DPIA-FRIA Model Template

Index

1. Description of the project in relation to data processing 4
1.1 Personal data processed 4
1.2 Processing operations 5
1.3 Description and analysis of the AI system 7
1.4 Actors involved in the processing 12
2. Need to carry out a DPIA and a FRIA 13
2.1 Need to carry out a DPIA 13
2.2 Need to carry out a FRIA 18
3. Data Protection Impact Assessment 20
3.1 Necessity and proportionality 20
3.1.1 Purpose of the processing 22
3.1.2 Principles of lawfulness 23
3.1.2.1 Legal basis for processing 23
3.1.2.2 Processing of children's data 24
3.1.2.3 Processing of special categories of data 25
3.1.2.4 Processing of crime data 26
3.1.2.5 Validity of consent 26
3.1.2.6 Data transfers 27
3.1.2.7 Lawfulness of processing to train AI 28
3.1.3. Principle of fairness in processing 28
3.1.4 Minimization principle 28
3.1.5 Principle of storage limitation 29
3.1.6 Principle of accuracy 30
3.1.7 Risks to people 30
3.1.8 Necessity and proportionality of the processing 32
3.1.9 Opinion of data subjects 33
3.2 Controls to safeguard people's rights 34
3.2.1 Controls to ensure the right to transparent information 34
3.2.2 Controls to ensure the right to information 35
3.2.3 Controls to guarantee the right of access 37

3.2.4 Controls to guarantee the right of rectification 38
3.2.5 Right to erasure 38
3.2.6 Right to restriction of processing 39
3.2.7 Right to data portability 40
3.2.8 Right to object 40
3.2.9 Right not to be subject to automated decisions 41
3.3. Data security risks 42
3.3.1 Impact 42
3.3.2 Initial probability 44
3.3.3 Initial risk 48
3.3.4 Security controls 49
3.3.5 Residual impact 53
3.3.6 Residual probability 55
3.3.7 Estimation of residual risk 59
4. Fundamental Rights Impact Assessment 60
4.1 Planning and scoping questionnaire 60
4.2 Risk matrices 61
Table 1. Probability 61
Table 2. Exposure 61
Table 3. Likelihood of harm occurring 62
Table 4. Severity of the harm 62
Table 5. Effort required to overcome harm and reverse adverse effects 63
Table 6. Severity 63
Table 1A. Data collection and risk analysis 63
Table 7. Overall risk impact 64
Table 2A. Risk management (I) 64
Table 3A. Risk management (II) 64

This impact assessment template is a model that seeks to identify and control the risks to the rights and freedoms of individuals, arising from the processing of personal data and the use of AI.

In some cases, an organisation may be required to carry out both a data protection impact assessment (Article 35 of the GDPR) and a fundamental rights impact assessment (Article 27 of the AI Act). In order to simplify this task, this template includes some preliminary sections that are useful for both assessments: a general description of the processing operations, to determine its main elements; and the activities to be developed (collectively identified as the "Project"), including the use of data and AI that is envisaged. The level of detail must be sufficient to assess the specific scenarios and risk indicators.

It should be noted that the use of AI may have an impact on one or more data processing operations of a processing activity. In order to correctly assess the risks, it is important to detect the flows and interconnections that exist throughout the life cycle of the processing of personal data and, if applicable, in the life cycle of the AI system.

GENERAL DESCRIPTION OF THE PROJECT

General description of the project

Is personal data used?	☐ Yes ☐ No
Is the data collected used for a purpose other than the processing being assessed?	☐ Yes ☐ No
Does the processing incorporate AI?	☐ Yes ☐ No

Does the project use prohibited AI practices set out in Article 5 of the AI Act?	☐ Yes ☐ No
If AI is used, could its use potentially affect the fundamental rights of the individuals concerned or third parties?	☐ Yes ☐ No
Is it possible to obtain the same results using less intrusive methods (e.g. synthetic data)?	☐ Yes ☐ No

What phase of the life cycle is the AI system in?	☐ Research ☐ Proof of concept ☐ Design ☐ Development ☐ Training ☐ Validation ☐ Deployment

1. Description of the project in relation to data processing

A detailed description of how personal and non-personal data is processed must be provided, as this will form the basis for assessing the necessity, proportionality and risks of the processing.

Detailed description of the processing and context

Purpose of the processing

1.1 Personal data processed

The characteristics of the data to be processed are relevant when determining the risks of the processing and compliance with some provisions of the Regulation.

