

DIPUTACIÓ DE
VALÈNCIA



Protecció de Dades i Seguretat de la Informació



Quaderns DivalData

Quaderns dirigits a delegats,
responsables i especialistes en protecció
de dades personals

Quadern núm. 17 | Novembre 2021

***DIRECTRIUS PER A L'ELABORACIÓ D'UNA
AVALUACIÓ D'IMPACTE EN PROTECCIÓ DE DADES***



Í N D E X



DIRECTRIUS PER A L'ELABORACIÓ D'UNA AVALUACIÓ D'IMPACTE EN PROTECCIÓ DE DADES

	Pàgina
Introducció	2
Quan ha de realitzar-se la EIPD	3
EIPD = gestió de riscos	7
Com abordar una EIPD	8
Material complementari i notícies	11



Vos convidem a traslladar-nos les temàtiques que resulten de vostre interès per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent

[enllac](#)



**UNA AVALUACIÓ D'IMPACTE ÉS UN
PROCÉS UTILITZAT PER A REFORÇARI
DEMOSTRAR EL COMPLIMENT**

INTRODUCCIÓ

La gestió del risc és un dels pilars de la direcció de qualsevol organització. Tota entitat o corporació, quan pretén iniciar amb garanties un nou producte o servei, ha de gestionar els elements d'incertesa que es deriven de la seua naturalesa, àmbit, context i fins.

El Reglament General de Protecció de Dades fa referència al terme “risc” en setanta-tres ocasions al llarg del text. Particularment, l'article 35, introdueix el concepte d'avaluació d'impacte relativa a la protecció de dades (EIPD).

En el text del Reglament no apareix una definició per al terme “avaluació d'impacte relativa a la protecció de dades”, però el Comité Europeu de Protecció de Dades sí que desenvolupa la definició de EIPD en les Directrius WP248 com “un procés concebut per a descriure el tractament, avaluar la seua necessitat i proporcionalitat i ajudar a gestionar els riscos per als drets i llibertats de les persones físiques derivats del tractament de dades personals avaluant-los i determinant les mesures per a abordar-los.”

Les EIPD són instruments importants per a la rendició de comptes, ja que ajuden els responsables no sols a complir els requisits del RGPD, sinó també a demostrar que s'han pres mesures adequades per a garantir el compliment del Reglament (vinya. art. 24).

En altres paraules, una EIPD és un procés utilitzat per a reforçar i demostrar el compliment.

En virtut del RGPD, l'incompliment dels requisits de la EIPD pot donar lloc a la imposició de sancions per part de l'Agència Espanyola de Protecció de Dades. La sanció pot ser imposada per:

- No dur a terme una EIPD quan el tractament requerisca una avaluació d'aquest tipus;
- Dur a terme una EIPD de manera incorrecta;
- No consultar a l'autoritat de control quan siga necessari.

Analitzem aquests extrems.



**ELS RESPONSABLES DELS
TRACTAMENTS DE DADES DE
REALITZAR UNA EIPD AMB CARÀCTER
PREVI A L'INTRODUCCIÓ DE TALS
TRACTAMENTS QUAN SIGA PROBABLE
QUE AQUESTS PER LA SEUA
NATURALESIA, ABAST, CONTEXT O FINS
COMPORTEN UN ALT RISC PER ALS
DRETS I LLIBERTATS DE LES PERSONES**

QUAN HA DE REALITZAR-SE LA EIPD

Una EIPD marcarà la forma en què hem de fer-nos càrrec dels riscos dels nostres tractaments, adoptant les mesures que resulten preceptives per a solucionar-los, de manera que puguem garantir que les dades personals siguen degudament protegits.

És a dir, la finalitat que es persegueix en realitzar una EIPD és possibilitar que els responsables del tractament adopten mesures tendents a reduir aqueixos riscos que ens obliguen a fer-la (disminuint la probabilitat de la seua materialització i les conseqüències negatives per als usuaris).

L'apartat 1 de l'article 35 del RGPD estableix, amb caràcter general, l'obligació que tenen els responsables dels tractaments de dades de realitzar una EIPD amb caràcter previ a la posada en funcionament de tals tractaments quan siga probable que aquests per la seua naturalesa, abast, context o fins comporten un alt risc per als drets i llibertats de les persones físiques, alt risc que, segons el propi Reglament, es veurà incrementat quan els tractaments es realitzen utilitzant "noves tecnologies".

