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

CLASSIFICACIÓ: **NIVELL "B"**

(Artícle 43.2 Reglament de Política de Seguretat i de la Protecció de Dades de Carácter Personal en la Diputació Provincial de València)

PROCEDIMENTS DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

CODI	P/PDP	**APROVACIÓ**	Decret nº 15875, de 27 de desembre de 2022, del President de la Diputació

CONTROL DOCUMENTAL

ELABORAT PER:	REVISAT PER:	APROVAT PER:
	Eusebio Moya López	Antoni Francesc Gaspar
Departament de Protecció de Dades i Seguretat de la Informació	Cap Departament de Protecció de Dades i Seguretat de la Informació	President Diputació de València

HISTÓRICO DEL DOCUMENTO:

Data	Edició	Revisió	Canvis Realitzats
27/12/2022	01	01	Aprovació inicial de la norma

FITXERS: NORMATIVA PDP ***LOCALITZACIÓ:***

DATA D'EMISSIÓ: Desembre 2022

INDEX

INTRODUCCIÓ

L'article 43.2 del Reglament de política de seguretat i de la protecció de dades de caràcter personal en la Diputació Provincial de València estableix que s'hauran d'elaborar un conjunt de procediments tècnics de caràcter obligatori orientats a resoldre les tasques, els processos de treball o les formes d'actuació considerats més rellevants, atés el perjudici que causaria una actuació inadequada de seguretat, desenvolupament, manteniment i explotació dels sistemes d'informació o de protecció de dades de caràcter personal, o per vindre imposats per la legislació aplicable.

Aquest precepte recull expressament com a integrats en el seu mandat els denominats Procediments de Protecció de Dades de Caràcter Personal, i l'article 39.1 atorga la competència per a la seua aprovació al president de la Diputació o el diputat/la diputada en qui aquest delegue.

Per Decret núm. 15875, de 27 de desembre de 2022, el president de la Diputació ha aprovat els presents Procediments de Protecció de Dades de Caràcter Personal.

En aquest document consten els procediments de treball relacionats amb la protecció de dades de caràcter personal de la Diputació de València. D'acord amb l'article 4 del Reglament de política de seguretat i de la protecció de dades de caràcter personal citat, la present normativa és aplicable a tots els departaments i les unitats de la Diputació de València, i resultarà d'obligat compliment en el tractament de les dades personals dut a terme.

1. PROCEDIMENTS DE TREBALL DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

P/PDP-001 PROCEDIMENT PER A LA CREACIÓ I MODIFICACIÓ DEL REGISTRE D'ACTIVITATS DE TRACTAMENT

OBJECTIUS I ABAST

Garantir una coordinació i comunicació adequades entre les diferents parts implicades en la inscripció, modificació i supressió en el Registre de les Activitats de Tractament (d'ara en avant, RAT) de la Diputació de València, amb la finalitat de garantir que s'acompleixen les obligacions establides en la normativa en matèria de protecció de dades.

Estan afectats:

- tots aquells tractaments de dades de caràcter personal de nova creació en la Diputació de València.
- aquells tractaments de dades ja inscrites en el RAT i que patisquen modificacions en la finalitat, en les categories de dades que es tracten o en qualsevol altra informació que haja de fer-se constar en el RAT.
- tots aquells tractaments de dades que deixen d'efectuar-se i que, en conseqüència, han de ser suprimits del RAT.

Entitats de la Diputació de València afectades:

- **El Delegat de Protecció de Dades**, encarregat de supervisar les altes, modificacions i supressions de tractaments en el RAT.

- **Qualsevol àrea o servei de la Corporació obligada a inscriure, modificar o suprimir una activitat de tractament de dades de caràcter personal**. Aquestes unitats, com a centres gestors del tractament (CGT), seran responsables de mantindre actualitzada la informació sobre activitats de tractament existents o la intenció de crear noves activitats que resulten de la seua competència.

DESPLEGAMENT

El CGT responsable en què es detecte la necessitat de crear, modificar o eliminar una activitat de tractament ho realitzarà a través de l'aplicatiu intern de gestió del RAT.

El Delegat de Protecció de Dades assessorarà el CGT en qualsevol qüestió que desitge consultar-se-li durant la creació, la modificació o l'eliminació d'una activitat de tractament en RAT.

El Delegat de Protecció de Dades supervisarà les accions d'alta, modificació o supressió dutes a terme en el RAT i podrà intervindre per a recaptar del CGT informació addicional o interessar qualsevol tipus d'aclariment. D'igual forma, el Delegat de Protecció de Dades podrà comunicar al CGT la no conformitat de l'actuació pretesa o practicada sobre el RAT.

La creació d'una nova activitat de tractament es realitzarà amb un mínim d'un **mes d'antelació** sobre la data en què estiga previst el començament del tractament. Això permetrà disposar d'aquell marge de temps per a adoptar les mesures necessàries per a la seua regularització.

P/PDP-002 PROCEDIMENT PER A L'EXERCICI DELS DRETS ARSOPL

OBJECTIUS I ABAST

Garantir l'exercici dels drets d'accés, rectificació, supressió, oposició, portabilitat i limitació del tractament per part dels titulars de les dades de caràcter personal. Aquest procediment serà comú per a tots els departaments i unitats de la corporació i per a qualsevol tractament/fitxer amb dades de caràcter personal, excepte en aquells supòsits en què les lleis aplicables a determinats tractaments/fitxers establisquen un procediment especial per a la rectificació o supressió de les dades contingudes en aquests, i en aquest cas s'estarà al que es disposa en aquelles.

Estan afectats:

- tots aquells tractaments de dades de caràcter personal el responsable del tractament del qual siga la Diputació de València.
- aquells tractaments de dades de caràcter personal dels quals la Diputació de València siga encarregat del tractament, i respecte dels quals s'haja pactat de manera expressa entre el responsable del tractament i la Diputació que aquesta atendrà, per compte i ordre del primer, els drets ARSOPL.

Entitats de la Diputació de València afectades:

- **El CGT responsable del fitxer/tractament de dades corresponent**. Aquestes unitats seran responsables d'atendre els drets ARSOPL que exerciten els titulars de les dades personals que tracten.

DESPLEGAMENT

1r. Legitimació

L'exercici dels drets ARSOPL té caràcter personalíssim, per la qual cosa únicament podrà sol·licitar-se i dur-se a terme per:

a) L'afectat o interessat (el titular de les dades personals)
b) El representant legal o voluntari de l'afectat o interessat:

- **legal**. Quan l'afectat es trobe en situació d'incapacitat o minoria d'edat que impossibilite l'exercici personal dels drets.
- **voluntari**. Mitjançant expressa designació per a l'exercici del dret.

En qualsevol cas, els titulars de la pàtria potestat podran exercitar en nom i representació dels menors de catorze anys els drets d'accés, rectificació, supressió, oposició o qualssevol altres que pogueren correspondre'ls en el context de la LOPDGDD.

En el cas que l'afectat haja mort, les persones vinculades al difunt per raons familiars o de fet així com els seus hereus podran dirigir-se al responsable o encarregat del tractament a fi de sol·licitar l'accés a les dades personals d'aquell i, si pertoca, la seua rectificació o supressió.

Les persones o institucions a les quals el difunt haguera designat expressament per a això podran també sol·licitar, conformement a les instruccions rebudes, l'accés a les dades personals d'aquest i, si pertoca la seua rectificació o supressió.

En cas de defunció de menors, aquests drets podran exercir-se també pels seus representants legals o, en el marc de les seues competències, pel Ministeri Fiscal, que podrà actuar d'ofici o a instàncies de qualsevol persona física o jurídica interessada.

