aplicable** en els tractaments de dades fetes per l'**Administració pública**.

Limitació



La persona titular de les dades pot sol·licitar a la Diputació la **suspensió del tractament** de les seues dades o limitar l'ús d'aquests.

No ser objecte de decisions automatitzades



No ser objecte de **decisiones automatitzades**, com l'elaboració de perfils, **que produïsquen efectes jurídics**.

Qüestions comunes als drets

- Poden exercir-se també per representant legal o voluntari.
- La Diputació ha de donar resposta en el termini d'**1 mes**.
- Davant qualsevol sol·licitud d'aquest tipus pose's en coneixement del Delegat de Protecció de Dades pdp@dival.es

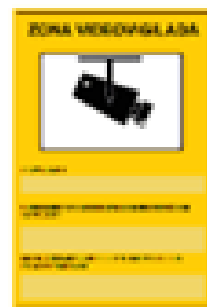


8. Videovigilància



Obligacions relatives al tractament d'imatges de persones físiques mitjançant **sistema de videovigilància** de la Diputació.

La Diputació únicament **utilitza** el sistema de videovigilància **per a preservar la seguretat de persones, béns i instal·lacions**.



1. Deure d'informació.- S'ha d'informar els interessats mitjançant la col·locació de distintius informatius en llocs prou visibles de les zones videovigilades. Al seu torn, s'informarà en document addicional, en espai en línia o codi QR.



2. Supresió.- Les imatges han de suprimir-se en el termini màxim d'**un mes des de la seua captació**. Excepció: enregistrament delictiu o infracció administrativa.



3. Prohibicions. - Captar imatges en la via pública (excepte Forces i Cossos de Seguretat); terrenys i habitatges privats confrontants o de qualsevol altre espai alié; banys, vestuaris o llocs anàlegs.



4. Contractació d'un tercer.- La Diputació ha de triar una empresa de seguretat privada i/o instal·ladora d'aquests sistemes, que ofereixca les garanties suficients. Es formalitzarà un contracte per encàrrec de tractament de dades.



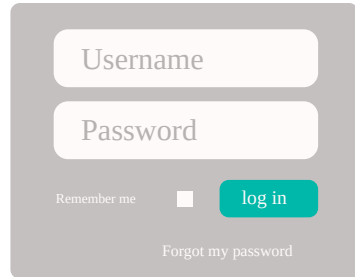
5. Accés a les imatges.- A les imatges gravades accediran només les persones autoritzades. S'han d'adoptar mesures de seguretat que impedisquen l'accés a les imatges per part de personal no autoritzat.



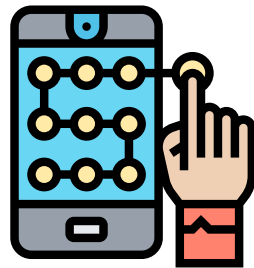
Bloc III

Bones pràctiques en el tractament de les dades per part de les persones usuàries del sistema d'informació

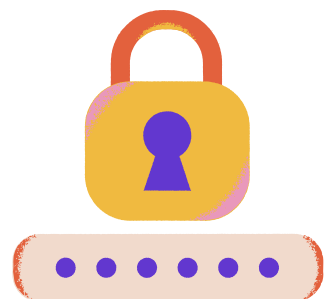
1. Bones pràctiques en el tractament automatitzat (informàtic) de dades personals



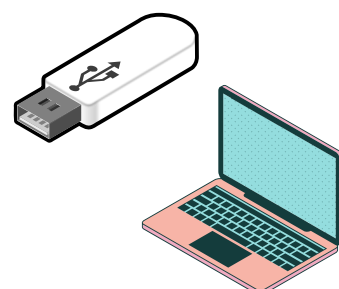
Protegeix les teues **contrasenyes** corporatives d'accés als sistemes d'informació, com si es tractara del PIN de la teua targeta de crèdit o claus d'accés al teu telèfon mòbil.