L'article 35.3 estableix que la EIPD es requerirà en particular en un d'aquests casos:

- 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 les categories especials de dades a què es refereix l'article 9, apartat 1, o de les dades personals relatives a condemnes i infraccions penals a què es refereix l'article 10 del RGPD;
- observació sistemàtica a gran escala d'una zona d'accés públic.



**UNA PRIMERA ANÀLISI QUALITATIVA
POT CONCLURE QUE NO ÉS
NECESSARI REALITZAR AQUESTA EIPD,
PERÒ CAL JUSTIFICAR-LO**

Per a facilitar als responsables dels tractaments la identificació d'aquells tractaments que no requereixen una EIPD, el RGPD disposa que les autoritats de control podran –com fa la nostra AEPD– publicar llistes amb els tractaments que requereixen i no requereixen de l'elaboració d'una EIPD. Aquestes llistes estan enllaçades en l'apartat de Material complementari, però vegem alguns exemples.

EXEMPLES DE SUPÒSITS OBLIGATORIS

- Tractaments que impliquen perfilat o valoració de subjectes, inclosa la recollida de dades del subjecte en múltiples àmbits de la seua vida (acompliment en el treball, personalitat i comportament), que cobrisquen diversos aspectes de la seua personalitat o sobre els seus hàbits.
- Tractaments que impliquen la presa de decisions automatitzades o que contribuïsqen en gran manera a la presa de tals decisions, incloent qualsevol tipus de decisió que impedisca a un interessat l'exercici d'un dret o l'accés a un bé o un servei o formar part d'un contracte.
- Tractaments que impliquen l'observació, monitoratge, supervisió, geolocalització o control de l'interessat de manera sistemàtica i exhaustiva, inclosa la recollida de dades i metadades a través de xarxes, aplicacions o en zones d'accés públic, així com el processament d'identificadors únics que permeten la identificació d'usuaris de serveis de la societat de la informació com poden ser els serveis web, TV interactiva, aplicacions mòbils, etc.
- Tractaments que impliquen l'ús de categories especials de dades a les quals es refereix l'article 9.1 del RGPD, dades relatives a condemnes o infraccions penals als quals es refereix l'article 10 del RGPD o dades que permeten determinar la situació financera o de solvència patrimonial o deduir informació sobre les persones relacionada amb categories especials de dades.



***CATEGORIES ESPECIALS DE DADES,
TRACTAMENTS A GRAN ESCALA O ÚS
DE LES NOVES TECNOLOGIES PODEN
MOTIVAR LA NECESSITAT D'UNA EIPD***

- Tractaments que impliquen l'ús de dades biomètriques amb el propòsit d'identificar de manera única a una persona física.
- Tractaments de dades de subjectes vulnerables o en risc d'exclusió social, incloent dades de menors de 14 anys, majors amb algun grau de discapacitat, discapacitats, persones que accedeixen a serveis socials i víctimes de violència de gènere, així com els seus descendents i persones que estiguen sota el seu guàrdia i custòdia.
- Tractaments que impliquen l'associació, combinació o enllaç de registres de bases de dades de dues o més tractaments amb finalitats diferents o per responsables diferents
- Tractaments que impliquen l'ús de dades a gran escala. Per a determinar si un tractament es pot considerar a gran escala es consideraran els criteris establits en la guia WP243 "Directrius sobre els delegats de protecció de dades (DPD)" del Grup de Treball de l'Article 29.
- Tractaments que impliquen la utilització de noves tecnologies o un ús innovador de tecnologies consolidades, incloent la utilització de tecnologies a una nova escala, amb un nou objectiu o combinades amb unes altres, de manera que supose noves formes de recollida i utilització de dades amb risc per als drets i llibertats de les persones.
- Tractaments de dades que impedisquen als interessats exercir els seus drets, utilitzar un servei o executar un contracte, com per exemple tractaments en els quals les dades han sigut recopilats per un responsable diferent al que els tractarà i aplica alguna de les excepcions sobre la informació que ha de proporcionar-se als interessats segons l'article 14.5 (b,c,d) del RGPD.