En cas de defunció de persones amb discapacitat, aquests drets també podran exercir-se, a més de per qui assenyala el paràgraf anterior, per qui haguera sigut designat per a l'exercici de funcions de suport, si tals facultats s'entengueren compreses en les mesures de suport prestades pel designat.

2n. Sol·licitud

La sol·licitud d'exercici de drets ARSOPL podrà efectuar-se a través d'un dels mitjans següents:

a) **Tramitació electrònica**. En la seu electrònica de la Diputació (www.sede.dival.es) es troba en el catàleg de tràmits el denominat “Drets Protecció de dades”, dins de la secció de “Atenció al ciutadà”.

b) **Tramitació en suport paper**. Utilitzant la sol·licitud tipus habilitada per a això, la instància general o qualsevol altre escrit que presente l'interessat.

c) **Tramitació per altres mitjans electrònics o telemàtics**. Mitjançant correu electrònic, mecanismes facilitats en portals web o entorns similars en Internet.

La tramitació a través d'algun dels mitjans dels apartats *a*) o *c*) haurà de reunir les condicions i garanties establides en el Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics, i resta de normativa sobre administració electrònica que siga aplicable. Aquests mitjans disposaran de sistemes que permeten l'establiment de mesures de seguretat d'acord amb el que s'estableix en Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

3r. Requisits

Haurà d'acreditar-se **la legitimitat** per a l'exercici dels drets ARSOPL d'acord amb les especificacions següents:

• les sol·licituds tramitades conforme a l'apartat *a*) del punt 2n. L'acreditació s'ajustarà al que disposa el Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics, així com a les normes que per a aquests procediments s'estableixen en la seu electrònica. L'acreditació en l'actuació per mitjà de representant es realitzarà d'acord amb el que disposa l'article 32 del citat Reial decret 203/2021.
• les sol·licituds tramitades conforme a l'apartat *b*) del punt 2n. L'acreditació es durà a terme:

- mitjançant l'aportació de fotocòpia del DNI, passaport o un altre document vàlid que l'identifique, quan el sol·licite l'interessat mateix.
- quan s'actue mitjançant representant, a més de l'anterior, mitjançant l'aportació dels mateixos documents anteriors

pertanyents al representant legal o voluntari, i dels documents que n'acrediten la representació.

• les sol·licituds tramitades conforme a l'apartat *c*) del punt 2n. L'acreditació es durà a terme mitjançant la validació de l'interessat (login) en el portal web, entorn d'Internet, etc, amb les credencials que s'hagen establit per a l'accés personalitzat o les associades al compte de correu electrònic utilitzat. L'acreditació s'ajustarà al que disposa el Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics. L'acreditació en l'actuació per mitjà de representant es realitzarà d'acord amb el que disposa l'article 32 del citat Reial decret 203/2021.

La sol·licitud **haurà de contindre**, com a mínim:

a. Nom i cognoms de l'interessat i, si pertoca, de la persona que el represente.
b. Petició en què es concreta la sol·licitud (accés, rectificació, supressió, oposició, portabilitat, limitació del tractament).
c. Direcció a l'efecte de notificacions, data i signatura del sol·licitant.
d. Documents acreditatius de la petició que es formula, si pertoca.
e. Quan s'actue mitjançant representant, l'aportació dels documents que acrediten la representació.

A més de l'anterior, si es tracta del **dret d'accés**, s'indicarà:

- El tipus de dades respecte als quals sol·licita l'accés (concrets, totals, d'un fitxer específic...)
- El sistema de consulta pel qual s'opta (còpia, en pantalla, format telemàtic, etc.)

Si es pretén el **dret de rectificació o supressió**:

- Les dades afectades, correcció o supressió que es pretén i, si pertoca, documentació justificativa.

En el cas de l'exercici del **dret d'oposició**:

- En el supòsit de no ser necessari el consentiment, indicació dels motius fundats i legítims que justifiquen l'oposició.

En els supòsits tramitats conforme a l'apartat *c*) del punt 2n, podran obviar-se els requisits citats per a la sol·licitud quan es pose a la disposició de l'interessat, després de la seua validació, l'accés al conjunt de les seues dades i la possibilitat d'exercitar *in situ* la modificació o cancel·lació d'aquests.

En el cas de l'exercici del **dret a la portabilitat**:

• En el supòsit de sol·licitar que les dades es transmeten directament a un altre responsable, indicació de les dades de contacte del responsable destinatari de les dades.

En el cas de l'exercici del **dret a la limitació del tractament:**

• Les dades respecte als que se sol·licita la limitació i, de ser possible, informació sobre la condició necessària per a obtindre la limitació del tractament (impugnació de l'exactitud de les dades personals; il·licitud del tractament i oposició a la supressió; absència de necessitat per als fins del

tractament, però necessitat per a la formulació, exercici o defensa de reclamacions; limitació del tractament mentre es verifica l'oposició sol·licitada).

4t. Procediment

Una vegada rebuda la sol·licitud, es comprovarà que reuneix tots els requisits citats en els punts anteriors. Si mancara algun d'ells, es requerirà el sol·licitant perquè esmene la sol·licitud conforme al que disposa la Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (**LPACAP)** o, si pertoca, Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics. La no esmena en el termini legal comportarà l'arxiu de la sol·licitud.

Si la sol·licitud compleix tots els requisits:

➢ ***sol·licitud d'accés.*** S'haurà de resoldre la sol·licitud.

La resolució expressa podrà:

- Comunicar la inexistència de dades personals de l'afectat.
- Denegar l'accés a l'afectat, en virtut de les causes previstes legalment, tot justificant-ne la denegació.
- Atorgar l'accés, tot acompanyant la informació preceptiva.

➢ ***sol·licituds de rectificació i supressió.*** S'haurà de resoldre la sol·licitud.

La resolució expressa podrà:

- Comunicar la inexistència de dades personals de l'afectat.
- Denegar la rectificació o supressió a l'afectat, en virtut de les causes previstes legalment, tot justificant-ne la denegació.
- Atorgar la rectificació o supressió.

➢ ***sol·licitud d'oposició.*** S'haurà de resoldre la sol·licitud.

La resolució expressa podrà:

- Comunicar la inexistència de dades personals de l'afectat.
- Denegar l'exclusió del tractament, en virtut de les causes previstes legalment, tot justificant-ne la denegació.
- Accedir a la petició, excloent del tractament les dades personals del sol·licitant.

➢ ***sol·licitud de portabilitat.*** S'haurà de resoldre la sol·licitud.

La resolució expressa podrà:

- Comunicar la inexistència de dades personals de l'afectat.
- Denegar la portabilitat de les dades personals, en virtut de les causes previstes legalment, tot justificant-ne la denegació.
- Accedir a la petició, remetent al sol·licitant les dades personals que li incumbisquen, que haguera facilitat a la Diputació de València, en un format estructurat, d'ús comú i lectura mecànica; o si pertoca, transmetent-los a un altre responsable del

tractament, quan l'interessat així ho vulga i siga tècnicament possible.

➢ ***sol·licitud de limitació del tractament.*** S'haurà de resoldre la sol·licitud.

La resolució expressa podrà:

- Comunicar la inexistència de dades personals de l'afectat.
- Denegar la limitació del tractament de les dades personals, en virtut de les causes previstes legalment, tot justificant-ne la denegació.
- Accedir a la petició, i en aquest cas, les dades objecte de limitació únicament podran ser objecte de tractament, amb excepció de la seua conservació, amb el consentiment de l'interessat o per a la formulació, l'exercici o la defensa de reclamacions, o amb la intenció de la protecció dels drets d'una altra persona física o jurídica o per raons d'interés públic important de la Unió o d'un determinat estat membre.

