Plantilla Model DPIA-FRIA

Índex

1. Descripció del projecte en relació amb el tractament de dades 4
1.1 Dades personals tractades 4
1.2 Processos de tractament 5
1.3 Descripció i anàlisi del sistema d'IA 7
1.4 Actors que intervenen en el tractament 12
2. Necessitat de dur a terme una AIPD i una FRIA 13
2.1 Necessitat de dur a terme una AIPD 13
2.2 Necessitat de dur a terme una FRIA 18
3. Avaluació d'Impacte en Protecció de Dades 20
3.1 Necessitat i proporcionalitat 20
3.1.1 Finalitat del tractament 22
3.1.2 Principis de licitud 23
3.1.2.1 Base legal per al tractament 23
3.1.2.2 Tractament de dades de menors 24
3.1.2.3 Tractament de categories especials de dades 25
3.1.2.4 Tractament de dades penals 26
3.1.2.5 Validesa del consentiment 26
3.1.2.6 Transferències de dades 27
3.1.2.7 Licitud del tractament per entrenar la IA 28
3.1.3. Principi de lleialtat del tractament 28
3.1.4 Principi de minimització 28
3.1.5 Principi de limitació del termini de conservació 29
3.1.6 Principi d'exactitud 30
3.1.7 Riscos per les persones 30
3.1.8 Necessitat i proporcionalitat del tractament 32
3.1.9 Opinió de les persones interessades 33
3.2 Controls per garantir els drets de les persones 34
3.2.1 Controls pel dret a tenir informació transparent 34
3.2.2 Controls per al dret d'informació 35
3.2.3 Controls per garantir el dret d'accés 37

3.2.4 Controls per garantir el dret de rectificació 38
3.2.5 Dret de supressió 38
3.2.6 Dret a limitar el tractament 39
3.2.7 Dret a la portabilitat de les dades 40
3.2.8 Dret d'oposició 41
3.2.9 Dret a no ser objecte de decisions automatitzades 41
3.3. Riscos en la seguretat de les dades 42
3.3.1 Impacte 42
3.3.2 Probabilitat inicial 45
3.3.3 Risc inicial 49
3.3.4 Controls de seguretat 50
3.3.5 Impacte residual 55
3.3.6 Probabilitat residual 56
3.3.7 Estimació del risc residual 60
4. Avaluació d'Impacte en els Drets Fonamentals 61
4.1 Qüestionari de planificació i abast 61
4.2 Matrius de risc 62
Taula 1. Probabilitat 62
Taula 2. Exposició 63
Taula 3. Probabilitat que es produeixi un perjudici (likelihood) 63
Taula 4. Gravetat del perjudici 63
Taula 5. Esforç per superar els perjudicis i revertir els efectes adversos 64
Taula 6. Gravetat (*severity*) 64
Taula 1A. Recollida de dades i anàlisi de riscos 64
Taula 7. Impacte general del risc 65
Taula 2A. Gestió de riscos (I) 65
Taula 3A. Gestió de riscos (II) 66

Aquesta plantilla avaluació d'impacte és un model que busca identificar i controlar els riscos per als drets i llibertats de les persones, derivats del tractament de dades personals i de l'ús de la IA.

En alguns casos, una organització pot tenir l'obligació de realitzar tant l'avaluació d'impacte en protecció de dades (art. 35 RGPD) com, també, l'avaluació d'impacte en drets fonamentals (art. 27 RIA). Per tal de simplificar aquesta tasca, aquesta plantilla inclou uns apartats previs que són útils per a les dues avaluacions: una descripció general del tractament, per determinar-ne els elements principals; i les activitats que es volen desenvolupar (identificades de manera conjunta com a «Projecte»), inclòs l'ús de dades i de la IA que es preveu. El nivell de detall ha de ser suficient per avaluar els supòsits i indicadors de risc detallats.

Cal tenir en compte que l'ús de la IA pot tenir impacte en una o diverses operacions de tractament de dades d'una activitat de tractament. Per poder avaluar correctament els riscos, és important detectar els fluxos i les interconnexions que hi ha en tot el cicle de vida del tractament de les dades personals i, si correspon, en el cicle de vida del sistema d'IA.

DESCRIPCIÓ GENERAL DEL PROJECTE

Descripció general del projecte

S'utilitzen dades personals?	☐ Sí ☐ No
S'utilitzen dades recollides amb una finalitat diferent a la del tractament avaluat?	☐ Sí ☐ No
El tractament incorpora IA ?	☐ Sí ☐ No

El projecte utilitza pràctiques prohibides d'IA establertes a l'article 5 del RIA?	☐ Sí ☐ No
Si s'utilitza la IA, a priori aquest ús podria afectar els drets fonamentals de les persones afectades o de tercers?	☐ Sí ☐ No
És possible obtenir els mateixos resultats mitjançant mètodes menys intrusius (per exemple, les dades sintètiques)?	☐ Sí ☐ No

En quina fase del cicle de vida es troba el sistema d'IA?	☐ Recerca ☐ Prova de concepte ☐ Disseny ☐ Desenvolupament ☐ Entrenament ☐ Validació ☐ Desplegament

1. Descripció del projecte en relació amb el tractament de dades

Cal fer una descripció del tractament de dades personals i no personals, al més detallada possible, ja que aquesta serà la base per avaluar la necessitat, la proporcionalitat i els riscos del tractament.

Descripció detallada del tractament i del context

Finalitat del tractament

1.1 Dades personals tractades

Les característiques de les dades a tractar són rellevants a l'hora de determinar els riscos del tractament i el compliment d'algunes disposicions del Reglament.

Tipus de dada	
Font / Origen	
Termini de conservació	
Hi ha dades mereixedores d'especial protecció? (econòmiques, violència de gènere, subvencions...)	☐ Sí ☐ No

Tipus de dada	
Se'n farà ús amb un propòsit diferent al de la recollida?	☐ Sí ☐ No
El tractament ofereix serveis de la societat de la informació a infants i té com a base el consentiment?	☐ Sí ☐ No
Es tracten dades de categories especials o de col·lectius vulnerables?	☐ Sí ☐ No
Es tracten dades relatives a condemnes o infraccions penals?	☐ Sí ☐ No
Si es fa ús d'IA, el conjunt de dades d'entrenament del model conté dades personals o s'han utilitzat dades que es poden considerar anònimes?	☐ Dades personals ☐ Anònim
Si s'utilitzen dades personals, el proveïdor d'IA ha dut a terme una AIPD?	☐ Sí ☐ No
[Proveïdor d'IA] En cas d'usar un model entrenat a partir d'un conjunt de dades que es pot considerar anònim, s'ha avaluat el risc de reidentificació?	☐ Sí ☐ No
[Responsable del desplegament] En cas d'ús d'IA, el conjunt de dades utilitzat per contextualitzar el funcionament del sistema (p. ex. afinament - *fine-tuning*) conté dades personals (incloses les obtingudes mitjançant raspat web - *web scraping*)?	☐ Sí ☐ No

1.2 Processos de tractament

L'objectiu d'aquesta secció és identificar els diferents components del procés, quan la IA s'utilitzi en fases o funcionalitats diferents dins de la mateixa finalitat general.

Procés	
Descripció	
El procés incorpora intel·ligència artificial (sistema o component)?	☐ Sí ☐ No (Vegeu apartat Descripció i anàlisi del sistema d'IA)
Dades tractades	
Resultat del procés	

Procés	
Persona destinatària	
Lloc del tractament	

Procés	
Descripció	
El procés incorpora intel·ligència artificial (sistema o component)?	☐ Sí ☐ No (Vegeu apartat Descripció i anàlisi del sistema d'IA)
Dades tractades	
Resultat del procés	
Persona destinatària	
Lloc del tractament	

Procés	
Descripció	
El procés incorpora intel·ligència artificial (sistema o component)?	☐ Sí ☐ No (Vegeu apartat Descripció i anàlisi del sistema d'IA)
Dades tractades	
Resultat del procés	
Persona destinatària	
Lloc del tractament	

1.3 Descripció i anàlisi del sistema d'IA

Quin tipus de sistema d'IA és?	☐ Model d'IA de propòsit general (GPAI) (model que pot utilitzar-se per a moltes tasques diferents) ☐ GPAI amb risc sistèmic (models d'IA molt potents, amb impacte potencial ampli i amb obligacions addicionals segons la normativa) ☐ Sistema IA generativa (IA capaç de generar contingut nou, com ara text, imatges, àudio, vídeo, codi, etc.) ☐ Sistema basat en GPAI (aplicació construïda a partir d'un model d'IA de propòsit general) ☐ Sistema IA agentiva (IA capaç d'actuar de manera relativament autònoma per assolir objectius concrets) ☐ Sistema d'IA específic. ☐ Altres. Especifiqueu: _____

Tipologia funcional	☐ IA discriminativa o classificadora (classifica, categoritza o identifica patrons) ☐ IA predictiva (estima probabilitats, riscos o esdeveniments futurs) ☐ IA generativa (genera text, imatges, àudio, vídeo, codi o altres continguts) ☐ IA agentiva (planifica, decideix o executa accions amb diferents graus d'autonomia) ☐ Sistema de recomanació o suport a la decisió (proposa opcions, recomanacions o decisions) ☐ Sistema de detecció d'anomalies o frau ☐ Sistema conversacional (xatbot, assistent virtual o copilot) ☐ Sistema de visió artificial (processa imatges o vídeo) ☐ Sistema multimodal (combina text, imatge, àudio, vídeo o altres modalitats) ☐ Sistema robotitzat o físic (robots, dispositius intel·ligents o vehicles autònoms) ☐ Altres. Especifiqueu: _____
Grau d'autonomia	☐ Assistència a l'usuari (*human-in-the-loop*) ☐ Recomanació amb validació humana obligatòria ☐ Execució semiautònoma ☐ Execució autònoma supervisada ☐ Execució autònoma sense intervenció humana ☐ Altres. Especifiqueu: _____

Arquitectura del sistema	☐ Model propi desenvolupat o entrenat per l'organització ☐ Model comercial de tercers ☐ Model de codi obert (*open source*) ☐ Sistema amb ajustament (*fine-tuning*) ☐ Sistema basat en RAG (generació augmentada amb recuperació d'informació) ☐ Sistema híbrid (combinació de diversos models o tecnologies) ☐ Altres. Especifiqueu: _____
Tecnologies de millora de la privacitat (PETs)	☐ No s'utilitzen PET ☐ Anonimització ☐ Pseudonimització ☐ Privacitat diferencial ☐ Aprenentatge federat ☐ Xifrat homomòrfic ☐ Computació multipart segura (SMPC) ☐ Entorns d'execució de confiança (TEE) ☐ Computació confidencial ☐ Dades sintètiques ☐ Proves de coneixement zero (ZKP) ☐ Desaprenentatge automàtic (*machine unlearning*) ☐ Altres. Especifiqueu: _____