Data type	
Source / Origin	
Retention period	
Is there any data requiring special protection? (financial, gender-based violence, subsidies...)	☐ Yes ☐ No

Data type	
Will the data be used for any purpose other than that for which it was collected?	☐ Yes ☐ No
Does the processing involve offering information society services to children and is it based on consent?	☐ Yes ☐ No
Is special category data or data relating to vulnerable groups processed?	☐ Yes ☐ No
Is data relating to criminal convictions or offences processed?	☐ Yes ☐ No
If AI is used, does the model's training dataset contain personal data, or has data that can be considered anonymous been used?	☐ Personal data ☐ Anonymous
If personal data is used, has the AI provider carried out a DPIA?	☐ Yes ☐ No
[AI Provider] If a model is being used that was trained on a dataset which can be considered anonymous, has the risk of re-identification been assessed?	☐ Yes ☐ No
[Deployer] If AI is used, does the dataset used to contextualise the operation of the system (e.g. fine-tuning) contain personal data (including data obtained through web scraping)?	☐ Yes ☐ No

1.2 Processing operations

The aim of this section is to identify the different components of the process when AI is used at different stages or for different functions within the same overall purpose.

Process	
Description	
Does the process incorporate artificial intelligence (system or component)?	☐ Yes ☐ No (See the section Description and analysis of the AI system)
Data processed	
Result of the process	

Process	
Recipient	
Place of processing	

Process	
Description	
Does the process incorporate artificial intelligence (system or component)?	☐ Yes ☐ No (See the section Description and analysis of the AI system)
Data processed	
Result of the process	
Recipient	
Place of processing	

Process	
Description	
Does the process incorporate artificial intelligence (system or component)?	☐ Yes ☐ No (See the section Description and analysis of the AI system)
Data processed	
Result of the process	
Recipient	
Place of processing	

1.3 Description and analysis of the AI system

What type of AI system is it?	☐ General-purpose AI (GPAI) model (model that can be used for many different tasks) ☐ GPAI with systemic risk (very powerful AI models with potentially far-reaching impacts and additional regulatory obligations) ☐ Generative AI system (AI capable of generating new content, such as text, images, audio, video, code, etc.) ☐ GPAI-based system (application built from a general purpose AI model) ☐ Agentic AI system (AI capable of acting relatively autonomously to achieve specific goals) ☐ Specific AI system. ☐ Others. Please specify: _____

Functional classification	☐ Discriminative or classifier AI (classifies, categorizes or identifies patterns) ☐ Predictive AI (estimates probabilities, risks or future events) ☐ Generative AI (generates text, images, audio, video, code or other content) ☐ Agentic AI (plans, decides or performs actions with varying degrees of autonomy) ☐ Recommendation or decision support system (proposes options, recommendations or decisions) ☐ Anomaly or fraud detection system ☐ Conversational system (chatbot, virtual assistant or copilot) ☐ Artificial vision system (processes images or video) ☐ Multimodal system (combines text, image, audio, video or other modalities) ☐ Robotic or physical system (robots, smart devices or autonomous vehicles) ☐ Others. Please specify: _____
Degree of autonomy	☐ Human-in-the-loop assistance ☐ Recommendation with mandatory human validation ☐ Semi-autonomous execution ☐ Supervised autonomous execution ☐ Autonomous execution without human intervention ☐ Others. Please specify: _____

System architecture	☐ Own model developed or trained by the organization ☐ Third-party commercial model ☐ Open source model ☐ Fine-tuning system ☐ Retrieval-augmented generation (RAG) system ☐ Hybrid system (combination of various models or technologies) ☐ Others. Please specify: _____
Privacy-enhancing technologies (PETs)	☐ No PETs are used ☐ Anonymization ☐ Pseudonymisation ☐ Differential privacy ☐ Federated learning ☐ Homomorphic encryption ☐ Secure Multi-Party Computing (SMPC) ☐ Trusted Execution Environments (TEE) ☐ Confidential computing ☐ Synthetic data ☐ Zero-knowledge proofs (ZKP) ☐ Machine unlearning ☐ Others. Please specify: _____