5é . Terminis de resposta

El termini màxim de resolució de les sol·licituds és d'un **mes des de la recepció d'aquelles**.

El termini d'un mes podrà prorrogar-se altres dos mesos en cas necessari, tenint en compte la complexitat i el nombre de sol·licituds. La Diputació de València informarà l'interessat de qualsevol d'aquestes pròrrogues en el termini d'un mes a partir de la recepció de la sol·licitud, tot indicant els motius de la dilació.

Si la Diputació de València no dona curs a la sol·licitud de l'interessat, l'informarà de la recepció de la sol·licitud, de les raons de la seua no actuació i de la possibilitat de presentar una reclamació davant una autoritat de control i d'exercitar les accions administratives i judicials que estime oportunes.

6é. Satisfacció dels drets

Les sol·licituds que resulten estimades comportaran la satisfacció dels drets interessats en els terminis assenyalats en el punt 5é. Per a això, s'actuarà de la manera següent:

➢ ***dret d'accés.*** El dret se satisfà posant en coneixement de l'interessat si les seues dades de caràcter personal estan sent objecte de tractament i, en tal cas, concedint l'accés a les seues dades personals i, si pertoca, a la següent informació: la finalitat del tractament que, si pertoca, s'estiga realitzant, les categories de dades personals de què es tracte, els destinataris o categories de destinataris als quals es van comunicar o seran comunicats les dades, el termini previst de conservació o els criteris per a determinar-lo, l'existència del dret a sol·licitar la rectificació, la supressió, l'oposició o la limitació del tractament de les seues dades, el dret a presentar una reclamació davant una autoritat de control, la informació sobre l'origen de les dades quan no s'hagen obtingut de l'interessat mateix, l'existència de decisions automatitzades, les garanties en cas que es transferisquen dades a un tercer país o organització internacional.

La Diputació de València facilitarà una còpia de les dades personals objecte de tractament. El dret a obtindre còpia no ha d'afectar negativament els drets i llibertats d'uns altres.

La informació que es proporcione a l'interessat ha de donar-se en forma llegible i intel·ligible.

El dret d'accés s'entendrà atorgat si la Diputació de València facilita a l'afectat un sistema d'accés remot, directe i segur a les dades personals que garantisca, de manera permanent, l'accés a la seua totalitat. A tals efectes, la comunicació per la Diputació de València de la manera en què aquest podrà accedir a aquest sistema bastarà per a tindre per atesa la sol·licitud d'exercici del dret. No obstant això, l'interessat podrà sol·licitar de la Diputació de València la informació referida als extrems previstos en l'article 15.1 del Reglament (UE) 2016/679 que no s'incloguera en el sistema d'accés remot (finalitat del tractament, categories de dades, destinataris, etc.).

Quan l'interessat haja presentat la sol·licitud per mitjans electrònics, la informació es facilitarà per mitjans electrònics, quan siga possible, llevat que l'interessat sol·licite que es facilite d'una altra manera. **Es pot considerar repetitiu l'exercici del dret d'accés quan l'interessat el sol·licite en més d'una ocasió durant el termini de sis mesos, llevat que hi haja causa legítima per a això. En cas de repetició, la Diputació de València podrà cobrar un cànon raonable en funció dels costos administratius afrontats o negar-se a actuar respecte de la sol·licitud. La Diputació de València suportarà la càrrega de demostrar el caràcter repetitiu d'aquesta sol·licitud.**

➢ ***drets de rectificació i supressió.*** El dret de rectificació se satisfà practicant la modificació de les dades que resulten ser inexactes o incompletes. El dret de supressió se satisfà suprimint les dades que resulten ser inadequades o excessives, sense perjudici del deure de bloqueig.

➢ ***dret d'oposició.*** El dret d'oposició se satisfà excloent del tractament les dades de caràcter personal afectades.

➢ ***dret a la portabilitat.*** El dret de portabilitat se satisfà facilitant a l'interessat les dades personals que li incumbisquen en un format estructurat, d'ús comú i lectura mecànica o, si pertoca, transmetent les dades a un altre responsable del tractament seleccionat per l'interessat, quan siga tècnicament possible.

➢ ***dret a la limitació del tractament.*** El dret a la limitació del tractament se satisfà limitant el tractament de les dades personals afectades, amb excepció de la seua conservació, a aquell que haguera consentit l'interessat o al necessari per a la formulació, l'exercici o la defensa de reclamacions, o amb la intenció de la protecció dels drets d'una altra persona física o jurídica o per raons d'interés públic important de la Unió o d'un determinat Estat membre. Tot interessat que haja obtingut la limitació del tractament ha de ser informat per la Diputació de València abans de l'alçament d'aquesta limitació.

Es comunicarà qualsevol rectificació o supressió de dades personals o limitació del tractament efectuada a cadascun dels destinataris als quals s'hagen comunicat les dades personals, llevat que siga impossible o exigisca un esforç desproporcionat. La Diputació de València informarà l'interessat sobre aquests destinataris, si aquest així ho sol·licita.

7é. Reclamacions i recursos

El procediment per a l'exercici dels drets ARSOPL és un procediment especial. Les normes del procediment administratiu comú contingudes en la **LPACAP** són d'aplicació subsidiària. Això suposa:

• Les resolucions (expresses o presumptes) sobre sol·licituds de drets ARSOPL esgoten la via administrativa davant la Diputació i l'interessat pot interposar la reclamació davant l'autoritat de control competent en matèria de protecció de dades**,** sense perjudici que interpose qualsevol altre recurs que estime procedent.

• Als actes de tràmit o les resolucions que desestimen una sol·licitud sense entrar en el fons de la petició (falta d'esmena en termini, manca de legitimació, etc.) els serà aplicable el règim general sobre recursos de la **LPACAP**.

8é. Constància

Haurà de deixar-se constància de totes les actuacions dutes a terme en relació amb l'exercici dels drets ARSOPL, amb independència de les característiques del fitxer o tractament de les dades (automatitzat, en paper, mixt), de les vies utilitzades per a l'exercici i dels resultats.

9é. Especialitats en el tractament de dades personals mitjançant dispositius de captació d'imatges i sons

Per la seua pròpia naturalesa, en el tractament de dades personals a través de dispositius de captació d'imatges i sons **únicament cal exercitar els drets d'accés, supressió i limitació**.

Quan se sol·liciten aquests drets es procedirà d'acord amb les especialitats següents:

➢ ***dret d'accés.*** A la documentació que acompanye la sol·licitud d'accés haurà d'adjuntar-se una imatge recent de l'interessat, en la qual se l'identifique perfectament.

La facilitació del dret d'accés no suposarà proporcionar a l'interessat el visionat dels enregistraments, perquè això podria comportar la vulneració dels drets de tercers. El personal que resulte autoritzat per la normativa interna de protecció de dades serà qui visualitze les imatges captades corresponents i, si pertoca, realitzarà un informe descrivint amb detall aquelles imatges en les quals puga identificar-se l'afectat i traslladarà l'informe a l'interessat. Únicament en aquells casos en què l'estat de la tecnologia ho permeta, sense implicar grans esforços i recursos, i les circumstàncies de les imatges captades no afecten drets de tercers, podrà facilitar-se puntualment l'accés visual als enregistraments.

