Directrius per a un Pla integrat per a la DPIA-FRIA

Octubre 2026

DPD en xarxa

Índex

Presentació 4

1. Els principals blocs de l'AIPD i la seva integració amb la FRIA 5
   1.1 La descripció sistemàtica 5
   1.2 L'avaluació 6
   1.3 Les mesures de mitigació 9

2. El flux de treball integrat de l'AIPD-FRIA i disseny del model 10

Coordinadors:

Alessandro Mantelero i Joana Marí

Participants:

Aida Mariscal (Centre de Telecomunicacions i Tecnologies de la Informació)

Albert Portugal (Consorci de Serveis Universitaris de Catalunya)

Albert Serra (Autoritat Catalana de Protecció de Dades)

Alessandro Mantelero (Universitat Politècnica de Torí)

Carles Garcia (Autoritat Catalana de Protecció de Dades)

Carlos López (Autoritat Catalana de Protecció de Dades)

Cristina Guzmán (Universitat Politècnica de Catalunya – BarcelonaTech (UPC))

Esther Garcia (CaixaBank, SA)

Irma Choy (Consorci AOC)

Joana Judas (Autoritat Catalana de Protecció de Dades))

Joana Marí (Autoritat Catalana de Protecció de Dades)

M. Ascensión Moro (Ajuntament de Sant Feliu de Llobregat)

M. Ester Santiago (Ajuntament de Barcelona)

Maria José Campo (Fundació TIC Salut i Social)

Maria José Candial (Ajuntament de Barcelona)

Mariona Perramon (Consorci de Serveis Universitaris de Catalunya)

Mireia Bosch (Departament de Justícia i Qualitat Democràtica)

Patricia Lozano (Universitat Oberta de Catalunya)

Rosa Parrilla (Departament de la Presidència)

Roser Bellido (Departament de Drets Socials i Inclusió)

Ruben Ortiz (Universitat de Barcelona)

Sara Hernández (Fundació TIC Salut i Social)



Barcelona, 2026

El contingut d'aquest document és propietat de l'Autoritat Catalana de Protecció de Dades i està subjecte a la llicència Creative Commons BY-NC-ND,
https://creativecommons.org/licenses/by-nc-nd/4.0/.

L'autoria de l'obra s'ha de reconèixer mitjançant la inclusió de la menció següent:
Obra titularitat de l'Autoritat Catalana de Protecció de Dades.
Llicència sota la llicència CC BY-NC-ND.

Avís: quan es reutilitza o distribueix l'obra, se n'han d'indicar clarament els termes de la llicència.

Avís legal: Les opinions expressades en aquest document són responsabilitat dels seus autors i no reflecteixen necessàriament l'opinió oficial de l'APDCAT. L'Autoritat Catalana de Protecció de Dades i, els autors i els membres del grup de treball no es fan responsables de les possibles conseqüències de les actuacions de les persones físiques o jurídiques arran de qualsevol informació continguda en aquest document.

Presentació

Aquest 2026, hem celebrat el desè aniversari del Reglament general de protecció de dades. Poc se'n pot destacar ja que no s'hagi dit amb anterioritat, però és evident que va ser una norma determinant per consolidar el dret fonamental a la protecció de dades, tant en l'àmbit europeu com internacional.

De fet, és la base sobre la qual s'ha construït tota l'estratègia europea de la dada. Així, el Reglament d'intel·ligència artificial, de 2024 i modificat el 2026, l'esmenta en diverses ocasions al llarg del seu articulat: per una banda, afirmant que no el desplaça (considerant 10 i article 2.7); per una altra, enfortint el paper de les autoritats de control de protecció de dades, en articles com el 5, el 57, el 74 o, un cop designades autoritats de protecció dels drets fonamentals, el 77. I, finalment, cal destacar l'article 27.

Aquest article regula les avaluacions d'impacte sobre els drets fonamentals en els sistemes d'intel·ligència artificial (AIDF) i estableix la relació entre aquesta avaluació i la de protecció de dades de l'RGPD i de la Directiva (UE) 2016/680 (AIPD). I en la redacció de 2026, arran de la reforma òmnibus aprovada per la Unió Europea, preveu que entre totes dues avaluacions s'hi poden incloure o referències creuades o les parts pertinents de l'AIDP a l'AIDF. Per tant, tots dos reglaments són complementaris.

Però de la norma a la pràctica hi ha un pas. I, per això, des de l'Autoritat Catalana de Protecció de Dades ens vam proposar omplir dos buits: el primer, com fer una avaluació d'impacte sobre els drets fonamentals; el segon, com integrar de forma efectiva les dues avaluacions.