Types of data processed	☐ Text ☐ Images ☐ Audio ☐ Video ☐ Documents ☐ Structured data (databases, files, spreadsheets) ☐ Biometric data ☐ Geolocation data ☐ Others. Please specify: _____
Origin of the personal data processed by the AI system	☐ Internal organisational data ☐ Data provided by users ☐ Data from other administrations or entities ☐ Open data ☐ Web scraping ☐ Data acquired from third parties ☐ Synthetic data ☐ Others. Please specify: _____

What are the purposes (specific objectives) of the AI system?	☐ Support for human decision-making ☐ Content generation or recommendations ☐ Classification or profiling of individuals ☐ Decision automation ☐ Automation of operational processes ☐ Others. Please specify: _____
[AI Provider] Do AI tools used for data processing (e.g. deep convolutional neural networks, support vector machines, etc.) use the least amount of personal data possible for the intended purpose?	☐ Yes ☐ No
[AI Provider] Has the need to use machine learning, in particular deep learning, been documented, if applicable?	☐ Yes ☐ No

[AI Provider] Can AI design options be considered to ensure data protection by design (federated learning, secure multi-party computing, homomorphic encryption, etc.)?	☐ Yes ☐ No If so, which ones?
What are the main characteristics of the system?	
List the processing operations with which the AI performs (link to point 1.2 Processing operations)	
In which countries will the AI system be made available?	
Identification of potential rights holders: who are the individuals or groups that may be affected by AI systems? Are vulnerable individuals or groups included?	

1.4 Actors involved in the processing

The actors involved in processing operations, their roles and the data they process are important factors in determining the risks of the processing.

		Role for the purposes of the AI Act	Role for the purposes of the GDPR
Name		☐ Provider ☐ Deployer	☐ Controller ☐ Processor
Processing operations in which it is involved			
Description			

Name		☐ Provider ☐ Deployer	☐ Controller ☐ Processor
Processing operations in which it is involved			
Description			

Name		☐ Provider ☐ Deployer	☐ Controller ☐ Processor
Processing operations in which it is involved			
Description			

Name		☐ Provider ☐ Deployer	☐ Controller ☐ Processor
Processing operations in which it is involved			
Description			

Name		☐ Provider ☐ Deployer	☐ Controller ☐ Processor
Processing operations in which it is involved			
Description			

2. Need to carry out a DPIA and a FRIA

A DPIA (Article 35 of the GDPR) is not required if any of the following situations apply:

Situation	
The processing is similar in nature, scope, context and purpose to another processing for which a DPIA has already been made.	
The processing has a legal basis in EU or Member State law, and a DPIA has already been carried out when this legal basis was adopted.	

Justification

If none of the above situations apply and the processing may pose a serious risk to the rights and freedoms of individuals, a DPIA must be carried out. The Article 29 Working Group (WG29) provided a list of characteristics that may be indicative of high risk.

2.1 Need to carry out a DPIA

DPIA technical sheet[1]

Current version and version log (explaining the history of changes made to the information contained in the DPIA template for this processing, if any)	
The team involved in this DPIA (providing details of	

[1] This technical sheet is based on Version 1.0 of the EDPB's Template for Data Protection Impact Assessment (DPIA), adopted on 10 March 2026.

their roles, tasks, responsibilities, etc.)			
Guidelines, standards, codes of conduct and other reference materials used to carry out this DPIA.			
Reasons for conducting the DPIA (more than one checkbox may be checked)	1. New processing activity: a DPIA will probably be required due to the high risk involved (obligation under Article 35(3) of the GDPR):	Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.	☐ Yes ☐ No
		Processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10.	☐ Yes ☐ No
		Systematic monitoring of a publicly accessible area on a large scale.	☐ Yes ☐ No
	2. New processing activity, DPIA likely to be required due to likely high-risk (legal obligation under national law)	Explanation:	
	3. New processing activity, DPIA likely to be required due to likely high-risk (following EDPB and national guidance):	Evaluation or scoring, including profiling and predicting, especially from “aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or	☐ Yes ☐ No

		behaviour, location or movements".	
		Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person".	☐ Yes ☐ No
		Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area".	☐ Yes ☐ No
		Sensitive data or data of a highly personal nature: this includes special categories of personal data, as defined in Article 9 (for example, information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10 of the GDPR.	☐ Yes ☐ No
		Data processed on a large scale, considering the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration or permanence of the data processing activity; and the geographical extent of the processing activity.	☐ Yes ☐ No
		Matching or combining datasets.	☐ Yes ☐ No

DPIA technical sheet[1]