➢ ***dret a la limitació del tractament.*** El dret a la limitació serà exercitable en l'únic sentit de conservar els arxius més enllà del termini de conservació, quan el tractament de dades siga il·lícit i l'interessat s'opose a la supressió de les seues dades i sol·licite en el seu lloc la limitació del seu ús, o quan la Diputació ja no necessite les dades per als fins del tractament però l'interessat sí que els necessite per a la formulació, l'exercici o la defensa de reclamacions.

➢ ***dret de supressió.*** No serà procent accedir a la sol·licitud de supressió d'imatges i/o sons que es troben en situació de bloqueig per les raons indicades en la normativa interna de protecció de dades.

P/PDP-003 PROCEDIMENT PER A GARANTIR L'EXACTITUD I ACTUALITAT DE LES DADES PERSONALS

OBJECTIUS I ABAST

Garantir que les dades de caràcter personal siguen exactes i posades al dia, de manera que responguen de manera veraç a la situació actual dels seus titulars i a la vigència del seu tractament. Es pretén establir mecanismes que permeten a la Diputació complir amb el deure de mantindre “d'ofici” l'exactitud, actualitat i pertinència de tractament respecte de les dades de caràcter personal dels quals resulte “responsable del tractament”, així com d'aquells altres que en qualitat d’“encarregat del tractament” comporte l'obligació de mantindre l'exactitud, l'actualitat i la vigència de les seues dades.

Estan afectats:

- tots aquells tractaments de dades de caràcter personal el “responsable del qual del tractament” siga la Diputació de València.
- aquells tractaments de dades de caràcter personal dels quals la Diputació de València siga “encarregat del tractament”, i la prestació del qual comporte l'obligació de mantindre l'exactitud, l’actualitat i la vigència de les dades.

Entitats de la Diputació de València afectades:

- **Qualsevol àrea o servei de la corporació que duga a terme el tractament amb dades de caràcter personal**. Aquestes unitats seran responsables d'assegurar l'exactitud, l’actualitat i la vigència de les dades personals.

DESPLEGAMENT

La diversitat en l'origen, maneres d'obtenció, tipologia, transformació, comunicació i finalitats de les dades de caràcter personal, entre altres, condicionen les actuacions per a aconseguir l'objectiu d'assegurar l'exactitud, l'actualitat i la vigència de les dades. Per això, les directrius següents hauran d'adequar-se per cada àrea afectada a la realitat del fitxer o tractament del qual resulte responsable.

• Sempre que resulte factible —atés l'esforç, recursos implicats i la possibilitat legal— s'haurà de procedir de manera periòdica i sistemàtica a traslladar als afectats la informació que es disposa d'ells amb el propòsit que puguen manifestar-ne l'exactitud i practicar, si pertoca, les modificacions pertinents. Quan les dades provinguen de tercers, per estar obligats a facilitar-los, se'ls inclourà com a destinataris. Es procurarà que aquests processos es realitzen, com a mínim, una vegada a l'any.

• Quan l'origen de les dades siguen fonts d'accés públic, s'establiran rutines que constaten periòdicament la vigència i, si pertoca, l'exactitud d'aquestes fonts. En aquest punt, s'ha de tindre en compte que ha desaparegut, en la normativa actual de protecció de dades, la referència a les "fonts accessibles al públic" com a causa de legitimació del tractament sense necessitat de consentiment. En l'actualitat, fins i tot en aquests casos, haurà de concórrer alguna de les causes legitimadores establides en la normativa de protecció de dades.

• Quan les dades provinguen d'altres administracions públiques s'intentarà, dins del marc legal, formalitzar acords que faciliten l'actualització i la vigència

de la informació, i s'ha de canalitzar preferentment mitjançant solucions tecnològiques d'interoperabilitat.

• Hauran de ser revisades periòdicament les dades de caràcter personal que cada unitat publique o difonga en Internet, en els llocs web i altres canals electrònics o telemàtics, amb independència que la titularitat d'aquests entorns corresponga o no a la Diputació de València. Es prestarà especial atenció a la vigència d'aquestes dades en aquests entorns, tot eliminant aquelles que hagen complit l'objecte de la seua publicitat; per a això, el **responsable de la informació** determinarà el marc temporal de vigència prèviament a la publicació o difusió de les dades.

• Quan es comuniquen dades personals a tercers en virtut d'una relació de prestació de serveis (encarregat del tractament), s'asseguraran els mecanismes perquè aquestes dades siguen objecte de les accions d'actualització i vigència. En qualsevol cas, s'evitarà que en supòsits de redundància unes mateixes dades oferisquen informació diferent.

P/PDP-004 PROCEDIMENT PER A GARANTIR LA NORMALITZACIÓ INFORMATIVA EN SEU ELECTRÒNICA, LLOCS WEB O ESPAIS EN INTERNET

OBJECTIUS I ABAST

Assegurar el compliment de l'article 17 del Reglament de Política de Seguretat i de la Protecció de Dades de Caràcter Personal en la Diputació Provincial de València, que estableix l'obligació que, tant la Seu Electrònica de la Diputació de València com qualsevol espai en Internet o tecnologies similars dels

continguts de les quals siga responsable la corporació, continga una referència al Registre d'Activitats de Tractament, les polítiques i normatives internes sobre protecció de dades de caràcter personal i, en particular, dels drets que assisteixen els titulars de les dades.

Estan afectats:

- la Seu Electrònica de la Diputació de València i qualsevol espai en Internet o tecnologies similars dels continguts de les quals siga responsable la corporació.

Entitats de la Diputació de València afectades:

- **El Servei d'Informàtica de la corporació**. Aquest servei serà responsable d'assegurar el compliment respecte de la Seu Electrònica, el portal web corporatiu i qualsevol espai en Internet o tecnologies similars l'administració directa de les quals porte.

- **Qualsevol àrea o servei de la corporació que administre directament qualsevol espai en Internet o tecnologies similars**. Aquestes unitats seran responsables d'assegurar el compliment respecte d'aquests espais.

DESPLEGAMENT

• En el supòsit de la Seu Electrònica, el portal web corporatiu i qualsevol espai en Internet o tecnologies similars l'administració directa de les quals porte el **Servei d'Informàtica**, el citat Servei implementarà i mantindrà actualitzades les pertinents referències de les polítiques i normatives internes sobre protecció de dades de caràcter personal i, en particular, dels drets que assisteixen els

titulars de les dades, utilitzant per a això les plantilles i referències documentals posades a disposició pel Departament de Protecció de Dades i Seguretat de la Informació.

• En la resta de supòsits, serà el **responsable de l'àrea o servei** que administre directament aquests espais qui implementarà i mantindrà actualitzades les pertinents referències de les polítiques i normatives internes sobre protecció de dades de caràcter personal i, en particular, dels drets que assisteixen els titulars de les dades, utilitzant per a això les plantilles i referències documentals posades a disposició pel Departament de Protecció de Dades i Seguretat de la Informació.

Està prohibit posar en servei qualsevol dels espais tecnològics referits sense que continga els requisits esmentats.

P/PDP-005 PROCEDIMENT PER A la GESTIÓ I NOTIFICACIÓ DE BRETXES DE SEGURETAT

OBJECTIUS I ABAST

Es descriu el procediment operatiu a seguir per a la gestió i notificació, si pertoca, a l'AEPD i als afectats, de les bretxes de seguretat que afecten dades personals, és a dir, quan implique destrucció, pèrdua, alteració, comunicació o accés no autoritzat a dades personals, i que permeta a l'organització respondre de manera ràpida, ordenada i eficaç a l'esdeveniment, minimitzant-ne les conseqüències sobre la mateixa organització i terceres parts implicades. Afecta a tots aquells esdeveniments que esdevinguen en la Diputació de València o

per compte d'un encarregat del tractament, en els quals pogueren veure's afectades la confidencialitat, la integritat o la disponibilitat de dades personals.