No utilitzes les **contrasenyes de tu àmbit privat o domèstic** com a claus d'accés al sistema d'informació de la Diputació.



Assegura't de protegir el teu equip quan abandones el teu entorn de treball, mitjançant el **bloqueig d'accés**. No alteres la configuració, física o lògica, dels equips informàtics o de telefonia, ni instal·les programari no autoritzat.



Xifrar els dispositius en els quals obraren dades personals o informació de caràcter confidencial de la Diputació.



Emmagatzema els arxius o fitxers informàtics en els **espais habilitats en el servidor informàtic**, per a poder ser protegits enfront de tercers i efectuar les còpies de seguretat.



Utilitzar el **correu electrònic** i Internet com a **instruments de treball**, únicament per a l'execució de les funcions o tasques assignades.

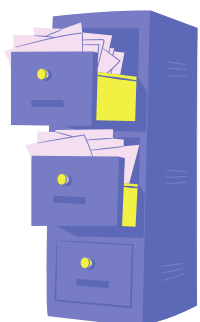


No accedir a correu electrònic, obrir els arxius adjunts o accedir a adreça d'Internet, **sospitós de ser nociu o perjudicial**.



Comunicar de manera immediata al Servei d'Informàtica i Delegat de protecció de dades **pdp@dival.es qualsevol incidència** que afecte la seguretat de les dades.

2. Bones pràctiques en el tractament no automatitzat (paper) de dades personals



Guardar tots els suports o documents que continguin informació de caràcter personal **en un lloc segur**, quan aquests no siguin usats, particularment, fora de la jornada laboral.



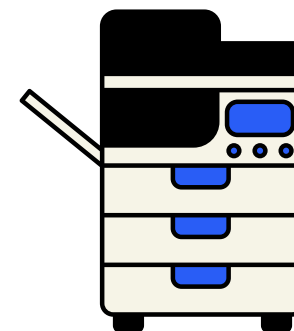
Mantindre degudament **custodiades les claus d'accés** als locals o dependències, despatxos, així com als armaris, arxivadors o altres elements que continga suports o documents en paper amb dades de caràcter personal.



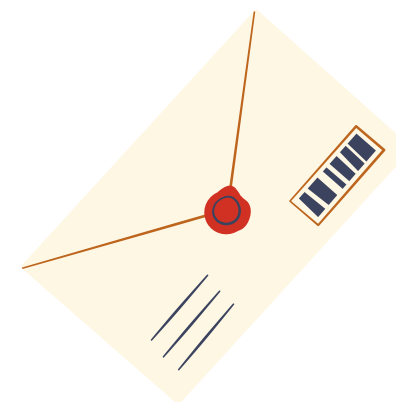
Documents no visibles en els escriptoris, taulells o un altre mobiliari. S'haurà de mantindre la confidencialitat de les dades personals que consten en els documents depositats o emmagatzemats en els escriptoris, taulells o un altre mobiliari.



No tirar suports o documents en paper, on es continguin dades personals, a papereres o contenidors, de manera que pugui ser llegible o fàcilment recuperable la informació.



No deixar en fotocopiadores, faxos o impressores papers amb dades de caràcter personal. Assegurar-se que **no queden documents impresos** que continguin dades personals, **en la safata d'eixida de la fotocopiadora**, impressora o faxos.



Si s'envien a tercers aliens a l'organització alguna **informació sensible**, que pugui contindre categories especials de dades, s'ha de realitzar, en sobre tancat i, en qualsevol cas, tindre present que haja d'efectuar-se per mitjà de **correu certificat** o a través d'una forma de correu ordinari **que permeti la seua completa confidencialitat**.



Comunicar de manera immediata al Delegat de protecció de dades **pdp@dival.es** qualsevol **incidència** que afecte la seguretat de les dades.



 **Diputació
de València** | Protecció de Dades
i Seguretat de la Informació