Modalitats de dades processades	☐ Text ☐ Imatges ☐ Àudio ☐ Vídeo ☐ Documents ☐ Dades estructurades (bases de dades, fitxers, fulls de càlcul) ☐ Dades biomètriques ☐ Dades de geolocalització ☐ Altres. Especifiqueu: _____
Origen de les dades personals tractades pel sistema d'IA	☐ Dades internes de l'organització ☐ Dades facilitades pels usuaris ☐ Dades procedents d'altres administracions o entitats ☐ Dades obertes (*open data*) ☐ Raspat web (*web scraping*) ☐ Dades adquirides a tercers ☐ Dades sintètiques ☐ Altres. Especifiqueu: _____

Quines són les finalitats (objectius específics) del sistema d'IA?	☐ Suport a la presa de decisions humanes ☐ Generació de contingut o recomanacions ☐ Classificació o perfilat de persones ☐ Automatització de decisions ☐ Automatització de processos operatius ☐ Altres. Especifiqueu: _____
[Proveïdor d'IA] Les eines d'IA utilitzades per al tractament de dades (per exemple, xarxes neuronals convolucionals profundes, màquines de vectors de suport, etc.) utilitzen la menor quantitat possible de dades personals per al fi previst?	☐ Sí ☐ No
[Proveïdor d'IA] S'ha documentat, si correspon, la necessitat d'utilitzar l'aprenentatge automàtic, en particular l'aprenentatge profund?	☐ Sí ☐ No

[Proveïdor d'IA] Es poden tenir en compte opcions de disseny d'IA amb vista a la protecció de dades des del disseny (aprenentatge federat, computació multipartita segura, xifratge homomòrfic, etc.)?	☐ Sí ☐ No En cas afirmatiu, quines?
Quines són les principals característiques del sistema?	
Enumereu els processos del tractament amb què opera la IA (enllaçar amb el punt 1.2 Processos de tractament)	
En quins països s'oferirà?	
Identificació dels possibles titulars de drets: qui són els individus o grups que poden veure's afectats pels sistemes d'IA? S'hi inclouen individus o grups vulnerables?	

1.4 Actors que intervenen en el tractament

Els actors que intervenen en el tractament, la seva funció i les dades que tracten són importants a l'hora de determinar els riscos del tractament.

		Rol a efectes del RIA	Rol a efectes de l'RGPD
Nom		☐ Proveïdor ☐ Responsable del desplegament	☐ Responsable ☐ Encarregat
Processos en què intervé			
Descripció			

Nom		☐ Proveïdor ☐ Responsable del desplegament	☐ Responsable ☐ Encarregat
Processos en què intervé			
Descripció			

Nom		☐ Proveïdor ☐ Responsable del desplegament	☐ Responsable ☐ Encarregat
Processos en què intervé			
Descripció			

Nom		☐ Proveïdor ☐ Responsable del desplegament	☐ Responsable ☐ Encarregat
Processos en què intervé			
Descripció			

Nom		☐ Proveïdor ☐ Responsable del desplegament	☐ Responsable ☐ Encarregat
Processos en què intervé			
Descripció			

2. Necessitat de dur a terme una AIPD i una FRIA

No cal fer una AIPD (art. 35 RGPD), si és d'aplicació algun dels supòsits següents:

Supòsit	
El tractament té naturalesa, abast, context i finalitat semblant a un altre tractament per al qual ja s'ha fet una AIPD.	
El tractament té una base jurídica en el dret de la UE o d'un estat membre, i ja s'ha fet una AIPD en el moment d'adoptar aquesta base jurídica.	

Justificació

Si cap dels supòsits anteriors és d'aplicació, si el tractament pot comportar un risc greu per als drets i les llibertats de les persones cal fer una AIPD.

El Grup de Treball de l'Article 29 (GT29) va proporcionar una llista de característiques que poden ser indicatives d'un risc elevat.

2.1 Necessitat de dur a terme una AIPD

Fitxa tècnica de l'AIPD[1]	
Versió actual i registre de versions (explicant l'historial dels canvis realitzats a la informació continguda a la plantilla AIPD per a aquest tractament, si n'hi ha)	
L'equip implicat en aquesta AIPD (proporcionant detalls dels seus rols, tasques, responsabilitats, etc.)	
Directrius, estàndards, codis de conducta i altres materials de referència	

[1] La ficha tècnica es basa en la Verssió 1.0 de la Plantilla per a la realització d'una avaluació d'impacte en protecció de dades del CEPD, adoptada el 10 de març de 2026.

Fitxa tècnica de l'AIPD[1]

utilitzats per dur a terme aquesta AIPD.			
Raons per dur a terme l'AIPD (es pot marcar més d'una casella de selecció)	1. Nova activitat de tractament, l'AIPD probablement serà necessària a causa de l'alt risc (obligació segons l'article 35.3 RGPD):	Avaluació sistemàtica i extensa dels aspectes personals relacionats amb les persones físiques basada en el tractament automatitzat, inclòs el perfilat, i en què es basen decisions que produeixen efectes legals sobre la persona física o que l'afecten significativament.	☐ Sí ☐ No
		Tractament a gran escala de categories especials de dades esmentades a l'article 9.1 RGPD o de dades personals relacionades amb condemnes penals i delictes esmentats a l'article 10.	☐ Sí ☐ No
		Monitoratge sistemàtic d'una àrea d'accés públic a gran escala.	☐ Sí ☐ No
	2. Nova activitat de tractament, AIPD possiblement requerida a causa d'un probable alt risc (obligació legal, segons la legislació nacional)	Justificació:	
	3. Nova activitat de tractament, possiblement requerida a causa del probable alt risc (seguint el CEPD i les directrius nacionals):	Avaluació o puntuació, inclòs perfilat i predicció, especialment dels aspectes relacionats amb el rendiment laboral del subjecte, situació econòmica, salut, preferències o interessos personals, fiabilitat o comportament, ubicació o moviments.	☐ Sí ☐ No
		Presa de decisions automatitzada amb efecte legal o significatiu similar:	☐ Sí ☐ No

Fitxa tècnica de l'AIPD[1]

		tractament que té com a objectiu prendre decisions sobre subjectes de dades que produeixen "efectes legals sobre la persona física" o que "afecten de manera similar la persona física".	
		Monitoratge sistemàtic: tractament utilitzat per observar, monitorar o controlar subjectes de dades, incloses dades recollides a través de xarxes o "un monitoratge sistemàtic d'una àrea accessible públicament".	☐ Sí ☐ No
		Dades sensibles o dades de caràcter altament personal: això inclou categories especials de dades personals, tal com es defineix a l'article 9 (per exemple, informació sobre les opinions polítiques dels individus). També, dades personals relacionades amb condemnes penals o delictes segons la definició de l'article 10 RGPD.	☐ Sí ☐ No
		Dades tractades a gran escala, considerant el nombre de subjectes implicats, ja sigui com un nombre específic o com una proporció de la població rellevant: el volum de dades i/o la gamma de diferents elements de dades que s'estan tractant; la durada, o permanència, de l'activitat de tractament de dades; l'extensió geogràfica de l'activitat de tractament.	☐ Sí ☐ No
		Comparació o combinació de conjunts de dades.	☐ Sí ☐ No

Fitxa tècnica de l'AIPD[1]

		Dades sobre subjectes vulnerables (a causa del desnivell de poder creixent entre els subjectes i el responsable de la informació de dades, cosa que significa que les persones potser no poden consentir fàcilment, oposar-se al tractament de les seves dades o exercir els seus drets).	☐ Sí ☐ No
		Ús innovador o aplicació de noves solucions tecnològiques o organitzatives.	☐ Sí ☐ No
		Quan el tractament en si mateix "impedeix que els subjectes exerceixin un dret o utilitzin un servei o un contracte".	☐ Sí ☐ No
		Altres (per exemple, llista nacional sobre les operacions de tractament subjectes al requisits d'una avaluació d'impacte de protecció de dades)	Indiqueu quines:
	4- Nova activitat de tractament, AIPD necessària o beneficiosa	Opinió o recomanació del DPD	☐ Sí ☐ No
		Opinió o recomanació dels subjectes de dades (o dels seus representants).	☐ Sí ☐ No
		Exigida per un codi de conducta, estàndard, bones pràctiques, etc.	☐ Sí ☐ No

Fitxa tècnica de l'AIPD[1]

		Altres (per exemple, gestionar riscos o demostrar responsabilitat i construir confiança).	Indiqueu quines:
	5. Activitats de tractament d'alt risc existents, per a les quals hi ha hagut un canvi en els riscos:	El tractament de dades ha canviat.	☐ Sí ☐ No
		El context organitzatiu o social de l'activitat de tractament ha canviat.	☐ Sí ☐ No
		Com?	
Abast d'aquesta AIPD (què s'ha considerat i què s'ha deixat fora de l'avaluació, i per què).			
Data de finalització			
Data de validació formal (aprovació per un funcionari responsable de l'AIPD com a completa i acabada)			
L'AIPD (o parts d'aquesta) està pensada per ser publicada o compartida externament?	☐ No	☐ Sí, es publicarà. Com?	☐ Sí, es compartirà externament. Com?

Cal fer l'AIPD? ☐ Sí ☐ No

Justificació:

Si s'ha nomenat un DPD, cal considerar la seva opinió respecte de la necessitat de fer una AIPD.

Opinió del DPD respecte de la necessitat de fer una AIPD

2.2 Necessitat de dur a terme una FRIA

A continuació, s'indiquen els requisits de necessitat a efectes de l'article 27 RIA. Si hi ha respostes afirmatives (*sí*) a les preguntes relatives a l'àmbit objectiu i/o a l'àmbit subjectiu, cal fer una FRIA.

Tanmateix, l'avaluació de l'impacte sobre els drets fonamentals també forma part del sistema de gestió de riscos a què es refereix l'article 9, que els proveïdors d'IA han d'adoptar, per a la qual cosa es pot emprar el model FRIA.