EXEMPCIÓ DE L'OBLIGACIÓ

Estan considerant un nou tractament i no saben si requeriria realitzar una avaluació d'impacte?

L'AEPD publicita exemples de tractaments exempts de realitzar una EIPD:



***NOUS TRACTAMENTS QUE SIGUEN
NECESSARIS PER AL COMPLIMENT
D'UNA OBLIGACIÓ LEGAL,
COMPLIMENT D'UNA MISSIÓ
REALITZADA EN INTERÉS PÚBLIC O EN
L'EXERCICI DE PODERS PÚBLICS
CONFERITS AL RESPONSABLE,
PODRIEN ESTAR EXEMPTS***

- Tractaments que es realitzen estrictament sota les directrius establides o autoritzades amb anterioritat mitjançant circulars o decisions emeses per les Autoritats de Control, en particular l'AEPD, sempre que el tractament no s'haja modificat des que va ser autoritzat.
- Tractaments que es realitzen estrictament sota les directrius de codis de conducta aprovats per la Comissió Europea o les Autoritats de Control, en particular l'AEPD, sempre que una EIPD completa haja sigut realitzada per la validació del codi de conducta i el tractament s'implementa incloent les mesures i salvaguardes definides en la EIPD.
- Tractaments que siguen necessaris per al compliment d'una obligació legal, compliment d'una missió realitzada en interés públic o en l'exercici de poders públics conferits al responsable, sempre que en el mateix mandat legal no s'obligue a realitzar una EIPD, i sempre que ja s'haja realitzat una EIPD completa.
- Tractaments realitzats en l'exercici de la seua labor professional per treballadors autònoms que exercisquen de manera individual, en particular mèdics, professionals de la salut o advocats, sense perjudici que puga requerir-se quan el tractament que duguen a terme complisca, de manera significativa, amb dues o més criteris establits en la llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a protecció de dades publicada per l'AEPD.
- Tractaments obligatoris per llei i realitzats en relació amb la gestió interna del personal de les PIMES amb finalitat de comptabilitat, gestió de recursos humans i nòmines, seguretat social i salut laboral, però mai relatius a les dades dels clients.

També s'esmenten alguns supòsits relatius a comunitats de propietaris i col·legis professionals i associacions sense ànim de lucre.



***CAL COMENÇAR PER LA DESCRIPCIÓ
SISTEMÀTICA DE LES OPERACIONS DE
TRACTAMENT PREVISTES I DELS FINS
DEL TRACTAMENT, INCLUSIVAMENT,
SI ESCAU, DE L'INTERÉS LEGÍTIM
PERSEGUIT PEL RESPONSABLE
DEL TRACTAMENT***

EIPD = GESTIÓ DE RISCOS

Cal recordar que estem davant el procés d'identificar, avaluar i gestionar els riscos.

El nostre estudi haurà d'incloure, doncs, una descripció sistemàtica de les operacions de tractament previstes i dels fins del tractament, inclusivament, quan siga procedent, l'interés legítim perseguit pel responsable del tractament; una avaluació de la necessitat i la proporcionalitat de les operacions de tractament respecte a la seua finalitat; i una avaluació dels riscos per als drets i llibertats dels interessats.

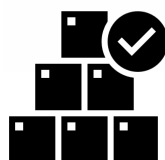
En altres paraules, aquesta gestió de riscos es divideix en tres parts:



La **identificació de les amenaces** (factors de risc concurrents que, en cas de materialitzar-se, pot provocar danys als drets dels interessats) i **dels riscos** (la combinació de la possibilitat que es materialitzen les amenaces prèviament identificades i les seues conseqüències).



L'avaluació **dels riscos** (consisteix a valorar l'impacte (significatiu o no) de l'exposició a l'amenaça, entés com els possibles danys que es poden produir si l'amenaça es materialitza, al costat de la probabilitat que aquesta es materialitze).



El **tractament dels riscos** detectats. El risc ha de ponderar-se sobre la base d'una avaluació objectiva mitjançant la qual es determine si les operacions de tractament de dades suposen un risc o si el risc és alt.