Queden afectats per aquest procediment:

- Totes aquelles dades personals la confidencialitat de les quals, integritat o disponibilitat pogueren veure's afectades per l'esdeveniment de seguretat.

Entitats de la Diputació de València que podrien veure's afectades:

- L'àrea **o servei de la corporació que detecte l'incident o que es veja afectat** per aquest.
- El **Servei d'Informàtica** de la corporació.
- El **Departament de Protecció de Dades i Seguretat de la Informació.**
- El **Delegat de Protecció de Dades.**
- **Si pertoca, responsables, encarregats, titulars de les dades i altres figures** que es determinen.

DESPLEGAMENT

El procediment d'actuació inclou les següents fases:

1r. Detecció, comunicació, identificació i classificació

1.A Detecció i comunicació

La detecció d'esdeveniments de seguretat de dades personals pot produir-se a través de fonts externes o internes:

• **Fonts externes:** Proveïdors de serveis informàtics, proveïdors de serveis de telecomunicacions, proveïdors de serveis de seguretat, entitats públiques: Instituto Nacional de Ciberseguridad (INCIBE), Centro Criptológico Nacional (CCN), CSIRT-CV (Centre d'Alerta i Resposta d'Incidents de Seguretat de la CV), Forces i cossos de seguretat de l'estat, etc.

• **Fonts internes:** Els usuaris dels sistemes d'informació de la Diputació o els mateixos sistemes interns de monitoratge: antivirus, analitzadors de logs, monitoratge de servidors o trànsits de xarxa, etc.

Amb independència de la persona que detecte l'esdeveniment, serà comunicat immediatament al responsable designat a aquest efecte, qui valorarà si es considera un esdeveniment de seguretat que s'haja de reportar com a tal.

Les dades mínimes de l'esdeveniment a emplenar per escrit seran:
• Data i hora de la detecció.
• Persona que ho ha detectat.
• Naturalesa de l'esdeveniment de seguretat de les dades personals.
• Descripció breu.
• Sistema afectat.

La comunicació dels fets es realitzarà preferentment a través del sistema automatitzat de notificació d'incidències existent a cada moment en la corporació, i s'habilitarà un ítem específic.

1.B Identificació i registre

L'anàlisi de les fonts d'informació abans esmentades permetrà determinar si s'està davant un incident de seguretat o no, així com la seua naturalesa, classe, tipus, si aquest incident ha afectat dades de caràcter personal i per tant constitueix una "bretxa de seguretat de les dades de caràcter personal" descrita en la normativa de protecció de dades i el nivell de risc al qual s'enfronta l'organització.

S'haurà de mantindre un registre documental dels incidents de seguretat, incloent-hi el tipus d'incident, descripció d'aquest, gravetat, estat i mesures adoptades per a la seua resolució.

1.C Anàlisis i classificació

Una vegada registrat l'incident de seguretat i recopilada la informació disponible en primera instància, el responsable designat a aquest efecte realitzarà una primera classificació: incident de seguretat o bretxa de seguretat.

- **Incident de seguretat:** qualsevol esdeveniment que afecte o impacte en les dimensions de la seguretat (Confidencialitat, Integritat, Disponibilitat, Traçabilitat o Autenticitat) ha de ser considerat almenys com un incident de seguretat de dades personals sempre que afecte un sistema d'informació que

continga aquestes dades personals, encara que l'impacte siga molt reduït i els inconvenients puguen ser esmenats ràpidament.

- **Bretxa de seguretat:** considerarem que un incident de seguretat és una *Bretxa de seguretat* quan ocasione la destrucció, la pèrdua o l'alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o accés no autoritzat a aquestes dades.

En cas que es tracte d'una bretxa de seguretat, és imprescindible avaluar el nivell de perjudici que pot causar als drets i llibertats dels afectats, determinant amb el major grau de precisió possible el nivell de severitat de les conseqüències per als individus. És així mateix imprescindible determinar si es tracta d'una bretxa de confidencialitat, integritat o disponibilitat, categoria i nombre d'afectats, categoria i nombre de registres de dades, etc.

En tots dos casos (incident o bretxa), es comunicarà immediatament al delegat de protecció de Dades, qui farà un seguiment a l'efecte d'emplenar, si pertoca, el deure de notificació en termini a l'autoritat de control i, si fora necessari, als titulars de les dades personals afectades.

2n. Resposta a l'incident

2.A Contenció

Durant el procés de resposta, en una primera fase s'intentarà contindre l'incident. Una part essencial de la contenció és la presa de decisions ràpides com pot ser tancar un sistema, aïllar-lo de la xarxa, deshabilitar unes certes funcions, etc.

2.B Solució

Després de l'aplicació de les mesures de contenció, es prendran les mesures correctores o d'erradicació necessàries i es verificarà el funcionament correcte d'aquestes, confirmant-ne la idoneïtat per a l'eliminació de l'incident.

S'ha de considerar també si les mesures aplicades són de caràcter temporal o si formen part d'una solució definitiva, i el sistema i/o la informació afectada ha tornat de nou de manera efectiva al seu estat original.

2.C Recuperació

Solucionat l'incident o la bretxa de seguretat i verificada l'eficàcia de les mesures adoptades, s'entrarà en la fase de recuperació, que té com a objectiu el restabliment del servei íntegrament, confirmant-ne el funcionament normal i evitant en la mesura que siga possible que succeïsquen nous incidents basats en la mateixa causa.

2.D Evidències

S'hauran de recaptar totes les evidències disponibles amb la informació generada pels sistemes involucrats en l'incident o bretxa de seguretat.

2.E Comunicació

La comunicació és fonamental durant tot el cicle de vida del procés de resposta, i ha de fer-se d'una manera contínua de manera que es tinga visibilitat clara tant de l'incident com de les accions preses per a afrontar-lo. És

especialment important quan l'incident transcendeix el perímetre de la Diputació i pren rellevància pública.

Els responsables de gestionar l'incident o bretxa de seguretat mantindran permanentment informat de totes les actuacions el delegat de Protecció de Dades.

2.F Informe de resolució

L'elaboració de l'informe de resolució té com a objectiu servir com a base de coneixement. Aquest s'ha de presentar en forma de línia temporal, de manera que facilite el seguiment de les diferents accions, i hauria d'incloure almenys informació relativa als següents apartats:

- Abast i impacte de l'incident.
- Controls preventius existents.
- Accions de resposta preses sobre les diferents alternatives considerades per a la resolució de la bretxa.
- Accions preses per a la prevenció de futures bretxes.
- Impacte en la resolució de l'incident de les accions de resposta preses.
- Accions definides per al seguiment.

S'haurà de comunicar l'informe de resolució al delegat de protecció de dades. Amb independència de l'informe de resolució implementat pels responsables de gestió de l'incident de seguretat, el delegat de protecció de dades emetrà un informe propi en el qual reflectirà les seues conclusions sobre tots els fets i actuacions dutes a terme, especialment sobre les possibles causes de l'incident, l'impacte sobre els drets i llibertats dels afectats i sobre la corporació, la gestió de l'incident i la identificació dels possibles responsables si pertoca. El

delegat elevarà el seu informe a la Presidència de la corporació i l'incorporarà a la seua Informe/Memòria anual corresponent.