Àmbit objectiu	El sistema està classificat com a alt risc segons l'article 6.2 RIA? (art. 27.1)	☐ Sí ☐ No
	No és un sistema d'IA destinat a ser utilitzat com a component de seguretat en la gestió i el funcionament de les infraestructures digitals crítiques, trànsit de vehicles o subministrament d'aigua, gas, calefacció o electricitat?	☐ Sí ☐ No
	El sistema està inclòs en algun dels àmbits enumerats als punts 1 i del 3 al 8 de l'annex III?	☐ Sí ☐ No
		Quin?
Àmbit subjectiu	El responsable del desplegament de sistemes d'IA d'alt risc és un organisme de dret públic:	☐ Sí ☐ No
	El responsable del desplegament de sistemes d'IA	☐ Sí ☐ No

	d'alt risc és una entitat privada que presta serveis públics:		
	El responsable del desplegament és algun dels que s'esmenten a l'annex III, punt 5, lletres *b* i *c*.	☐ Sí ☐ No	
		Quin?	
Qüestions generals	És el primer ús del sistema d'IA?	☐ Sí ☐ No	
	Hi ha un FRIA previ per al mateix sistema o un de similar?	☐ Sí ☐ No	
	El proveïdor ha facilitat una avaluació d'impacte FRIA reutilitzable?	☐ Sí ☐ No	
	En cas afirmatiu, quin element ha canviat o ha deixat d'estar actualitzat que justifica la necessitat de refer el FRIA	la finalitat	☐ Sí ☐ No
		el context d'ús	☐ Sí ☐ No
		els processos	☐ Sí ☐ No
		les categories de persones afectades / col·lectius	☐ Sí ☐ No
		la freqüència o intensitat d'ús	☐ Sí ☐ No
		els riscos potencials	☐ Sí ☐ No
		la supervisió humana	☐ Sí ☐ No

Si (i) ja s'ha efectuat una FRIA prèviament o (ii) n'hi ha una FRIA del proveïdor que ja cobreix tots els riscos rellevants, no cal una nova FRIA. Això, sempre i quan tots els riscos s'hagin analitzat en relació amb el context d'ús i no hi hagi hagut canvis.

En relació amb l'AIPD (art. 27.3 RIA)	Existeix una AIPD d'acord amb l'article 35 RGPD relacionada amb el sistema?	☐ Sí ☐ No
	Quines parts cal complementar amb un FRIA?	

3. Avaluació d'Impacte en Protecció de Dades

3.1 Necessitat i proporcionalitat

L'avaluació de la necessitat i proporcionalitat del tractament es fa en relació amb la finalitat del tractament, que s'ha descrit a la secció anterior.

Necessitat i proporcionalitat des de la perspectiva del SIA	Necessitat social o de política pública	El sistema aporta algun benefici directe a “la humanitat”? (considerant 27)	☐ Sí ☐ No
		Contribueix a objectius públics (equitat, transparència, accessibilitat, eficiència)?	☐ Sí ☐ No
		Respon a problemes estructurals (saturació de serveis, manca de personal, etc.)?	☐ Sí ☐ No
		El sistema és socialment acceptable i comprensible per als usuaris afectats?	☐ Sí ☐ No
	Avaluació inspirada en polítiques públiques	Quin problema o necessitat concreta es vol resoldre amb aquest sistema d’IA?	
		Per què aquest problema és rellevant o crític per a l’organització?	
		Quines solucions no algorítmiques o tradicionals hi ha actualment?	
		Justifica perquè el “no fer res” (o mantenir la situació actual) no és una opció i quins beneficis específics aporta la IA (eficiència, precisió, escalabilitat)?	
	Necessitat d’utilitzar el tipus concret d’IA seleccionat	Hi ha alternatives igual d’efectives amb menor impacte en drets?	☐ Sí ☐ No
		En cas afirmatiu, per què no seria suficient una IA de baix risc o un sistema més simple, o bé per què s’ha descartat l’alternativa tecnològica “més simple”?	Justificació

		El nivell d'automatització és realment necessari per assolir la finalitat?	☐ Sí ☐ No

3.1.1 Finalitat del tractament

En principi, les dades recollides s'utilitzen per assolir la finalitat del tractament que va motivar la recollida. Ara bé, en alguns casos, el Reglament permet el tractament de dades que han estat recollides amb una finalitat diferent.

S'utilitzen dades recollides amb una finalitat diferent a la del tractament original?	☐ Sí ☐ No

En cas afirmatiu

Les següents condicions permeten el tractament de les dades amb una finalitat diferent a la de recollida.	
S'ha obtingut el consentiment de les persones interessades pel tractament amb la nova finalitat.	☐ Sí ☐ No
El tractament esta basat en el dret de la Unió o dels estats membres que constitueix una mesura per salvaguardar:	
La seguretat nacional.	☐ Sí ☐ No
La defensa.	☐ Sí ☐ No
La seguretat pública.	☐ Sí ☐ No
La prevenció, la investigació, la detecció i el tractament de delictes penals.	☐ Sí ☐ No
Altres objectius importants d'interès públic.	☐ Sí ☐ No
La protecció de la independència judicial i dels procediments judicials.	☐ Sí ☐ No
La prevenció, la investigació, la detecció i el tractament d'infraccions en normes deontològiques.	☐ Sí ☐ No

En cas afirmatiu

La protecció de la persona interessada o dels drets i llibertats d'altres.	☐ Sí ☐ No
L'execució de demandes civils.	☐ Sí ☐ No

Si no aplica cap de les condicions anteriors, cal que la nova finalitat sigui compatible amb la finalitat que va motivar la recollida de les dades.

Finalitat inicial.	
Dades.	
Nova finalitat.	
Justificació de la compatibilitat.	

Finalitat inicial.	
Dades.	
Nova finalitat.	
Justificació de la compatibilitat.	

3.1.2 Principis de licitud

3.1.2.1 Base legal per al tractament

Un tractament és lícit si aplica alguna de les bases legals següents:

La persona interessada ha donat el seu consentiment per al tractament de les seves dades personals, per una o diverses finalitats específiques.	☐ Sí ☐ No
El tractament és necessari per executar un contracte en què la persona interessada n'és part o per aplicar mesures precontractuals.	☐ Sí ☐ No
El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.	☐ Sí ☐ No

La persona interessada ha donat el seu consentiment per al tractament de les seves dades personals, per una o diverses finalitats específiques.	☐ Sí ☐ No
El tractament és necessari per protegir interessos vitals de la persona interessada o d'una altra persona física.	☐ Sí ☐ No
El tractament és necessari per complir una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament.	☐ Sí ☐ No
El tractament és necessari per satisfer els interessos legítims del responsable del tractament o d'un tercer, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de la persona interessada (en particular, quan és un menor).	☐ Sí ☐ No

Justificació de la licitud del tractament.

A banda, cal que el tractament no incorri en cap il·lícit en un sentit més ampli. Per exemple, infringir el copyright o acords contractuals.

Confirma que el tractament no incorre en cap tipus d'il·lícit.

3.1.2.2 Tractament de dades de menors

Els menors necessiten una protecció especial en el tractament de les seves dades, perquè poden no ser conscients dels riscos que comporta.

El tractament ofereix serveis de la societat de la informació a infants i té com a base el consentiment?	☐ Sí ☐ No
En cas afirmatiu, s'ha tingut en compte l'edat mínima de consentiment?	☐ Sí ☐ No
S'utilitzen les dades del menor per elaborar perfils i/o per prendre decisions total o parcialment automatitzades sobre ells?	☐ Sí ☐ No

3.1.2.3 Tractament de categories especials de dades

Es tracten dades de categories especials?	☐ Sí ☐ No

En cas afirmatiu

El tractament de categories especials de dades està prohibit, llevat que apliqui algun dels supòsits següents.	
La persona interessada ha donat el seu consentiment explícit per al tractament amb una finalitat específica, tret que el dret de la UE o de l'estat membre no ho permeti.	☐ Sí ☐ No
El tractament és necessari per complir obligacions o per exercir drets en l'àmbit del dret laboral i de la seguretat i la protecció social.	☐ Sí ☐ No
El tractament és necessari per protegir interessos vitals de la persona interessada o d'una altra persona física, en el supòsit que l'interessat no estigui capacitat per donar el consentiment.	☐ Sí ☐ No
El tractament és legítim i amb garanties, fet per una associació sense ànim de lucre de caràcter polític, filosòfic, religiós o sindical, sempre que el tractament afecti persones amb qui mantenen contactes en relació amb aquestes finalitats i les dades no es comuniquin a tercers sense el consentiment de les persones interessades.	☐ Sí ☐ No
El tractament fa referència a dades que l'interessat ha fet manifestament públiques.	☐ Sí ☐ No
El tractament és necessari per formular, exercir o defensar reclamacions, o quan els tribunals actuen en la seva funció judicial.	☐ Sí ☐ No
El tractament és necessari per raons d'interès públic essencial.	☐ Sí ☐ No
El tractament és necessari per a finalitats de medecina preventiva o laboral, avaluació de la capacitat laboral del treballador, diagnòstic mèdic, prestació d'assistència o tractament de tipus sanitari o social.	☐ Sí ☐ No
El tractament és necessari per raons d'interès públic en l'àmbit de la salut pública.	☐ Sí ☐ No
El tractament és necessari amb la finalitat d'arxiu amb interès públic, investigació científica o històrica, o amb finalitat estadística.	☐ Sí ☐ No
[Proveïdor d'IA] El tractament és necessari per detectar i corregir els biaixos associats als sistema d'IA d'alt risc, d'acord amb l'article 10.5 RIA?	☐ Sí ☐ No

En cas afirmatiu

[Responsable del desplegament / Proveïdor d'IA] En cas afirmatiu, s'han establert mesures per evitar la recuperació de les dades personals utilitzades en el moment de fer ús del sistema d'IA?	☐ Sí ☐ No

Justificació de la licitud del tractament de dades de categories especials

3.1.2.4 Tractament de dades penals

Es tracten dades relatives a condemnes o infraccions penals?	☐ Sí ☐ No

En cas afirmatiu

Tot i que les dades relatives a condemnes o infraccions penals no són categories especials de dades, hi ha un requisit addicional per tractar-les: el tractament només és pot portar a terme sota la supervisió de les autoritats públiques o quan ho autoritzi el dret de la unió o de l'estat membre.

Justificació de la licitud del tractament de dades penals

3.1.2.5 Validesa del consentiment

Si un tractament té com a base legal el consentiment, cal que es compleixin les següents condicions perquè aquest sigui vàlid:

El responsable pot demostrar que l'ha recollit.	☐ Sí ☐ No
La sol·licitud de consentiment és intel·ligible, de fàcil accés i en un llenguatge clar.	☐ Sí ☐ No
L'execució d'un contracte no es pot supeditar a rebre el consentiment respecte de dades personals no necessàries per executar el contracte.	☐ Sí ☐ No

El responsable pot demostrar que l'ha recollit.	☐ Sí ☐ No
S'ha informat les persones interessades de la possibilitat de retirar el consentiment en qualsevol moment.	☐ Sí ☐ No
Si la persona interessada no vol consentir, se li ofereix una opció alternativa que no la perjudica ni implica tracte desfavorable.	☐ Sí ☐ No

3.1.2.6 Transferències de dades

Per evitar que les persones interessades vegin reduïts els seus drets, L'RGPD és especialment restrictiu amb les transferències de dades amb països on el RGPD no aplica.