**EL RESPONSABLE DEL TRACTAMENT
ÉS QUI REALITZARÀ LA EIPD,
AMB ASSESSORAMENT DEL DELEGAT
DE PROTECCIÓ DE DADES, PER LA
SEUA FUNCIÓ DE SUPORT I
ASSESSORAMENT**

COM ABORDAR UNA EIPD

El responsable del tractament és qui realitzarà la EIPD, amb assessorament del Delegat de Protecció de Dades (per la seua funció de suport i assessorament), si haguera sigut nomenat, o de l'encarregat del tractament, segons el que es disposa en contracte per encàrrec del tractament, en el seu cas.

Així mateix, podrien concórrer altres persones o figures, amb diferents rols i responsabilitats. Si escau, el responsable recaptarà l'opinió dels interessats en relació amb el tractament previstos.

Per a la metodologia, existeixen indicacions de l'AEPD i un model a l'efecte de poder utilitzar-se en les administracions públiques (vegeu l'apartat de material complementari).

En essència, l'avaluació ha d'incloure les mesures, garanties i mecanismes previstos per a mitigar el risc, garantir la protecció de les dades personals i demostrar la conformitat amb el Reglament.

El contingut de l'avaluació haurà d'incloure com a mínim:

1. Una exposició ordenada de les activitats de tractament previstes i dels fins del tractament, inclusivament, quan siga procedent, l'interés legítim perseguit pel responsable del tractament. *Vegeu l'Annex I de la Guia AEPD per a la realització de EIPD.*
2. Una valoració de l'exigència i la proporcionalitat de les operacions de tractament respecte a la seua finalitat. *Annex II de la Guia AEPD per a realitzar EIPD.*
3. Una apreciació dels perills per als drets i llibertats dels interessats.
4. Les mesures contemplades per a fer front als riscos i amenaces.
5. Garanties, mesures de seguretat i mecanismes destinats a garantir la protecció de dades personals i a demostrar la conformitat amb el reglament, tenint en compte els drets i interessos legítims dels interessats i d'altres persones afectades.



**ELS RISCOS QUE HEM D'OBSERVAR
SÓN TANT AQUELLS RELATIUS A LES
PERSONES, COM ELS QUE
PODEN AFECTAR L'ORGANITZACIÓ
SI NO COMPLIM AMB
LA PROTECCIÓ DE DADES**

FASES

- IDENTIFICAR LA NECESSITAT D'UNA EIPD

Com ja es va indicar, realitzar un EIPD no és una obligació per a totes les organitzacions, encara que és recomanable fer-ho en tots els casos que es tracten dades personals. Quan no siga obligatori es pot optar per una aproximació menys formalitzada. El resultat ajudarà a a protegir les dades, mantindre una bona reputació i evitar sancions.

- ANÀLISI DEL PROJECTE I FLUXOS D'INFORMACIÓ

Aquesta segona etapa és de gran importància per a realitzar una bona EIPD. Per a això, serà necessari analitzar en profunditat el projecte que engloba el tractament de dades personals, com per exemple categories tractades, actors implicats, tecnologies, cessions a tercers, etc.

- IDENTIFICACIÓ RISCOS

Amb tota la informació obtinguda en l'etapa anterior s'hauran d'identificar els possibles riscos als quals estan exposats les dades, valorar la probabilitat i el impacte que tindria la materialització de l'amenaça.

Els riscos poden ser de dos tipus:

- Per a les persones, el principal a tindre en compte, pot posar en risc la seua privacitat;
- Per a la organització, quan no implementara una correcta política de protecció de dades.

- GESTIÓ DE RISCOS

Una vegada analitzat el projecte i definits els riscos, s'hauran de identificar els controls i mesures de seguretat necessàries. Aquesta fase ha de ser duta a terme i consensuada entre tots els actors implicats en el tractament.

- COMPLIMENT NORMATIU

Es comprovarà que el contingut de la EIPD compleix amb la legislació en matèria de protecció de dades (LOPDGDD i RGPD), així com, en el seu cas, l'altra legislació aplicable per ser d'obligat compliment.