3r. Procés de notificació

Independentment de les notificacions internes que s'hagen de produir per a gestionar un incident de seguretat, la Diputació de València haurà de notificar a:

3.A l'autoritat de control en protecció de dades

En cas de bretxa de la seguretat de les dades personals, la Diputació de València haurà de notificar a l'autoritat de control competent sense dilació indeguda i, de ser possible, a tot tardar 72 hores després que haja tingut constància d'ella, llevat que siga improbable que aquesta bretxa de la seguretat constituïsca un risc per als drets i les llibertats de les persones físiques. El termini de 72 hores comença a calcular-se des de l'instant en què es tinga constància que l'incident de seguretat ha afectat dades personals, incloent-hi les hores transcorregudes durant caps de setmana i dies festius.

S'establirà la metodologia i es facilitaran les eines necessàries per a poder valorar la procedència de la comunicació de la bretxa a l'autoritat de control.

En cas que es determine la procedència de notificar a l'autoritat, la notificació es realitzarà a través del formulari destinat a aquest efecte en la Seu Electrònica de l'Agencia Española de Protección de Datos (AEPD): “Notificació de bretxes de seguretat de les dades personals (art. 33 RGPD)” o pel que assenyale l'autoritat de control autonòmica, si pertoca.

En la notificació, es proporcionarà la informació següent:

· Dades identificatives i de contacte de l'entitat/responsable del tractament.
· Dades identificatives i de contacte de l'encarregat del tractament, en cas que estiguera implicat en la bretxa.
· Dades identificatives i de contacte del delegat de Protecció de Dades.
· Dades de la notificació: indicar si es tracta d'una nova bretxa de dades personals o de la modificació d'una notificació feta amb anterioritat.
·Informació sobre el tractament: des de quan es realitza; nombre aproximat de persones físiques sobre les quals es tracten dades; àmbit geogràfic.
· Informació sobre la bretxa i les seues conseqüències: accidental/intencionat; origen de l'incident; com ha ocorregut la bretxa; dimensions afectades; en cas de bretxa de confidencialitat, si les dades estaven protegides; en cas de bretxa de disponibilitat, si s'ha recuperat la disponibilitat de les dades personals; en cas de bretxa d'integritat, si les dades han sigut alterats i usats de manera il·legal; possibles conseqüències sobre les persones físiques i grau d'afectació; constància que s'hagen materialitzat les conseqüències identificades; resum de la bretxa.
· Tipus de dades afectades.
· Perfil de les persones afectades (menors, membres de col·lectius vulnerables, altres perfils) i nombre de persones afectades.
· Implicacions transfrontereres.
· Mesures de seguretat adoptades abans de la bretxa.
· Accions preses després de l'incident
· Comunicació als afectats
· Documentació adjunta
· Indicació de si es tracta d'una notificació completa o inicial.

Si en el moment de la notificació no fora possible facilitar tota la informació, podrà facilitar-se posteriorment, de manera gradual en diferents fases. La primera notificació es realitzarà en les primeres 72 hores i almenys es realitzarà una comunicació final o de tancament quan es dispose de tota la informació relativa a l'incident.

Quan es realitze la primera notificació, s'haurà d'informar si es proporcionarà més informació a posteriori. També es podrà aportar informació addicional mitjançant comunicacions intermèdies a l'autoritat de control sota petició d'aquesta, o quan es considere adequat actualitzar la situació d'aquesta.

Abans del termini màxim de 30 dies hàbils des de la notificació inicial, s'haurà de completar tota la informació mitjançant una “modificació” de la notificació anterior, inclosa la decisió presa sobre la comunicació de la bretxa de dades personals als afectats.

Quan la notificació inicial no siga possible en el termini de 72 hores, la notificació haurà de realitzar-se igualment, i s’hi hauran de constar i justificar els motius de la dilació.

A manera de contingència, en cas de no estar disponible el servei electrònic de l'AEPD, s'haurà de contactar amb l'Agencia, en el número de telèfon o una altra via de contacte establida en el seu portal web, i acordar el canal alternatiu pel qual realitzar la notificació.

A cada notificació se li assignarà una referència que s'haurà de mantindre i incloure en les successives comunicacions relacionades, si n'hi haguera, amb la finalitat de proporcionar un seguiment complet de l'incident.

Les notificacions de bretxes de seguretat davant l'autoritat de control seran dutes a terme pel Delegat de protecció de dades.

3.B Els afectats

Quan siga probable que la bretxa de seguretat de dades personals comporte un alt risc per als drets i les llibertats de les persones físiques, es comunicarà a l'afectat sense dilació indeguda.

S'establirà la metodologia i es facilitaran les eines necessàries per a poder valorar la procedència de la comunicació de la bretxa als interessats.

Així mateix, la bretxa haurà de ser comunicada als afectats a sol·licitud de l'autoritat de control competent.

La comunicació serà realitzada en un llenguatge clar i senzill i haurà de contindre, com a mínim, la informació següent:

• Dades de contacte del delegat de Protecció de Dades.
• Descripció general de l'incident i moment en què s'ha produït.
• Les conseqüències possibles de la bretxa de la seguretat de les dades personals.
• Descripció de les dades i informació personal afectades.
• Resum de les mesures implantades fins al moment per a controlar els possibles danys.

• Altres informacions útils als afectats per a protegir les seues dades o previndre possibles danys.

La notificació s'haurà de realitzar, preferentment, de manera directa a l'afectat; ja siga per telèfon, correu electrònic, correu postal o a través de qualsevol altre mitjà dirigit a l'afectat que es considere adequat.

L'àrea o departament responsable de les dades implicades, en coordinació amb el Servei d'Informàtica, durà a terme les notificacions als afectats.

4t. Seguiment i tancament

Aquesta fase té per objectiu solucionar possibles deficiències en la gestió d'incidents i incorporar millores que permeten una millor resposta en les execucions següents. Ha de servir per tant per a:

• Depurar errors o actualitzar informació que s'haja evidenciat obsoleta.
• Detectar mecanismes nous de control que puguen ser necessaris o millorar els ja existents, i modificar si pertoca les mesures tècniques i organitzatives definides en la fase de preparació.
• Revisar l'eficàcia del procés de gestió d'incidents.
• Analitzar la informació que encara estiga pendent de processar i que puga aportar millores.
• Comunicar els resultats del procés i realitzar una valoració final de l'incident que s'afija a l'informe de resolució per al tancament.

P/PDP-006 PROCEDIMENT D'ANÀLISI DE RISCOS

OBJECTIUS I ABAST

Analitzar els riscos dels tractaments de dades que duu a terme la Diputació de València, amb la finalitat d'establir mesures de seguretat adequades per a garantir els drets i llibertats de les persones físiques les dades personals de les quals són tractats per la Diputació.

Estan afectats:

- Tots aquells tractaments de dades de caràcter personal el “Responsable del qual del Tractament” o “Encarregat del tractament” siga la Diputació de València.

Entitats de la Diputació de València afectades:

- El **Centre Gestor del tractament de dades (CGT)**.
- El **Servei d'Informàtica**.
- El **Departament de Protecció de Dades.**

DESPLEGAMENT

1r. Descripció de les operacions d'activitats de tractament

S'haurà d'efectuar una descripció dels tractaments subjectes a l'anàlisi de riscos, cosa que permetrà obtindre un coneixement del cicle de vida de les dades, de les activitats realitzades i de qualsevol element que hi intervé. Les

activitats de tractament es podran agrupar per processos comuns exposats a riscos similars.