És fan transferències a tercers països o a organitzacions internacionals?	☐ Sí ☐ No

En cas afirmatiu

Aquestes transferències estan permeses si la Comissió Europea considera que el país o organització ofereix un nivell adequat de protecció, si s'han establert les garanties suficients segons l'article 46 o si aplica alguna de les excepcions de l'article 49.

Dades transferides.	
País.	
Condició que permet la transferència.	

Dades transferides.	
País.	
Condició que permet la transferència.	

3.1.2.7 Licitud del tractament per entrenar la IA

[Proveïdor d'IA] Si es reutilitzen dades disponibles públicament o dades obtingudes d'un tercer (per exemple, un proveïdor de dades) per entrenar la IA, comproveu que no està reutilitzant un conjunt de dades que s'hagi creat clarament de manera il·lícita?	☐ Sí ☐ No
La font de les dades està clarament identificada i documentada?	☐ Sí ☐ No
El conjunt de dades és el resultat d'un delicte o una infracció (filtració, robatori, etc.) o ha estat objecte d'una condemna o sanció pública per part d'una autoritat competent i, com a conseqüència, s'ha hagut de retirar o se n'ha prohibit l'ús?	☐ Sí ☐ No
Les condicions en les quals es van recollir les dades estan prou documentades?	☐ Sí ☐ No
El conjunt de dades conté informació sensible o que infringeixi drets? Si és així, es fan comprovacions exhaustives per garantir que el tractament és lícit?	☐ Sí ☐ No

3.1.3. Principi de lleialtat del tractament

Un tractament és lleial si fa un ús de les dades previsible per part de les persones interessades, i del tractament no se'n deriven conseqüències adverses pera a les persones interessades que no siguin justificables.

Justificació de tractament lleial

3.1.4 Principi de minimització

Les dades han de ser adequades, rellevants i limitades a l'estrictament necessari per acomplir la finalitat del tractament.

Tipus de dades.	

Justificació de l'adequació, la rellevància i la necessitat

Tipus de dades.	

Justificació de l'adequació, la rellevància i la necessitat

Tipus de dades.	

3.1.5 Principi de limitació del termini de conservació

Les dades personals no s'han de conservar més temps de l'estrictament necessari per complir amb la finalitat del tractament. A la descripció del tractament, es va especificar el termini de conservació de les dades. Cal justificar que els terminis donats compleixen el principi de limitació del termini de conservació.

Justificació que els terminis de conservació donats compleixen amb la limitació del termini de conservació

Cal que els mecanismes establerts per esborrar les dades siguin efectius (és automàtic o s'ha d'activar manualment? romanen les dades a les còpies de seguretat del sistema un cop esborrades? quant de temps i com es garanteix que no es tracten?

Descriu els mecanismes establerts per esborrar les dades

Les dades es poden conservar indefinidament amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística.

Es conserven dades amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística.	

En cas afirmatiu, quines mesures s'han implantat per garantir el principi de minimització

3.1.6 Principi d'exactitud

El tractament de dades inexactes pot afectar negativament les persones. El principi d'exactitud demana que les dades siguin exactes i que es prenguin les mesures adequades per garantir que les que siguin inexactes s'actualitzin o s'esborrin sense dilació.

Controls de la qualitat de les dades[2]

Mesures per corregir les dades

3.1.7 Riscos per les persones

L'objectiu d'aquest punt és identificar els possibles efectes negatius sobre les persones, quantificar-los i si és necessari proposar mesures per mitigar-los.

En aquesta secció avaluarem el tractament tal i com està dissenyat. És a dir, no considerem els casos en que falla la seguretat del sistema (sigui aquesta fallada accidental o intencionada).

En la identificació dels potencials efectes negatius del tractament sobre les persones convé tenir en compte el punt de vista de les persones interessades i del delegat de protecció de dades.

Potencials efectes negatius del tractament sobre les persones

Per cadascun dels efectes negatius identificats, cal estimar el nivell de risc associat. El risc depèn de dos factors: l'impacte que té sobre les persones (baix, mitjà, alt o molt alt) i la probabilitat que es materialitzi (baixa, mitjana, alta). L'impacte s'estima directament dels

[2] Inclou la fase d'entrenament dels models d'IA

potencials efectes. Per determinar la probabilitat, cal analitzar en quines circumstancies fan que els efectes negatius és materialitzin (les amenaces) i estimar la probabilitat d'aquestes.

El risc es determina, en funció de l'impacte i de la probabilitat, seguint la taula següent:

	Impacte			
Probabilitat	Baix	Mitjà	Alt	Molt alt
Baixa	Risc baix	Risc baix	Risc mitjà	Risc alt
Mitjana	Risc baix	Risc mitjà	Risc alt	Risc alt
Alta	Risc mitjà	Risc alt	Risc alt	Risc alt

Primer s'estimarà el risc associat a cada amenaça. El risc global serà el màxim dels riscos de les amenaces.

Efecte sobre les persones

Impacte:

Amenaça	Probabilitat	Risc

Risc estimat

Efecte sobre les persones

Impacte:

Amenaça	Probabilitat	Risc

Risc estimat:

Efecte sobre les persones

Llevat que el risc sigui baix, cal buscar mesures per reduir-lo. Això és especialment necessari en els casos de risc alt o molt alt. Si no és possible reduir un risc alt, abans de començar el tractament cal consultar l'autoritat de protecció de dades competent sobre la idoneïtat del tractament.

En cas que s'hagi alterat el tractament inicial per fer-lo menys lesiu per les persones, caldrà revisar i actualitzar les seccions anteriors de l'AIPD.

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

3.1.8 Necessitat i proporcionalitat del tractament

Amb la informació recollida en aquesta secció, cal justificar que el tractament és necessari (propòsit buscat no es pot atènyer amb cap altre mesura més moderada) i proporcional (no provoca més danys que beneficis).

Justificació de la idoneïtat del tractament per al propòsit que es busca

Justificació de la necessitat del tractament

Justificació que el tractament és proporcional

3.1.9 Opinió de les persones interessades

L'RGPD estableix que, si és possible, cal recollir l'opinió de les persones interessades sobre el tractament.

Opinió les persones interessades sobre la necessitat i la proporcionalitat del tractament

En cas que no es considera apropiat recollir l'opinió de les persones interessades, cal justificar-ho.

Per què no s'ha recollit l'opinió de les persones interessades?

Si l'opinió de les persones interessades respecte al tractament difereix de la visió que el responsable ha donat a l'apartat 2.7 i es pretén portar endavant el tractament, cal justificar el perquè.

Per què es porta endavant el tractament tot i les discrepàncies de les persones interessades?

3.2 Controls per garantir els drets de les persones

3.2.1 Controls pel dret a tenir informació transparent

La transparència és transversal i ha de ser present en totes les comunicacions amb les persones interessades.

Tota comunicació amb les persones interessades ha de ser concisa, intel·ligible, de fàcil accés i ha de fer ús d'un llenguatge clar i senzill.	☐ Sí ☐ No

El reglament regula com s'ha de fer aquesta comunicació.

La informació es donarà per escrit (incloent mitjans electrònics).	☐ Sí ☐ No
Pel cas de peticions fetes amb mitjans electrònics, la informació es donarà preferentment de forma electrònica.	☐ Sí ☐ No
Si la persona interessada ho demana, la informació es donarà oralment.	☐ Sí ☐ No

El responsable ha de respondre les peticions d'exercici de drets d'una persona interessada dins uns terminis establerts:

Sense demora indeguda i no més enllà d'un mes.	☐ Sí ☐ No
Si la complexitat o el número de peticions ho justifica, es pot estendre el període en dos mesos. En aquest cas cal informar de les raons dins el primer mes.	☐ Sí ☐ No

Si el responsable no ha de respondre a la petició d'exercici de drets d'una persona interessada, cal:

Avisar la persona interessada d'aquest fet sense demora indeguda i com a màxim en un mes.	☐ Sí ☐ No
Explicar les raons per no portar a terme la petició (per exemple, la petició és repetitiva o el responsable no pot identificar la persona interessada).	☐ Sí ☐ No
Informar de la possibilitat de recórrer la decisió davant una autoritat supervisora o un jutjat.	☐ Sí ☐ No

Només si la petició és excessiva (per exemple, per repetitiva), es podrà cobrar un càrrec per cobrir els costos de tramitar-la.	☐ Sí ☐ No

3.2.2 Controls per al dret d'informació

A l'hora de recollir dades personals, el responsable del tractament ha d'informar les persones interessades de diferents aspectes del tractament.

[Responsable del desplegament] El proveïdor del sistema d'IA ha facilitat la informació necessària per complir el deure d'informar els interessats de manera adequada?[3]	☐ Sí ☐ No

Els articles 13 i 14 especifiquen que cal informar les persones interessades dels punts que es detallen a la taula següent:

La identitat i les dades de contacte del responsable.	☐ Sí ☐ No
Les dades de contacte del delegat de protecció de dades (si n'hi ha).	☐ Sí ☐ No
La finalitat del tractament.	☐ Sí ☐ No
La base legal del tractament.	☐ Sí ☐ No
L'interès legítim del responsable, si aquesta és la base legal del tractament.	☐ Sí ☐ No
Els destinataris o categories de destinataris de les dades.	☐ Sí ☐ No
El termini de conservació de les dades o el criteri emprat per determinar-lo.	☐ Sí ☐ No
La intenció de transmetre les dades fora de la UE, si escau.	☐ Sí ☐ No
La decisió de la Comissió Europea respecte de la suficiència de la seguretat que ofereix el país o organització destinatària.	☐ Sí ☐ No
L'existència del dret d'accés a les dades.	☐ Sí ☐ No
L'existència del dret de rectificació i supressió.	☐ Sí ☐ No
L'existència del dret de limitació del tractament.	☐ Sí ☐ No
L'existència del dret d'oposició al tractament.	☐ Sí ☐ No
L'existència del dret de portabilitat de dades.	☐ Sí ☐ No

[3] Aquest punt pren especial rellevància per complir correctament amb les obligacions establertes a l'article 86 del RIA.

La identitat i les dades de contacte del responsable.	☐ Sí ☐ No
L'existència del dret a revocar el consentiment (si aquesta és la base legal del tractament).	☐ Sí ☐ No
L'existència del dret a presentar una reclamació davant una autoritat de control.	☐ Sí ☐ No
Que la comunicació de les dades és un requisit legal o contractual, si escau.	☐ Sí ☐ No
L'existència de decisions automatitzades.	☐ Sí ☐ No
El propòsit de fer servir dades amb una finalitat diferent a la que va motivar la recollida, si s'escau.	☐ Sí ☐ No
La procedència de les dades, si no s'han obtingut directament de la persona interessada.	☐ Sí ☐ No

Hi ha algunes exempcions a l'obligatorietat d'informar, que depenen de la forma en què s'han recollit les dades.