Al primer buit hi vam donar resposta el gener de 2025, amb la presentació del model FRIA català: una metodologia pionera i provada amb diversos casos d'ús. Va ser fruit de la feina d'un grup de treball liderat pel professor Alessandro Mantelero, de la Universitat Politècnica de Torí, en el marc de DPD en Xarxa, la comunitat d'aprenentatge impulsada per l'APDCAT. Aquest model va ser un dels primers que va adoptar l'Agència de Drets Fonamentals de la Unió Europea. D'aquest model FRIA, el 7 d'octubre de 2026 se n'ha presentat l'eina FRIA, que permet dur a terme l'avaluació d'impacte de forma automatitzada i àgil.

El segon buit l'omplim amb aquestes orientacions, que són el resultat de la feina del mateix grup de treball, que no es va aturar i ha continuat treballant per proporcionar als DPD i a les organitzacions un nou recurs que facilitarà el compliment normatiu.

Des de l'APDCAT, continuem compromesos amb la garantia del dret a la protecció de dades i de la resta de drets fonamentals. I continuarem treballant-hi, de la mà dels grans professionals amb què comptem a Catalunya.

Meritxell Borràs i Solé
Directora
Autoritat Catalana de Protecció de Dades

1. Els principals blocs de l'AIPD i la seva integració amb la FRIA

En els apartats següents, s'examinen els elements principals de l'AIPD tal com s'estableix a l'article 35 de l'RGPD. S'hi descriu el contingut de l'AIPD sobre la base de la pràctica internacional i l'experiència del sector públic a Catalunya. Utilitzant la plantilla de l'AIPD de l'APDCAT, es proporcionaran directrius per identificar els elements clau que cal incloure en cada fase, amb l'objectiu de crear una AIPD que pugui complementar fàcilment la FRIA exigida pel RIA.

El model resultant no pretén substituir la plantilla de l'AIPD de l'APDCAT ni les plantilles existents desenvolupades per diverses institucions, sinó presentar un model àgil que es pugui integrar fàcilment amb la plantilla de FRIA adoptada per l'APDCAT (d'aquest model FRIA, el 7 d'octubre de 2026 se n'ha presentat l'eina FRIA, que permet dur a terme l'avaluació d'impacte de forma més eficient).

La nova plantilla permet als usuaris ampliar la secció de l'AIPD, per incloure-hi una avaluació més àmplia del compliment de les disposicions de l'RGPD en general i, en especial, quan s'incorpora IA als tractament de dades personals.

Aquest exercici de simplificació ha estat necessari atenent al que estableix l'article 27.4 del RIA, on s'indica que:

> "4. Si ya se cumplen cualesquiera de las obligaciones establecidas en el presente artículo mediante la evaluación de impacto relativa a la protección de datos realizada en virtud del artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, el responsable del despliegue podrá, al llevar a cabo la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo, incluir referencias cruzadas a las secciones pertinentes de dicha evaluación de impacto relativa a la protección de datos o incluir las partes pertinentes de esta en la evaluación de impacto relativa a los derechos fundamentales."

La metodologia s'estructura a partir de **dues parts comunes a ambdues avaluacions** que, en un model integrat, poden examinar-se una sola vegada i els resultats de la qual es poden utilitzar tant per a l'AIPD com per a la FRIA. Aquesta anàlisi és crucial per evitar repetir dues vegades l'avaluació dels mateixos elements (per exemple, el context d'ús) i per crear un flux d'informació coherent entre les dues avaluacions.

1.1 La descripció sistemàtica

Aquesta és la primera part tant de l'AIPD com de la FRIA. Consisteix a fer una anàlisi de les necessitats i descriure les solucions previstes que es desenvoluparan, amb referència al seu context d'ús. S'ha de proporcionar informació general preliminar als usuaris de l'eina d'avaluació d'impacte, sobre la naturalesa i la finalitat de l'avaluació i sobre els conceptes generals d'avaluació basada en el risc, que són presents tant a l'RGPD com al RIA.

Pel que fa a la descripció de les solucions previstes, els projectes que impliquin l'ús de dades personals, així com els que impliquin IA, han de descriure com s'utilitzen tant les dades com la IA. Per això, cal proporcionar informació detallada sobre la naturalesa de les dades i el seu tractament, que s'integrarà amb la informació sobre el sistema d'IA utilitzat. De la mateixa manera, es necessita informació sobre les persones directament implicades en el

desenvolupament del projecte i la seva funció en virtut de l'RGPD (responsable del tractament, corresponsable del tractament, encarregat del tractament, sotsencarregat del tractament) i del RIA (proveïdor, responsables del desplegament), les possibles categories de titulars de drets afectats i els contextos d'ús.