La descripció dels tractaments i les activitats que comporten ha de ser emplenada pel CGT corresponent i podrà implicar més d'un CGT. La descripció de l'entorn tecnològic en el qual es desenvolupen les activitats de tractament ha de ser emplenada, si pertoca, pel Servei d'Informàtica.

2n. Gestió de riscos

L'adequada gestió de riscos requereix un procés d'identificació, avaluació i tractament dels riscos als quals està exposat cada activitat de tractament o cada procés comú exposat a riscos similars.

Una vegada identificats els riscos inherents a l'activitat de tractament de partida, s'aplicaran mesures de seguretat i control que reduïsquen el seu nivell d'exposició. Per a cadascun dels riscos identificats, s'hauran d'establir tantes mesures de seguretat com siguen necessàries per a garantir un nivell de seguretat i control adequat que reduïsca l'exposició al risc.

La Diputació de València establirà la metodologia i facilitarà les eines necessàries per a poder efectuar l'anàlisi de riscos.

Els riscos identificats i les mesures de control definides hauran de documentar-se, amb l'objectiu d'evidenciar l'avaluació de riscos realitzada i tindre una base de treball davant futures revisions de l'anàlisis derivades de canvis en les activitats de tractament.

Finalment, atés que els riscos són variables i poden canviar davant variacions en les activitats de tractament, s'ha de garantir una gestió de riscos adequada mitjançant el monitoratge continu dels riscos i l'avaluació periòdica de l'efectivitat de les mesures de control definides per a reduir el nivell d'exposició al risc. Per tant, es revisarà l'anàlisi de riscos realitzat davant qualsevol canvi significatiu en les activitats de tractament que puga derivar en l'aparició de riscos nous.

L'avaluació dels riscos associats als tractaments de dades personals haurà de ser complementada amb les disposicions internes relatives a l'avaluació de riscos dels sistemes d'informació.

El Departament de Protecció de Dades i Seguretat de la Informació prestarà assessorament en les activitats destinades a l'avaluació de riscos dels tractaments de dades personals.

P/PDP-007 PROCEDIMENT PER A L'AVALUACIÓ D'IMPACTE DE PROTECCIÓ DE DADES (AIPD)

OBJECTIUS I ABAST

Identificar en quins supòsits és necessari dur a terme una Avaluació d'Impacte de Protecció de Dades i, si pertoca, les consideracions a tindre en compte perquè aquesta Avaluació es duga a terme satisfactòriament.

Estan afectats:

- Tots els tractaments de dades de caràcter personal el "responsable del tractament" del qual siga la Diputació de València, en particular aquells que utilitzen noves tecnologies i que, per la seua naturalesa, abast, context o fins, comporten un alt risc per als drets i llibertats de les persones físiques.

Entitats de la Diputació de València afectades:

- El **Centre Gestor del tractament de dades (CGT).**
- El **Servei d'Informàtica**, si pertoca**.**
- El **Delegat de Protecció de Dades.**
- El **Departament de protecció de Dades i Seguretat de la informació**

DESPLEGAMENT

El **Departament de Protecció de Dades i Seguretat de la Informació** establirà la metodologia i facilitarà les eines necessàries per a poder dur a terme l'anàlisi de necessitat i, si pertoca, la EIPD.

El **Delegat de Protecció de Dades** oferirà l'assessorament que se li sol·licite sobre l'avaluació d'impacte relativa a la EIPD i en supervisarà l'aplicació.

Cada **CGT** és responsable de dur a terme l'anàlisi de necessitat de realitzar la EIPD, executar la EIPD en cas de resultar necessari i posar en coneixement del Delegat de protecció de dades el resultat de les anteriors.

El **Servei d'Informàtica** durà a terme l'anàlisi dels elements tecnològics del tractament que incidisquen en la valoració de l'impacte.

1r. Anàlisi de la necessitat de realitzar EIPD

La normativa en matèria de protecció de dades exigeix dur a terme una Avaluació d'Impacte en la Protecció de Dades (d'ara en avant, EIPD) per a tot aquell tractament nou que probablement comporte per la seua naturalesa, abast, context o finalitats, un risc alt per als drets i llibertats de les persones físiques. **Les EIPD hauran de dur-se a terme abans de posar en marxa el tractament.**

Per a analitzar si una activitat de tractament requereix EIPD de manera prèvia a posar en marxa aquest tractament, es tindran en compte la finalitat del tractament, les categories i el volum de dades que es recull, la duració i l'extensió geogràfica del tractament, així com les operacions de tractament de les quals seran objecte, especialment si es tracta de tractaments automatitzats com ara l'elaboració de perfils.

Naturalesa del tractament: S'han de valorar les característiques més bàsiques del tractament i veure si aquestes poden implicar un risc alt.

Abast del tractament: S'han de valorar els efectes o les conseqüències del tractament, identificant fins a quin punt pot arribar i si aquest pot suposar un risc alt.

Context del tractament: S'ha de valorar el conjunt de circumstàncies sota les quals es realitzaran les activitats de tractament, amb l'objectiu de verificar si poden suposar un risc alt.

Finalitats del tractament: S'han d'identificar cadascuna de les finalitats del tractament i analitzar si aquestes deriven en un risc alt.

En qualsevol cas, serà obligatori realitzar una EIPD quan concórrega alguna de les causes següents:

- Avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques que es base en un tractament automatitzat, com l'elaboració de perfils, i sobre la base dels quals es prenguen decisions que produïsquen efectes jurídics per a les persones físiques o que els afecten significativament de manera similar;
- Tractament a gran escala de categories especials de dades i dades relatives a condemnes i infraccions penals.
- Observació sistemàtica a gran escala d'una zona d'accés públic.

Així mateix, es tindran en compte les possibles llistes de tractaments que requereixen EIPD que l'Agencia Española de Protección de Datos puga publicar una llista de tractaments, així com unes altres per a les activitats de tractament en les quals no seria necessari.

El CGT que vulga dur a cap el tractament procedirà prèviament a la realització de l'anàlisi de necessitat mitjançant les utilitats habilitades per a tal fi pel Departament de Protecció de Dades i Seguretat de la Informació. L'anàlisi de necessitat i el seu resultat serà comunicat al delegat de protecció de dades.

El resultat de l'anàlisi de necessitat determinarà l'obligació o no d'executar una EIPD.

2n. Realització de la EIPD

En cas que el resultat de l'anàlisi de necessitat determine l'obligació de realitzar una EIPD.

La EIPD haurà de contindre, com a mínim:
Una descripció sistemàtica de l'activitat de tractament prevista.
Una avaluació de la necessitat i proporcionalitat de les operacions de tractament respecte a la seua finalitat.
Una avaluació dels riscos.
Les mesures de seguretat previstes per a mitigar els riscos i garantir la protecció de les dades personals.
El CGT corresponent procedirà a la realització de la EIPD mitjançant les utilitats habilitades per a tal fi pel Departament de Protecció de Dades i Seguretat de la Informació.

Si fora necessari avaluar aspectes o parts del tractament de dades que foren competència o de coneixement d'altres unitats diferents al CGT, el CGT indicarà quins són els citats aspectes o parts del tractament i la unitat interna afectada, a la qual se li comunicarà per a l'avaluació específica. Especialment, es comunicarà al Servei d'Informàtica sempre que hi haja aspectes o elements de caràcter tecnològic que hagen de ser objecte de l'avaluació.

La EIPD i el seu resultat seran comunicats al delegat de protecció de dades.

3r. Consulta prèvia a l'autoritat de control

Si després d'haver realitzat la EIPD, el resultat de la mateixa determina que el tractament comporta un risc alt per als drets i llibertats dels interessats si el responsable no pren mesures per a per a mitigar-lo, serà necessari elevar consulta a l'autoritat de control competent abans dur-ho a terme.