- Si les dades s'han obtingut directament de la persona interessada, no hi ha l'obligació d'informar-la si ja disposa de la informació.
- Si les dades no s'han obtingut directament de la persona interessada, no cal informar-la si es dona alguna de les següents condicions: la persona interessada ja disposa d'aquesta informació, la comunicació és impossible o suposa un esforç desproporcionat, així està regulat per una norma de la UE o dels estats membres o la informació té caràcter confidencial sobre la base del secret professional.

Si no s'informa, cal justificar-ho.

S'aplica el dret d'informació a totes les dades tractades?	

Si aplica alguna exempció al dret d'informació, cal dir quina, a quines dades i justificar el perquè

Si s'informa les persones interessades, el Reglament determina quan cal fer-ho[4].

[4] RGPD art. 13(1) i 14(3),

Si les dades es recullen directament de les persones interessades, en el moment de recollir-les.	☐ Sí ☐ No
Si les dades es recullen indirectament, cal complir les condicions següents:	
En un període raonable de temps i no superior a un mes.	☐ Sí ☐ No
Si ens comuniquem amb les persones interessades, com a molt tard en el moment de la primera comunicació.	☐ Sí ☐ No
Si es volen comunicar les dades a tercers, abans de comunicar-les.	☐ Sí ☐ No

3.2.3 Controls per garantir el dret d'accés

La persona interessada té el dret d'obtenir del responsable del tractament la confirmació que s'estan tractant les seves dades i, en aquest cas, el dret d'accés a les dades personals i a la informació següent:

La finalitat del tractament.	☐ Sí ☐ No
Les categories de dades tractades.	☐ Sí ☐ No
Les persones destinatàries de les dades.	☐ Sí ☐ No
El termini de conservació de les dades.	☐ Sí ☐ No
Els drets a rectificar i suprimir les dades.	☐ Sí ☐ No
Els drets a limitar i oposar-se al tractament.	☐ Sí ☐ No
El dret a reclamar davant una autoritat de control.	☐ Sí ☐ No
Si les dades no s'han obtingut de la persona interessada, l'origen de les dades.	☐ Sí ☐ No
L'existència de decisions automatitzades, si escau.	☐ Sí ☐ No
Garanties en la transferència de dades fora de la UE, si escau.	☐ Sí ☐ No

A banda de conèixer quina informació s'ha de transmetre a les persones interessades, cal assegurar-se que es donen les condicions per fer efectiu el dret d'accés.

S'ha establert un procediment estàndard per la gestió de sol·licituds d'accés?	☐ Sí ☐ No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds d'accés?	☐ Sí ☐ No

3.2.4 Controls per garantir el dret de rectificació

Les persones tenen el dret a que és rectifiquin les seves dades, si aquestes no són exactes.

S'ha establert un procediment per la gestió de sol·licituds de rectificació?	☐ Sí ☐ No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de rectificació?	☐ Sí ☐ No

Si el responsable ha compartit les dades, cal que informi les persones destinatàries sobre la rectificació.

S'ha establert un procediment per notificar la rectificació a les persones destinatàries?	☐ Sí ☐ No

3.2.5 Dret de supressió

Les persones tenen el dret a que s'esborri la seva informació quan es dona algun dels següents casos:

- Les dades ja no són necessàries en relació amb la finalitat per què es van recollir.
- La persona interessada treu el seu consentiment i no hi ha cap altra base legal pel tractament.
- La persona interessada s'oposa al tractament i no hi ha cap altre factor superior que el legitimi.
- Les dades s'han tractat sense una base legal.
- Les dades s'han d'esborrar d'acord amb una obligació legal que afecta el responsable.
- Les dades s'utilitzen per oferir serveis de la societat de la informació a infants.

En canvi, el dret de supressió no aplica en els següents casos:

- Per exercir el dret a la llibertat d'expressió i d'informació.
- Per complir una obligació legal o en l'interès públic.
- Amb la finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, i amb finalitat estadística (si el compliment d'aquestes finalitats es veiés afectat per la supressió de les dades).
- Per presentar, exercir o defensar reclamacions legals.

El personal té capacitat per decidir si aplica el dret a supressió?	☐ Sí ☐ No

Es recomanable establir un canal estàndard perquè les persones interessades puguin demanar de fer efectiu el dret de supressió. Ara bé, cal assegurar-se que el personal està capacitat per detectar les sol·licituds que es facin per altres mitjans.

S'ha establert un procediment per la gestió de sol·licituds de supressió?	☐ Sí ☐ No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de supressió?	☐ Sí ☐ No

Si el responsable del tractament comparteix les dades, ha de prendre les mesures apropiades (tenint en compte els costos i la tecnologia disponible) per notificar les persones destinatàries sobre la petició de supressió.

S'ha establert un procediment per notificar la petició de supressió a les persones destinatàries?	☐ Sí ☐ No

3.2.6 Dret a limitar el tractament

L'article 18 dona a les persones el dret a limitar el tractament de les seves dades, en els casos següents:

- La persona interessada ha demanat la rectificació de les seves dades i el responsable està verificant si són exactes.
- Les dades s'han tractat sense una base legal.
- La persona interessada necessita que el responsable guardi les dades per iniciar, exercir o defensar una reclamació.
- La persona interessada s'ha oposat al tractament i el responsable està avaluant si els motius legítims del responsable prevalen sobre els de la persona interessada.

El personal està capacitat per decidir si aplica el dret a limitar el tractament?	☐ Sí ☐ No

Cal assegurar-se que el personal està capacitat per detectar les sol·licituds de limitació del tractament.

S'ha establert un procediment per la gestió de sol·licituds de limitació del tractament?	☐ Sí ☐ No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de limitació del tractament?	☐ Sí ☐ No

A l'hora de limitar el tractament, cal tenir en compte les diferents formes que aquest pot tenir: recollida de dades, anàlisi de dades, disseminació de resultats, etc.

Es tenen en compte totes les possibles formes de tractament a l'hora de limitar-lo?	☐ Sí ☐ No

Si s'han compartit dades, cal informar les persones destinatàries de les peticions de limitació del tractament.

S'ha establert un procediment per notificar la petició de limitació del tractament a les persones destinatàries?	☐ Sí ☐ No

3.2.7 Dret a la portabilitat de les dades

Les persones tenen el dret a demanar les dades que han facilitat al responsable del tractament en els següents cassos:

- Si el tractament està basat en el consentiment, o és necessari per executar un contracte o per aplicar mesures precontractuals.
- El tractament es fa amb mitjans automatitzats.

El dret a la portabilitat de dades no es limita a les dades que les persones han donat de forma explicita; també afecta les dades que s'han recollit de l'observació de les persones.

El personal està capacitat per decidir si aplica el dret a la portabilitat de dades?	☐ Sí ☐ No

El dret a la portabilitat de dades no ha d'afectar negativament a altres persones. En particular:

- Si les dades personals contenen informació d'una tercera persona, cal avaluar si aquesta darrera pot veure afectats els seus drets i llibertats.
- Si les dades estan associades a diverses persones (per exemple, un compte bancari compartit), cal buscar el consens de totes les persones interessades.

El procediment per fer efectiu el dret a la portabilitat de dades té en compte l'efecte sobre els drets i les llibertats de les altres persones?	☐ Sí ☐ No

Cal assegurar-se que el personal està capacitat per detectar les sol·licituds de portabilitat de dades.

S'ha establert un procediment per la gestió de sol·licituds de portabilitat de dades?	☐ Sí ☐ No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de portabilitat de dades?	☐ Sí ☐ No

El reglament determina la forma en la que s'ha de fer la portabilitat.

S'usa un format estructurat, d'ús comú i que sigui de fàcil lectura mecànica?	☐ Sí ☐ No

3.2.8 Dret d'oposició

Les persones tenen el dret a oposar-se al tractament de la seva informació quan aquest tractament es fa sobre la base de:

- L'interès públic o l'exercici de poders públics conferits al responsable del tractament.
- L'interès legítim del responsable del tractament.

En aquest cas, el responsable ha de cessar en el tractament, llevat que acrediti motius legítims que prevalguin sobre els drets de l'interessat.

El personal està capacitat per decidir si aplica el dret a d'oposició?	☐ Sí ☐ No

Cal assegurar-se que el personal està capacitat per detectar les sol·licituds d'oposició.

S'ha establert un procediment per la gestió de sol·licituds d'oposició al tractament?	☐ Sí ☐ No
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds d'oposició al tractament?	☐ Sí ☐ No

El reglament especifica com s'ha d'actuar en rebre una petició d'oposició al tractament en diversos casos.

Si la petició s'oposa al tractament amb finalitats de màrqueting, aquesta ha de ser acceptada sense excepció.	☐ Sí ☐ No
Si la petició s'oposa al tractament amb finalitat d'investigació científica o històrica, o amb finalitat estadística, ha de ser acceptada llevat que el tractament es faci en l'interès públic.	☐ Sí ☐ No

3.2.9 Dret a no ser objecte de decisions automatitzades

Es fa un tractament automatitzat que té efectes jurídics o altres efectes significatius per les persones?	☐ Sí ☐ No
En cas afirmatiu, quina base legal ho permet?	
És necessari per l'execució d'un contracte entre la persona interessada i el responsable.	☐ Sí ☐ No
Està autoritzat pel dret de la unió o d'un estat membre.	☐ Sí ☐ No

Es fa un tractament automatitzat que té efectes jurídics o altres efectes significatius per les persones?	☐ Sí ☐ No
La persona interessada ha donat el seu consentiment explícit.	☐ Sí ☐ No

La persona interessada sempre té dret a obtenir intervenció humana, a expressar el seu punt de vista i a impugnar la decisió.

Existeix un procediment perquè les persones puguin demanar intervenció humana, expressar el seu punt de vista i impugnar la decisió?	☐ Sí ☐ No
Hi ha personal a l'organització amb la capacitat de revisar les decisions i canviar-les?	☐ Sí ☐ No

Les decisions automatitzades només poden fer ús de categories especials de dades si hi ha el consentiment explícit de la persona interessada, o si el tractament es fa per protegir els interessos vitals de la persona interessada o d'una altra persona.

Es fa ús de categories especials de dades en el tractament automàtic?	☐ Sí ☐ No
En cas afirmatiu, quina base legal que ho permet?	
La persona interessada ha donat el seu consentiment explícit.	☐ Sí ☐ No
El tractament es fa per protegir els interessos vitals de la persona interessada o d'una altra persona.	☐ Sí ☐ No

3.3. Riscos en la seguretat de les dades

D'acord amb l'RGPD, les mesures emprades per protegir la informació han de ser apropiades al risc per als drets i les llibertats de les persones. En aquesta secció seguim una metodologia senzilla per analitzar els riscos relacionats amb la seguretat de les dades. És a dir, els riscos associats a la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades.