1.2 L'avaluació

Quant a la fase d'avaluació, cal assenyalar que l'AIPD i la FRIA són obligacions legals amb un abast limitat, definit, respectivament, per l'article 35 de l'RGPD i l'article 27 del RIA. Tanmateix, en l'àmbit de la protecció de dades, igual com en el de la IA, l'avaluació prèvia dels riscos té un abast que va més enllà de les avaluacions d'impacte regulades.

En virtut de l'RGPD, els riscos s'han de tenir en compte a l'hora d'aplicar el Reglament, fins i tot si no suposen un risc elevat per als drets i llibertats de les persones físiques. També en aquests casos continua essent necessari aplicar adequadament tots els principis establerts a l'article 5 de l'RGPD i a les disposicions pertinents del Reglament, amb la finalitat de minimitzar qualsevol impacte, fins i tot els de menor abast, sobre el dret a la protecció de dades i altres drets fonamentals. Per tant, una avaluació general dels riscos és inherent a totes les activitats de tractament, mentre que una AIPD formal només és obligatòria en casos d'alt risc.[1]

El mateix s'aplica a la FRIA. Malgrat limitar-se a determinades categories de responsables del desplegament i determinades situacions, la protecció garantida dels drets fonamentals exigeix el deure de protegir activament aquests drets, i una FRIA és una eina útil per aconseguir aquest objectiu. A més, la FRIA, en termes de metodologia per avaluar l'impacte sobre els drets fonamentals, també **pot ser utilitzada pels proveïdors d'IA** per complir amb l'article 9 pel que fa als riscos que plantegen per als drets fonamentals i, amb caràcter general, per qualsevol entitat que incorpori sistemes d'IA en la seva organització, atès que en el context de la Unió Europea la garantia i protecció dels drets fonamentals, recollits a la Carta dels Drets Fonamentals de la Unió Europea, és comuna a qualsevol actuació.

Pel que fa al compliment estricte de l'RGPD i el Reglament d'IA, un model que integri l'AIPD i la FRIA requereix una anàlisi prèvia dels requisits legals establerts per aquestes dues normatives, a fi de determinar els supòsits en què ambdues són obligatòries. Aquesta avaluació es fa a la secció 2 del model d'avaluació (Necessitat de dur a terme una AIPD i una FRIA).

Pel que fa a l'avaluació del risc per als «drets i llibertats de les persones físiques» (article 35 de l'RGPD) i «l'impacte en els drets fonamentals» (article 27 de la Llei d'IA), hi ha diferències perquè el Reglament europeu d'IA, a l'article 1, es refereix a la «protecció de [...] els drets fonamentals consagrats en la Carta». No obstant això, més enllà de la qualificació jurídica d'aquests drets, l'enfocament metodològic és el mateix: se centra en el risc en termes de perjudici a aquests drets, tenint en compte la probabilitat que es produeixi un dany i la gravetat d'aquest dany.[2]

---

[1] Vegeu també article 29 Data Protection Working Party (nota 2), 8 («In cases where it is not clear whether a AIPD is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.»).

[2] Vegeu l'article 3, apartat 2, de la Llei d'IA; l'article 25, apartat 1, i el considerant 75 de l'RGPD. Segons el considerant 76 de l'RGPD, «La probabilitat i la gravetat del risc per als drets i llibertats de l'interessat s'ha de determinar d'acord amb la naturalesa, l'abast, el context i les finalitats del tractament de dades.»

Com es pot observar a les taules següents, extretes de la plantilla de l'avaluació d'impacte en protecció de dades de la CNIL[3] i la FRIA de l'APDCAT[4], la metodologia d'avaluació de riscos està alineada de la mateixa manera en els dos instruments.

Taula 3. CNIL PIA

3.2 Risk assessment: potential privacy breaches

Analysis and assessment of risks

Risk	Main risk sources	Main threats	Main potential impacts	Main controls reducing the severity and likelihood	Severity	Likelihood
Illegitimate access to data						
Unwanted change of data						
Disappearance of data						

Assessment of the risks

Risks	Acceptable/can be improved on?	Corrective controls	Residual severity	Residual likelihood
Illegitimate access to data	[*The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.*]	[*Where applicable, he shall indicate here any additional controls that would prove necessary.*]		
Unwanted change of data	[*The assessor must determine whether the existing or planned controls (already undertaken) sufficiently reduce this risk for it to be deemed acceptable.*]	[*Where applicable, he shall indicate here any additional controls that would prove necessary.*]		

[3] Vegeu CNIL (nota 7), 20.
[4] Vegeu Autoritat Catalana de Protecció de Dades (nota 6), 19.