El delegat de protecció de dades realitzarà la consulta, que haurà d'incloure el següent:

Les responsabilitats respectives del responsable del tractament, els corresponsables i els encarregats del tractament implicats en el tractament.

Les finalitats i els mitjans del tractament.

Les mesures i les garanties establides per a protegir els drets i les llibertats dels interessats.

Les dades de contacte del delegat de Protecció de Dades.

L'avaluació d'impacte.

Qualsevol altra informació a sol·licitud de l'autoritat de control.

La comunicació es durà a terme a través del canal habilitat a aquest efecte per l'Agencia Española de Protección de Datos en la seua Seu Electrònica: “Consulta prèvia a l'inici de tractaments de risc alt (art. 36 RGPD)”.

Si l'autoritat de control considera que el tractament previst podria infringir el RGPD, en particular quan el responsable no haja identificat o mitigat prou el risc, ha d'assessorar en un termini de huit setmanes des de la sol·licitud de la consulta. Aquest termini podrà prorrogar-se sis setmanes, en funció de la complexitat del tractament previst. L'autoritat de control informarà el responsable i, si pertoca, l'encarregat de tal pròrroga en el termini d'un mes a

partir de la recepció de la sol·licitud de consulta, tot indicant els motius de la dilació.

Mentre l'autoritat de control no s'haja manifestat, no podrà dur-se a terme el tractament de dades en qüestió.

P/PDP-008 PROCEDIMENT DE DILIGÈNCIA EN LA CONTRACTACIÓ D'ENCARREGATS DE TRACTAMENT

OBJECTIUS I ABAST

Verificar el compliment de la legislació en matèria de protecció de dades per part dels prestadors de serveis amb accés a dades personals de la Diputació de València. La corporació triarà, únicament, encarregats que oferisquen garanties suficients per a aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament siga conforme amb els requisits de la normativa de protecció de dades i es garantisca la protecció dels drets dels interessats.

Estan afectats:

- Tots aquells tractaments de dades de caràcter personal que duguen a terme els prestadors de serveis per compte de la Diputació de València (encarregats del tractament).

Entitats de la Diputació de València afectades:

- Cada **unitat administrativa responsable de les prestacions de serveis** amb accés a dades personals.

- El **Departament de Protecció de Dades i Seguretat de la Informació**.

DESPLEGAMENT

Cada unitat administrativa responsable de prestacions de serveis remetrà als prestadors de serveis que tinguen accés a dades personals un formulari amb diverses qüestions d'obligada resposta, amb la finalitat de valorar el grau de compliment en relació amb la normativa de protecció de dades. Així mateix, es requeriran evidències de compliment. Les qüestions versaran sobre el grau d'adequació de l'encarregat del tractament a la normativa de protecció de dades, entre elles:

-Elaboració de Registre d'Activitats del Tractament
-Nomenament de delegat de Protecció de Dades
-Compliment del deure d'informació
-Realització d'anàlisi de riscos
-Adequació de les polítiques web
-Informació en relació amb les transferències internacionals de dades i garanties
-Informació sobre subcontractació
-Formació al personal en matèria de protecció de dades
-Subscripció de normes d'ús TIC i compromisos de confidencialitat per part de les persones treballadores
-Mesures de seguretat implementades
-Certificacions de seguretat
-Realització d'auditories
-Incidents o bretxes de seguretat patides
-Procediments de resposta enfront d'incidents i bretxes de seguretat

Els formularis de valoració seran facilitats pel Departament de Protecció de Dades i Seguretat de la Informació i, una vegada emplenats, seran posats a la disposició del delegat de Protecció de Dades, qui valorarà, conforme al qüestionari i les evidències remeses, si acompleixen la normativa de protecció de dades.

En cas que algun prestador no oferisca garanties suficients, s'haurà de valorar si es pot esmenar i/o prestar una mesura compensatòria o alternativa, establint un termini a aquest efecte. En un altre cas, es valorarà la contractació amb aquest proveïdor per part de la Diputació de València.

P/PDP-009 PROCEDIMENT INFORMATIU SOBRE VULNERACIÓ DE NORMATIVA DE PROTECCIÓ DE DADES

OBJECTIUS I ABAST

Regular un mecanisme o instrument de transparència i recopilació d'informació utilitzat internament pel delegat de Protecció de Dades amb les finalitats següents:

• Fer saber als possibles implicats que s'ha apreciat alguna acció que poguera ser constitutiva d'infringir la normativa legal o interna en matèria de protecció de dades personals.

• Poder incorporar major informació que poguera ser rellevant perquè el delegat valore jurídicament l'abast exacte de la possible vulneració.

• Informar en tot moment els implicats de les actuacions que el delegat puga emprendre en el marc de les seues competències.

Estan afectats:

- Tots els tractaments de dades de caràcter personal als quals resulte d'aplicació el Reglament de Política de Seguretat i de la Protecció de Dades de Caràcter Personal de la Diputació de València i que, per tant, es troben sota la supervisió del delegat de Protecció de Dades.

Entitats de la Diputació de València afectades:

- Personal i unitats administratives que tracten dades personals i estiguen subjectes a l'aplicació de la normativa legal i interna en la matèria.
- El **delegat de Protecció de Dades**.

DESPLEGAMENT

El delegat podrà iniciar el procediment informatiu en el curs de qualsevol de les seues actuacions quan el considere necessari per al compliment dels objectius de transparència i recopilació d'informació.

Fases. El procediment informatiu està conformat per dues fases:

• **Fase I**. Es trasllada als implicats informació mínima com ara: antecedents de fet, normativa aplicable, possibles vulneracions detectades i possibles responsables (si ja es contemplen responsables). Segons el paper o

protagonisme que exercisca en el procediment concret, algun implicat pot rebre només part de la citada informació. S'incorpora també la informació que, si és el cas, puguen aportar els interessats.

S'entén per implicades aquelles persones, unitats administratives o entitats que poden ser protagonistes en una possible vulneració normativa: responsables directes i indirectes de la vulneració, titulars de les dades afectades, unitats gestores o tercers que han participat en qualsevol fase del tractament de dades involucrat, testimonis o informadors en general que poden aportar informació rellevant.

• **Fase II**. Es comunica als implicats la informació relativa als possibles responsables (si ja es contemplen responsables), la informació aportada per altres implicats, si és el cas, i les conclusions del delegat després de la valoració del conjunt d'informació que conforma el procediment. Segons el paper o protagonisme que exercisca en el procediment concret, algun implicat pot rebre només part de la informació.

Terminis. Amb caràcter general, el termini per a aportar informació per part dels implicats serà de deu dies hàbils des que se'ls comunica la Fase I. Excepcionalment podria ampliar-se aquest termini en deu dies hàbils més si el delegat ho considera oportú, atesa la complexitat de la informació a aportar pels implicats, a la pròpia naturalesa dels suports, fonts o depositaris de la informació o a la dificultat de concretar o identificar a responsables. El procediment informatiu es tanca o conclou amb la comunicació de la Fase II. El termini màxim per a concloure el procediment informatiu serà de sis mesos.

El delegat pot deixar en suspens el transcurs dels citats terminis si de les informacions i esbrinaments aportats s'infereix la possible existència d'altres

implicats, i considera oportú incorporar-los al procediment informatiu. En aquest supòsit, els terminis es reprendran quan les actuacions amb els nous implicats s'equiparen amb les dutes a terme amb la resta d'implicats.