3.3.1 Impacte

Avaluem l'impacte que la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades personal tenen sobre la persona interessada.

Per fixar l'impacte sobre les persones de la pèrdua de la seguretat de les dades, cal tenir en compte les característiques del tractament. Entre d'altres:

- El tractament dades de categories especials o altres dades especialment sensibles (informació financera, localitzacions, etc.).

- La monitorització de persones.
- El tractament de dades de grups amb necessitats especials (menors, autoritats, etc.).
- El tractament de gran quantitat de dades de cada persona.

Amb l'objectiu de contextualitzar el càlcul de l'impacte, es plantegen diferents d'escenaris en que es perd alguna d'aquestes propietats.

Impacte que la pèrdua de la confidencialitat de les dades (és a dir, d'un accés no autoritzat a les dades) té sobre les persones.

Exemples de casos de pèrdua de confidencialitat:

- Pèrdua o robatori d'un ordinador que conté dades personals.
- Enviament per error de dades personals a persones no autoritzades.
- Possibilitat d'accedir de forma no autoritzada al compte d'una persona.
- Un error de configuració en una web exposa les dades personals de les seves persones usuàries.
- Robatori d'informació de les instal·lacions del responsable o de l'encarregat del tractament.
- Un empleat d'un centre mèdic consulta de forma no autoritzada l'expedient d'un pacient.

Impacte

Baix	Mitjà	Alt	Molt alt

Justificació

Impacte que la pèrdua de la integritat de les dades (és a dir, de la modificació no autoritzada de les dades) té sobre les persones.

- Un empleat o empleada modifica per error les dades d'un client.
- Un error en la xarxa de comunicacions altera les dades mentre estan en trànsit.
- Per motius operacionals, una empresa manté diverses còpies de les dades, però un canvi en alguna de les còpies no és propaga a les altres.
- Pèrdua de part d'un expedient, com a conseqüència d'una fallada en el sistema de tractament.

Impacte

Baix	Mitjà	Alt	Molt alt

Justificació

Impacte

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones.

Exemples de casos de pèrdua de la disponibilitat:

- Un fitxer és corromp o s'esborra i no hi ha una còpia de seguretat.
- Es perd un expedient del qual només hi havia una còpia en paper.
- Un servei de consulta de dades deixa d'estar disponible (per exemple, el servei per accedir al registres electrònics de salut).

Impacte

Baix	Mitjà	Alt	Molt alt

Justificació

L'impacte del sistema serà el màxim dels tres.

Impacte

Baix	Mitjà	Alt	Molt alt

Justificació

3.3.2 Probabilitat inicial

La taula següent mostra característiques del tractament que incrementen els riscos de seguretat de les dades. Estimarem la probabilitat de fallada en la seguretat en funció del número de característiques es compleixen.

Maquinari i programari	
Q1. El sistema de tractament està connectat a sistemes externs a l'organització? La connexió amb sistemes externs a l'organització incrementa l'exposició a amenaces, podent la informació ser capturada o modificada maliciosament mentre està en trànsit. Això es produeix, per exemple, quan s'han contractat serveis al núvol, es realitzen connexions en modalitat de teletreball als sistemes de l'organització o es permeten accessos a través d'internet a la xarxa interna per connectar-se a les bases de dades corporatives, entre d'altres supòsits.	☐ Sí ☐ No
Q2. Alguna part del tractament es fa a través d'internet? La interacció amb les persones interessades a través d'internet exposa el sistema de tractament a amenaces externes, com ara *phishing*, *SQL injection, man-in-the-middle attacks, DoS i XSS*. Aquestes amenaces poden comprometre el sistema de tractament i afectar les propietats de seguretat de les dades (confidencialitat, integritat i disponibilitat). Permetre que el personal accedeixi al sistema de tractament a través d'internet també incrementa l'exposició a atacs externs i, a banda, incrementa la possibilitat que el personal faci un mal ús de la informació (accidental o intencionat). Alguns exemples d'aquests tipus de tractament poden ser els tractaments que fan ús del correu electrònic, aquells en què el manteniment o la supervisió es fa a través d'internet o bé l'ús de serveis al núvol com ara Google Drive, Microsoft One Drive, Amazon Web Services (AWS), Microsoft Azure, entre d'altres.	☐ Sí ☐ No

Maquinari i programari

Q3. Manca document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament? Si el sistema de tractament no està ben dissenyat o els elements que el componen no estan configurats adequadament els riscos per a la seguretat de les dades s'incrementen. Per garantir un bon disseny i una bona configuració del sistema de tractament hi ha multitud de guies en seguretat amb diferent temàtica que es poden adoptar per seguir-les, com ara de disseny de la xarxa local, tallafocs, segmentació de xarxa, xarxes privades virtuals (VPN), configuració de sistema operatiu, antivirus, ús de contrasenyes segures, múltiple factor d'autenticació (MFA), etc. Disposar d'un document de bones pràctiques ajuda a dimensionar el sistema de tractament tenint en compte les necessitats computacionals, de comunicació, de seguretat i d'emmagatzematge. També permet configurar correctament el programari, aplicar una metodologia de desenvolupament que prioritzi la seguretat de les dades durant tot el cicle de vida de l'aplicació, utilitzar aplicacions segures en el núvol o establir criteris sobre l'ús i la tipologia de dades que es poden gestionar en aquest entorn, entre d'altres actuacions.	☐ Sí ☐ No
Q4. Manca document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament? Disposar d'un document de bones pràctiques que reculli aquests aspectes és essencial per garantir el manteniment, la monitorització i un pla de resposta a incidents del sistema adequats. El manteniment s'ha de fer tant dels dispositius i maquinari com del programari. La monitorització permet analitzar un incident un cop s'ha produït i ajuda a detectar comportaments sospitosos a fi d'evitar que l'incident tingui lloc, o per reduir-ne l'impacte. El pla de resposta a incidents permet tenir un enfocament sistemàtic per abordar i gestionar els incidents de seguretat. Aquest document de bones pràctiques pot recollir tasques importants com l'aplicació d'actualitzacions de seguretat del sistema operatiu, la realització de còpies de seguretat regulars, l'ús de sistemes automàtics de detecció o correlació d'esdeveniments de seguretat, així com la realització periòdica d'auditories per a la revisió de vulnerabilitats i la seguretat general, entre d'altres.	☐ Sí ☐ No
Q5. Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament? La seguretat física de les instal·lacions de tractament és essencial. Sense això, no es pot garantir la seguretat del sistema de tractament (ja sigui electrònic o no). Això pot donar-se, per exemple, quan el CPD no està degudament protegit amb un sistema que impedeixi l'accés a les persones no autoritzades o no està protegit contra accidents naturals i industrials (fallades elèctriques, inundacions, etc.), quan l'arxiu s'ha distribuït en diferents àrees de manera que no se'n pugui garantir la seguretat o quan es fa un ús de serveis al núvol sense tenir garanties que les instal·lacions del proveïdor estan degudament protegides, entre d'altres supòsits.	☐ Sí ☐ No

Ús del sistema de tractament

Q6. Hi ha una manca de claredat en la definició dels rols i les responsabilitats del personal? Una manca de claredat en la definició dels rols i les responsabilitats pot donar lloc a un ús descontrolat de les dades (ja sigui accidental o intencionat). Per exemple, un treballador només hauria de consultar les dades que li són necessàries per dur a terme les seves tasques. També ha de ser responsable de destruir la informació quan ja no sigui necessària, així com de garantir-ne la seguretat quan es comunica a una altra organització o persona, entre d'altres.	☐ Sí ☐ No
Q7. Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament? Quan els usos acceptables dels sistemes de tractament no estan definits clarament, s'incrementa el risc de fer-ne un mal ús i d'introduir vulnerabilitats al sistema. Per exemple, la instal·lació d'un programari de compartició de fitxers podria comportar la compartició involuntària d'informació o accedir a pàgines web malicioses podria facilitar l'entrada de programari maliciós i de robatori de dades, entre d'altres riscos.	☐ Sí ☐ No
Q8. El personal pot connectar dispositius externs al sistema? La connexió de dispositius externs (telèfon mòbil, memòria USB, etc.) al sistema de tractament pot representar un risc de seguretat, atès que pot facilitar l'entrada de programari maliciós, la introducció de vulnerabilitats i l'extracció no autoritzada d'informació. Per aquest motiu, és imprescindible establir una política clara que reguli l'ús de dispositius externs per part del personal de l'organització.	☐ Sí ☐ No
Q9. Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament? La manca d'un registre de les activitats (log file) pot afavorir les males pràctiques del personal i dificultar la investigació d'incidents un cop s'han produït, atesa la manca de traçabilitat, tal com estableix l'Esquema Nacional de Seguretat (ENS). Aquest fet compromet la capacitat de detectar, analitzar i respondre a possibles amenaces. Per tant, és necessari disposar d'un registre adequat que permeti conèixer qui accedeix als sistemes d'informació i assegurar que les activitats registrades siguin monitoritzades de manera efectiva.	☐ Sí ☐ No

Persones que intervenen en el tractament

Q10. El personal rep permisos que no són necessaris per complir les tasques que té encomanades? Com més gran sigui el nombre de persones que tenen accés a unes dades, més gran és la probabilitat que es produeixi un abús. Per evitar-ho, és essencial que el sistema controli l'accés del personal i autoritzi només els accessos que són estrictament necessaris per complir les tasques que té encomanades.	☐ Sí ☐ No
Q11. S'ha externalitat alguna part del tractament a un encarregat? L'encarregat és la persona física o jurídica, autoritat pública, servei o organisme que presta al responsable un servei que comporta el tractament de dades personals per compte d'aquest. Per exemple, una empresa o entitat pública que ofereix un servei d'allotjament d'informació en els seus servidors o el gestor d'un servei públic municipal, entre d'altres supòsits. L'externalització del tractament o part del tractament a un encarregat suposa una pèrdua de control sobre les dades. Cal escollir un encarregat que ofereixi garanties suficients respecte de la implantació i el manteniment de les mesures de seguretat apropiades, i definir clarament les seves responsabilitats.	☐ Sí ☐ No
Q12. Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD? Una manca de coneixements sobre l'ús que s'espera del sistema, sobre seguretat de la informació o sobre les obligacions i limitacions que imposa l'RGPD pot donar lloc a males pràctiques. Així, per exemple, el personal podria ser més propens a seguir les instruccions d'un correu de phishing o, a l'hora de desar documents, no ser conscient de garantir-ne la seguretat, entre d'altres situacions.	☐ Sí ☐ No
Q.13. Hi ha algun mecanisme de supervisió humana (IA)?	☐ Sí ☐ No

Altres característiques

Q14. L'empresa o altres empreses del sector han patit atacs darrerament? L'existència d'atacs anteriors ha de servir com a lliçó per identificar vulnerabilitats i reforçar la seguretat, així com d'advertència de potencials atacs futurs.	☐ Sí ☐ No

Altres característiques

Q15. S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament? La presència d'errors en el sistema de tractament incrementa la probabilitat de patir un atac. De la mateixa manera, les alertes o advertències respecte potencials fallades en la seguretat del sistema també poden indicar una probabilitat més alta de patir atacs.	☐ Sí ☐ No
Q16. Es tracten dades d'especial interès o dades d'un nombre molt gran de persones usuàries? La presència massiva de dades i la presència de dades d'especial interès són una motivació extra per als possibles atacants.	☐ Sí ☐ No

Calculem la probabilitat inicial de en funció del nombre de respostes afirmatives d'acord amb la taula següent:

Respostes Afirmatives	**Probabilitat Inicial**
0 - 4	Baixa
5 – 9	Mitjana
10 - 15	Alta

Nombre de respostes afirmatives	
Probabilitat inicial estimada	

3.3.3 Risc inicial

Un cop estimat l'impacte i la probabilitat inicial, aplicarem la taula de la Secció 3.1.7 per calcular el risc inicial (sense els controls de seguretat).