Taula 4. APDCAT FRIA

Taula 2A. Gestió de riscos (I)

Drets/llibertats afectats	Probabilitat	Gravetat	Impacte global	Mesures per prevenir/mitigar els impactes

Taula 3A. Gestió de riscos (II)

Drets/llibertats afectats	Probabilitat (residual)	Gravetat (residual)	Impacte residual

D'acord amb la metodologia general d'avaluació de riscos**, la probabilitat i la gravetat dels possibles perjudicis s'examina** basant-se en el disseny del projecte, es preveuen les possibles mesures de mitigació i es duu a terme una nova avaluació, per definir l'impacte d'aquestes mesures i els riscos residuals. Aquest procés iteratiu és coherent amb l'enfocament basat en el risc, adoptat tant per l'AIPD com per la FRIA.

Tanmateix, mentre que l'AIPD analitza els diversos riscos d'un dret únic, reflectint la naturalesa procedimental de la protecció de dades en termes de possibles violacions (per exemple, accés no autoritzat a les dades o canvis no desitjats), la FRIA considera cada dret afectat en tota la seva dimensió, sense identificar subconjunts de riscos per cap tipus de perjudici potencial. Això es deu, també, al fet que la protecció dels drets fonamentals diferents del dret a la protecció de dades no té una naturalesa procedimental similar i, en les seves respectives normatives, es basa en la definició d'un àmbit de protecció concret i en la prohibició d'interferir-hi, tret de quan hi prevalguin altres béns i interessos jurídics d'acord amb la llei.

Per tant, per alinear l'AIPD i la FRIA, no cal revisar les matrius utilitzades en l'AIPD per avaluar el nivell de risc per a la protecció de dades, ja que aquestes matrius continuen formant part de l'avaluació general de l'impacte sobre aquest dret.

No obstant això, les mesures de mitigació adoptades en matèria de protecció de dades també poden beneficiar altres drets, fet que s'ha de tenir en compte en termes de controls establerts, actualitzant la secció C del qüestionari FRIA.

Altrament, cal tenir en compte que el tractament de dades personals pot generar riscos per a altres drets i llibertats de les persones, més enllà del mateix dret a la protecció de dades personals. Per tant, l'AIPD pot ajudar també a identificar impactes potencials en altres drets derivats del tractament realitzat i, en especial, de l'ús que es fa de la IA.

1.3 Les mesures de mitigació

El bloc final de l'AIPD consisteix a identificar les mesures de mitigació més adequades per reduir l'impacte en la protecció de dades.

De conformitat amb l'article 35, apartat 7, lletra *d*, aquestes mesures són les «previstes per afrontar els riscos, incloses garanties, mesures de seguretat i mecanismes que garanteixen la protecció de dades personals per demostrar la conformitat amb aquest Reglament, tenint en compte els drets i interessos legítims dels interessats i d'altres persones afectades.»

Entre aquestes mesures de mitigació, s'hi poden incloure els elements del compliment de l'RGPD que poden contribuir a reduir el risc. A més, aquests elements també són rellevants des de la perspectiva de la FRIA, ja que poden ajudar a reduir els efectes negatius sobre altres drets i llibertats.

La qualitat de les dades, per exemple, pot reduir els biaixos i els efectes negatius sobre el dret a la no discriminació, mentre que la supervisió humana[5] pot ser eficaç en la presa de decisions basada en dades, no sols en termes de compliment de l'RGPD, sinó també com una intervenció que mitiga l'impacte sobre altres drets afectats.[6]

En relació amb l'anterior, les diverses preguntes sobre aquests diferents aspectes incloses a l'AIPD s'han de replantejar dins de la lògica de les possibles mesures que cal adoptar per mitigar els riscos, en lloc de com a elements d'una verificació del compliment.

[5] Vegeu també l'article 14 del RIA.
[6] La mateixa consideració es pot aplicar a la transparència, que és un factor que permet comprendre les possibles conseqüències negatives de l'ús de les dades, també en el context de la IA, i que es pot combinar amb les obligacions de transparència previstes al RIA (Vegeu també l'article 13 del RIA.). El correcte compliment de les obligacions de transparència dels proveïdors de sistemes d'IA establertes al RIA és essencial per al compliment de les obligacions del responsable del tractament en termes de l'RGPD.

2. El flux de treball integrat de l’AIPD-FRIA i disseny del model

D’acord amb les consideracions expressades en les seccions anteriors, el flux de treball general de la plantilla del model AIPD-FRIA pot descriure's com es mostra al diagrama següent:



Plantilla del Model DPIA-FRIA


DPD
en xarxa