**S'HAURAN D'APLICAR LES MESURES
NECESSÀRIES PER A PROTEGIR LES
DADES PERSONALS INDICADES PELS
RESPONSABLES DE L'ENTITAT O
CORPORACIÓ**

- **INFORME FINAL**

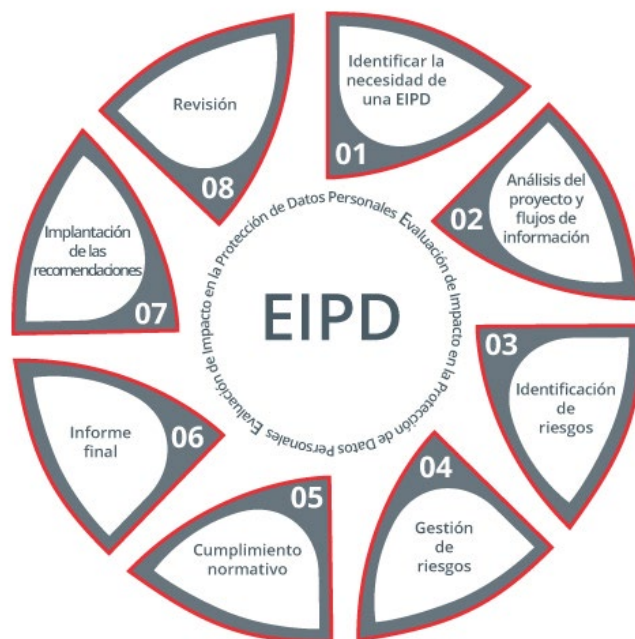
En l'informe final s'inclourà tota la informació que s'ha generat durant les etapes anteriors. Aquest informe haurà d'estar elaborat amb un llenguatge clar, evitant la inclusió de tecnicismes de qualsevol tipus. Aquest informe serà remés als màxims responsables de l'organització perquè prenguen les decisions necessàries en funció de les recomanacions indicades.

- **IMPLANTACIÓ DE LES RECOMANACIONS**

Una vegada revisat l'informe, s'hauran d'aplicar les mesures necessàries per a protegir les dades personals indicades pels responsables de l'organització. En aquesta fase es definiran els recursos necessaris i el responsable de la seua execució.

- **REVISIÓ**

Una vegada acabat el procés es analitzarà el resultat final i l'efectivitat dels controls presos. També s'identificaran nous riscos als quals estan exposats les dades.



Font: INCIBE



MATERIAL COMPLEMENTARI

- “Gestió del risc i avaluació d'impacte en tractaments de dades personals” (guia de l'AEPD). Consulta en [aquest enllaç](#).
- Llista de tractaments que requereixen avaluació d'impacte relativa a protecció de dades (AEPD). Consulta en [aquest enllaç](#).
- Llista orientativa de tipus de tractaments de dades que no requereixen una avaluació d'impacte relativa a la protecció de dades (AEPD). Consulta en [aquest enllaç](#).
- Eina "Avalua-Risc *RGPD" (AEPD). Consulta en [aquest enllaç](#).
- Eina “Gestiona *EIPD” (AEPD). Consulta en [aquest enllaç](#).

NOTÍCIES

- **L'AEPD publica un model d'informe per a ajudar les empreses a realitzar avaluacions d'impacte en la protecció de dades.**

El document recopila els aspectes que han de ser tinguts en compte pel sector privat per a elaborar un informe d'Avaluació d'Impacte (EIPD), complementant a la Guia pràctica publicada per l'Agència. Consulta la publicació en [aquest enllaç](#).

- **El BOE publica la Instrucció 1/2021, de 2 de novembre, de l'Agència Espanyola de Protecció de Dades, per la qual s'estableixen directrius respecte de la funció consultiva de l'Agència, de conformitat amb el 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 la lliure circulació d'aqueixes dades, la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, i l'Estatut de l'Agència Espanyola de Protecció de Dades, aprovat pel Reial decret 389/2021, d'1 de juny.**

La instrucció serà aplicable a l'activitat consultiva de l'AEPD. Consulta la Instrucció en [aquest enllaç](#).

- **L'Agència Espanyola de Protecció de Dades (AEPD) ha sancionat a l'Ajuntament de Molina de Segura per mancar de delegat de protecció de dades.**

Consulta la notícia en [aquest enllaç](#).