Impacte sobre la confidencialitat	
Impacte sobre la integritat	
Impacte sobre la disponibilitat	
Màxim dels impactes	
Probabilitat	
Risc inicial	

3.3.4 Controls de seguretat

Un cop calculat el risc inicial, cal determinar quins controls (mesures per millorar la seguretat) s'han d'aplicar.

Hi ha moltes llistes de controls. Aquí fem ús dels controls de l'Esquema Nacional de Seguretat(RD 311/2024).Els controls de l'ENS són força complexos. A la Guia sobre l'AIPD trobareu indicacions i criteris per determinar quins aplicar.

Baix	Mitjà	Alt	Control	Aplicat
Marc organitzatiu				
Sí	Sí	Sí	Política de seguretat [org.1] (sistema)	
Sí	Sí	Sí	Normativa de seguretat [org.2] (sistema)	
Sí	Sí	Sí	Procediments de seguretat [org.3] (sistema)	
Sí	Sí	Sí	Procés d'autorització [org.4] (sistema)	
Marc Operacional				
				Planificació
Sí	Sí	Sí	Arquitectura de seguretat [op.pl.2] (sistema)	
Sí	Sí	Sí	Adquisició de noves components [op.pl.3] (sistema)	
Sí	Sí	Sí	Dimensionament [op.pl.4] (D)	

Baix	Mitjà	Alt	Control	Aplicat
No	Sí	Sí	Components certificats [op.pl.5] (sistema)	
				Control d'accés
Sí	Sí	Sí	Identificació [op.acc.1] (sistema)	
Sí	Sí	Sí	Requeriments d'accés [op.acc.2] (ICAT)	
No	Sí	Sí	Segregació de funcions i tasques [op.acc.3] (ICAT)	
Sí	Sí	Sí	Procés de gestió de drets d'accés [op.acc.4] (ICAT)	
Sí	Sí	Sí	Mecanisme d'autenticació per a usuaris externs [op.acc.5] (ICAT)	
Sí	Sí	Sí	Mecanisme d'autenticació per a usuaris interns [op.acc.6] (ICAT)	
				Explotació
Sí	Sí	Sí	Inventari d'actius [op.exp.1] (sistema)	
Sí	Sí	Sí	Configuració de seguretat [op.exp.2] (sistema)	
Sí	Sí	Sí	Gestió de la configuració de la seguretat [op.exp.3] (sistema)	
Sí	Sí	Sí	Manteniment i actualitzacions de seguretat[op.exp.4] (sistema)	
No	Sí	Sí	Gestió de canvis [op.exp.5] (sistema)	
Sí	Sí	Sí	Protecció contra codi maliciós [op.exp.6] (sistema)	
Sí	Sí	Sí	Gestió d'incidències [op.exp.7] (sistema)	
Sí	Sí	Sí	Registre de l'activitat de les persones usuàries [op.exp.8] (sistema)	
Sí	Sí	Sí	Registre de la gestió d'incidències [op.exp.9] (sistema)	
Sí	Sí	Sí	Protecció de Claus criptogràfiques [op.exp.10] (sistema)	

Baix	Mitjà	Alt	Control	Aplicat
				Serveis externs
No	Sí	Sí	Contractació i acords de nivell de servei [op.ext.1] (sistema)	
No	Sí	Sí	Gestió diària [op.ext.2] (sistema)	
No	No	Sí	Protecció de la cadena de subministrament [op.ext.3] (Sistema)	
No	Sí	Sí	Interconnexió de sistemes [op.ext.4] (sistema)	
				Serveis en el núvol
Si	Sí	Sí	Protecció dels Serveis en el núvol [op.nub.1] (sistema)	
				Continuïtat del servei
No	Sí	Sí	Anàlisi d'impacte [op.cont.1] (D)	
No	No	Sí	Pla de continuïtat [op.cont.2] (D)	
No	No	Sí	Proves periòdiques [op.cont.3] (D)	
No	No	Si	Mitjans alternatius [op.cont.4] (D)	
				Monitorització del sistema
Sí	Sí	Sí	Detecció d'intrusions [op.mon.1] (sistema)	
Sí	Sí	Sí	Sistema de mètriques [op.mon.2] (sistema)	
Sí	Sí	Sí	Vigilància [op.mon.3] (sistema)	
Mesures de protecció				
				Protecció de les instal·lacions i les infraestructures
Sí	Sí	Sí	Àrees separades i control d'accés [mp.if.1] (sistema)	
Sí	Sí	Sí	Identificació de les persones [mp.if.2] (sistema)	

Baix	Mitjà	Alt	Control	Aplicat
Sí	Sí	Sí	Condicionament dels locals [mp.if.3] (sistema)	
Sí	Sí	Sí	Energia elèctrica [mp.if.4] (D)	
Sí	Sí	Sí	Protecció contra incendis [mp.if.5] (D)	
No	Sí	Sí	Protecció contra inundacions [mp.if.6] (D)	
Sí	Sí	Sí	Registre d'entrada i de sortida d'equipament [mp.if.7] (sistema)	
				Gestió del personal
No	Sí	Sí	Caracterització del lloc de treball [mp.per.1] (sistema)	
Sí	Sí	Sí	Deures i obligacions [mp.per.2] (sistema)	
Sí	Sí	Sí	Conscienciació [mp.per.3] (sistema)	
Sí	Sí	Sí	Formació [mp.per.4] (sistema)	
Protecció dels equips				
Sí	Sí	Sí	Lloc de treball buidat [mp.eq.1] (sistema)	
No	Sí	Sí	Bloqueig del lloc de treball [mp.eq.2] (sistema)	
Sí	Sí	Sí	Protecció de portàtils [mp.eq.3] (sistema)	
Sí	Sí	Sí	Altres dispositius connectats a la xarxa [mp.eq.4] (C)	
				Protecció de les comunicacions
Sí	Sí	Sí	Perímetre segur [mp.com.1] (sistema)	
Sí	Sí	Sí	Protecció de la confidencialitat [mp.com.2] (C)	
Sí	Sí	Sí	Protecció de l'autenticitat i de la integritat [mp.com.3] (IA)	
No	Sí	Sí	Segregació de fluxos d'informació [mp.com.4] (sistema)	

Baix	Mitjà	Alt	Control	Aplicat
				Protecció dels suports de la informació
Sí	Sí	Sí	Etiquetat [mp.si.1] (C)	
No	Sí	Sí	Criptografia [mp.si.2] (IC)	
Sí	Sí	Sí	Custodia [mp.si.3] (sistema)	
Sí	Sí	Sí	Transport [mp.si.4] (sistema)	
Sí	Sí	Sí	Esborrat i destrucció [mp.si.5] (C)	
				Protecció de les aplicacions informàtiques
No	Sí	Sí	Desenvolupament d'aplicacions [mp.sw.1] (sistema)	
Sí	Sí	Sí	Acceptació i posada en servei [mp.sw.1] (sistema)	
				Protecció de la informació
No	Sí	Sí	Qualificació de la informació [mp.info.2] (C)	
Sí	Sí	Sí	Signatura electrònica [mp.info.3] (IA)	
No	No	Sí	Segells temporals [mp.info.4] (T)	
Sí	Sí	Sí	Neteja de documents [mp.info.5] (C)	
Sí	Sí	Sí	Còpies de seguretat [mp.info.6] (D)	
				Protecció dels serveis
Sí	Sí	Sí	Protecció del correu electrònic [mp.s.1] (sistema)	
Sí	Sí	Sí	Protecció de serveis i aplicacions web [mp.s.2] (sistema)	
Sí	Sí	Sí	Protecció navegació web [mp.s.3] (sistema)	
No	Sí	Sí	Protecció contra la denegació de servei [mp.s.4] (D) (impacte, probabilitat)	

3.3.5 Impacte residual

Els controls de seguretat poden reduir l'impacte d'un incident de seguretat. Per exemple, el xifratge de certa informació pot limitar l'extensió d'una pèrdua de confidencialitat, una còpia de seguretat pot limitar l'impacte d'una pèrdua de la disponibilitat de la informació i l'ús de signatura electrònica pot permetre la detecció, i per tant la reducció de l'impacte, d'una pèrdua de la integritat.

Impacte que la pèrdua de la confidencialitat de les dades (és a dir, d'un accés no autoritzat a les dades) té sobre les persones

Impacte

Baix	Mitjà	Alt	Molt alt

Impacte residual

Baix	Mitjà	Alt	Molt alt

Justificació

Impacte que la pèrdua de la integritat de les dades (és a dir, de la modificació no autoritzada de les dades) té sobre les persones

Impacte

Baix	Mitjà	Alt	Molt alt

Impacte residual

Baix	Mitjà	Alt	Molt alt

Justificació

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones

Impacte

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones

Baix	Mitjà	Alt	Molt alt

Impacte residual

Baix	Mitjà	Alt	Molt alt

Justificació

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones

Impacte

Baix	Mitjà	Alt	Molt alt

Impacte residual

Baix	Mitjà	Alt	Molt alt

Justificació

L'impacte residual del sistema serà el màxim dels tres anteriors.

Impacte residual del sistema

Baix	Mitjà	Alt	Molt alt

3.3.6 Probabilitat residual

Per reduir la probabilitat cal eliminar la casuística que fa que les preguntes de la secció 3.2.2 tinguin resposta afirmativa.

Moltes vegades no és factible eliminar la casuística associada a les preguntes de la secció 3.2.2. En aquest cas, per canviar una resposta afirmativa a negativa, cal justificar que, en el context del sistema de tractament, els controls implementats fan que l'objecte de la pregunta tingui un pes negligible en l'aparició d'incidents de seguretat.

Cal revisar les respostes donades en el càlcul de la probabilitat inicial tenint en compte els controls implementats.

Respondre només en aquelles preguntes on s'ha canviat la resposta, en base als controls que s'hagin implementat. S'han posat exemples de mesures de seguretat per justificar aquest canvi, sens perjudici que hi hagi altres controls que també puguin reduir la probabilitat.

Maquinari i programari

Q1	Està el sistema de tractament connectat a sistemes externs a l'organització?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
Q2	Alguna part del tractament es fa a través d'internet?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
Q3	Manca document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura de caràcter organitzatiu i de formació dels treballadors.	
Q4	Manca document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb formació de treballadors i mesures relacionades amb la monitorització o registres.	
Q5	Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament?	
	Controls implementats i justificació per reduir probabilitat	

Maquinari i programari

	Qualsevol mesura relacionada amb monitorització o registres.

Procediments relacionats amb el tractament

Q6	Hi ha una manca de claredat en la definició dels rols i les responsabilitats dels treballadors?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura organitzativa i/o relacionada amb formació de treballadors.	
Q7	Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb formació de treballadors.	
Q8	Pot el personal connectar dispositius externs al sistema?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
Q9	Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	

Persones que intervenen en el tractament

Q10	El personal rep permisos que no són necessaris per complir les tasques que té encomanades?	
	Controls implementats i justificació per reduir probabilitat	

Persones que intervenen en el tractament

	Qualsevol mesura relacionada amb el control d'accessos i la formació als usuaris.	
Q11	S'ha externalitat alguna part del tractament a un encarregat?	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb control d'accessos, serveis externs, serveis al núvol, monitorització del sistema.	
Q12	Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD.	
	Controls implementats i justificació per reduir probabilitat	
	Qualsevol mesura relacionada amb formació de treballadors.	

Altres característiques

Q13	Ha patit l'empresa o altres empreses del sector atacs darrerament?	
	Controls implementats i justificació per reduir probabilitat	
	Per exemple, s'han realitzat millores, en relació amb l'autenticació dels usuaris tant interns com externs, s'ha millorat la gestió d'incidents, s'ha millorat la vigilància i monitoratge dels sistemes o la pròpia xarxa corporativa.	
Q14	S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament?	
	Controls implementats i justificació per reduir probabilitat	
	Per exemple, s'han millorat els procediments interns de seguretat, la gestió de configuració de la seguretat, o el sistema de mètriques.	
Q15	Es tracten dades d'especial interès o dades d'un nombre molt gran de persones usuàries?	
	Controls implementats i justificació per reduir probabilitat	
	Per exemple, s'ha millorat la gestió de configuració de la seguretat, o existència de sistemes redundants, o en general sistemes per a millorar la confidencialitat, la integritat o l'autenticitat.	

La probabilitat residual es calcula comptant el número de respostes afirmatives.

Respostes afirmatives	Probabilitat inicial
0 - 4	Baixa
5 – 9	Mitjana
10 - 14	Alta

3.3.7 Estimació del risc residual

Un cop estimat l'impacte residual i la probabilitat residual, calculem el risc residual seguint la taula de la Secció 3.1.7.

	Impacte			
Probabilitat	Baix	Mitjà	Alt	Molt alt
Baixa	Risc baix	Risc baix	Risc mitjà	Risc alt
Mitjana	Risc baix	Risc mitjà	Risc alt	Risc alt
Alta	Risc mitjà	Risc alt	Risc alt	Risc alt

Impacte residual sobre la confidencialitat Impacte residual sobre la integritat Impacte residual sobre la disponibilitat	
Màxim dels impactes residual Probabilitat residual	
Risc residual	

Si el risc residual és alt, cal proposar nous controls per reduir-lo. Si no és possible reduir-lo, abans d'iniciar el tractament cal fer una consulta prèvia l'autoritat de protecció de dades competent sobre la seva idoneïtat.

4. Avaluació d'Impacte en els Drets Fonamentals

En aquest apartat, s'examinen els impactes sobre els drets i llibertats fonamentals diferents del dret a la protecció de dades, que ja han estat objecte de l'AIPD.

4.1 Qüestionari de planificació i abast

Secció A[5] **Descripció complementària del sistema d'IA, inclosos els fluxos de dades relacionats**	Quins són els principals objectius del sistema d'IA? Quins tipus de dades es tracten (personals, no personals, categories especials)?
Secció B Context de drets fonamentals	Quins drets fonamentals es veuen potencialment afectats per l'ús del sistema d'IA? Quins instruments jurídics internacionals/regionals de protecció dels drets humans/fonamentals s'han aplicat a nivell operatiu? Quins són els tribunals o organismes més rellevants en matèria de drets fonamentals en el context d'ús? Quines són les decisions i disposicions més rellevants en matèria de drets humans/fonamentals?
Secció C Controls implementats	Quines polítiques i procediments s'han implementat per avaluar el possible impacte sobre els drets fonamentals, inclosa la participació de les parts interessades? S'ha efectuat, desenvolupat i aplicat una avaluació d'impacte en relació amb qüestions específiques (per exemple, protecció de dades) o algunes característiques del sistema (per exemple, l'ús de la biometria)?

[5] A la Secció A del model integrat, les qüestions relatives a les principals característiques del sistema, els països on s'oferia i la identificació de les persones afectades i dels responsables, han passat a la part general de l'avaluació (1.3 Descripció i anàlisi del sistema d'IA).

Secció D Intervenció de les parts interessades i diligència deguda	Quins són els principals grups o comunitats potencialment afectats pel sistema d'IA, inclòs el seu desenvolupament? Quines parts interessades, a més dels individus o grups que poden veure's afectats pels sistemes d'IA, hi han de participar (per exemple, la societat civil i les organitzacions internacionals, experts, associacions industrials, periodistes)? Hi ha altres titulars d'obligacions que hi hagin de participar, a part del proveïdor i el responsable del desplegament de la IA (per exemple, autoritats nacionals, organismes governamentals)? Han participat en el procés d'avaluació els socis comercials, inclosos els proveïdors de serveis (per exemple, subcontractistes en sistemes d'IA i conjunts de dades)? El proveïdor d'IA ha dut a terme una avaluació de la seva cadena de subministrament, per identificar si les activitats dels proveïdors/contractistes que participen en el desenvolupament de productes/serveis poden afectar els drets fonamentals? El proveïdor ha promogut estàndards o auditories de drets fonamentals, per garantir el respecte dels drets fonamentals entre els proveïdors? El proveïdor i el responsable del desplegament de la IA han comunicat públicament les possibles repercussions del sistema d'IA en els drets fonamentals? El proveïdor i el responsable del desplegament de la IA han proporcionat formació sobre estàndards de drets fonamentals al personal encarregat de la gestió i la contractació relacionades amb el sistema d'IA?

4.2 Matrius de risc

Taula 1. Probabilitat

Baixa	El risc de perjudici és improbable o altament improbable.
Mitjana	El risc de perjudici es pot produir.
Alta	Es preveu que es produeixi el risc de perjudici.
Molt alta	El risc que es produeixi el perjudici és gairebé una certesa. .

Taula 2. Exposició

Baixa	Pocs o molt pocs individus de la població identificada de titulars de drets estan potencialment afectats.
Mitjana	Una part substancial, però no la majoria, de la població identificada de titulars de drets està potencialment afectada.
Alta	La majoria de la població identificada de titulars de drets està potencialment afectada.
Molt alta	Gairebé tota la població identificada de titulars de drets està potencialment afectada.

Taula 3. Probabilitat que es produeixi un perjudici (*likelihood*)

		Probabilitat			
		Baixa	**Mitjana**	**Alta**	**Molt alta**
Exposició	**Baixa**	B	B/M	B/A	B/MA
	Mitjana	M/B	M	M/A	M/MA
	Alta	A/B	A/M	A	A/MA
	Molt alta	MA/B	MA/M	MA/A	MA

Probabilitat			
Baixa	Mitjana	Alta	Molt alta

Taula 4. Gravetat del perjudici

Baixa	Els individus i grups afectats poden trobar només perjudicis menors en l'exercici dels seus drets i llibertats.
Mitjana	Els individus i grups afectats poden trobar-se amb moderats perjudicis en l'exercici dels seus drets i llibertats.

Alta	Els individus i grups afectats poden enfrontar-se a seriosos perjudicis en l'exercici dels seus drets i llibertats.
Molt alta	Els individus i grups afectats poden trobar-se amb perjudicis molt greus o fins i tot irreversibles en l'exercici dels seus drets i llibertats.

Taula 5. Esforç per superar els perjudicis i revertir els efectes adversos

Baix	Els perjudicis soferts es poden superar sense problemes (per exemple, temps dedicat a modificar la informació, molèsties, irritacions, etc.).
Mitjà	Els perjudicis soferts es poden superar malgrat algunes dificultats (per exemple, costos addicionals, por, incomprensió, estrès, petites dolències físiques, etc.).
Alt	Els perjudicis soferts es poden superar encara que amb serioses dificultats (per exemple, pèrdues econòmiques, danys materials, empitjorament de la salut, etc.).
Molt alt	Els perjudicis soferts són extremadament, si no impossibles, de superar (per exemple, dolències psicològiques o físiques de llarga durada, mort, etc.).

Taula 6. Gravetat (*severity*)

		Gravetat			
		Baix	**Mitjana**	**Alta**	**Molt alta**
Esforç	**Baix**	B	B/M	B/A	B/MA
	Mitjà	M/B	M	M/A	M/MA
	Alt	A/B	A/M	A	A/MA
	Molt alt	MA/B	MA/M	MA/A	MA

Gravetat			
Baix	Mitjà	Alt	Molt alt

Taula 1A. Recollida de dades i anàlisi de riscos

Drets/ Llibertats potencialment afectats	Descripció de l'impacte	Probabilitat			Gravetat		
		Probabilitat de resultats adversos	Exposició	Probabilitat	Gravetat de l'impacte	Esforç	Gravetat

Taula 7. Impacte general del risc

		Gravetat			
		Baixa	Mitjana	Alta	Molt alta
Probabilitat	Baixa				
	Mitjana				
	Alta				
	Molt alta				

Risc global			
Baix	Mitjà	Alt	Molt alt

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)[6]

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

[6] En aquesta taula, s'hi haurà d'incorporar una referència al resultat final de l'AIPD pel que fa a la probabilitat i gravetat residual, que es pot fer mitjançant una crida a la pàgina concreta de l'AIPD on es descriuen les mesures adoptades.