		Data concerning vulnerable data subjects (because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily give consent to, or oppose, the processing of their data, or exercise their rights).	☐ Yes ☐ No
		Innovative use or applying of new technological or organisational solutions.	☐ Yes ☐ No
		When the processing in itself "prevents data subjects from exercising a right or using a service or contract".	☐ Yes ☐ No
		Other (e.g. national list regarding the processing operations subject to the requirements of a data protection impact assessment) _____	
	4- New processing activity, DPIA necessary or beneficial	DPO opinion or recommendation	☐ Yes ☐ No
		Data subject's (or their representatives') opinion or recommendation.	☐ Yes ☐ No
		Required by a code of conduct, standard, best practices, etc.	☐ Yes ☐ No

DPIA technical sheet[1]

		Others (for example, managing risks or demonstrating accountability and building trust): _____	
	5. Existing high-risk processing activities for which there has been a change in risks:	Data processing has changed.	☐ Yes ☐ No
		The organisational or societal context of the processing activity has changed.	☐ Yes ☐ No
		How?	
Scope of this DPIA (what has been considered and what has been left out of the assessment and why).			
Completion date			
Formal validation date (approval of the DPIA as complete and finished by a responsible official)			
Is the DPIA (or parts of it) intended to be published or shared externally?	☐ No	☐ Yes, it is going to be published. How?	☐ Yes, it is going to be shared externally. How?

Is it necessary to carry out a DPIA? ☐ Yes ☐ No

Justification:

If a DPO has been appointed, their opinion on the need for a DPIA must be considered.

Opinion of the DPO regarding the need to carry out a DPIA

2.2 Need to carry out a FRIA

The following are the criteria for determining whether a FRIA is required under Article 27 of the AI Act. If there are positive answers (yes) to the questions relating to both the objective and subjective scope, a FRIA will need to be carried out.

However, the assessment of the impact on fundamental rights also forms part of the risk management system referred to in Article 9, which AI providers must adopt. The FRIA model can therefore be used for this purpose, too.

Objective scope	Is the system classified as high-risk under Article 6(2) of the AI Act? (Article 27(1))	☐ Yes ☐ No
	Is the AI system not intended to be used as a safety component in the management and operation of critical digital infrastructure, road traffic or the supply of water, gas, heating or electricity?	☐ Yes ☐ No
	Is the system included in any of the areas listed in points 1 and 3 to 8 of Annex III of the AI Act?	☐ Yes ☐ No
		Which one?
Subjective scope	Is the deployer of the high-risk AI system is a public law body?	☐ Yes ☐ No
	Is the deployer of the high-risk AI system a private entity that provides public services?	☐ Yes ☐ No

	Is the deployer one of those listed in Annex III, point 5, letters *b* and *c*, of the AI Act?	☐ Yes ☐ No	
		Which one?	
General questions	Is this the first use of the AI system?	☐ Yes ☐ No	
	Is there a previous FRIA for the same system or a similar one?	☐ Yes ☐ No	
	Has the AI provider provided a reusable FRIA?	☐ Yes ☐ No	
	If so, which element has changed or is no longer up to date, making it necessary to carry out the FRIA again?	the purpose	☐ Yes ☐ No
		the context of use	☐ Yes ☐ No
		the processes	☐ Yes ☐ No
		the categories of affected people / groups	☐ Yes ☐ No
		the frequency or intensity of use	☐ Yes ☐ No
		potential risks	☐ Yes ☐ No
		human supervision	☐ Yes ☐ No

If (i) a FRIA has already been carried out or (ii) a FRIA provided by the AI provider already covers all relevant risks, a new FRIA is not required. This is provided that all risks have been analysed in relation to the context of use and there have been no changes.

In relation to the DPIA (Article 27(3) of the AI Act)	Is there a DPIA relating to the AI system in accordance with Article 35 of the GDPR?	☐ Yes ☐ No

	What parts need to be supplemented with a FRIA?	

3. Data Protection Impact Assessment

3.1 Necessity and proportionality

The assessment of the necessity and proportionality of the processing is made in relation to the purpose of the processing, which has been described in the previous section.

Necessity and proportionality from the perspective of the AI system	Social or public policy need	Does the system provide any direct benefit to “humanity”? (recital 27)	☐ Yes ☐ No
		Does it contribute to public objectives (equity, transparency, accessibility, efficiency)?	☐ Yes ☐ No
		Does it address structural problems (overburdened services, staff shortages, etc.)?	☐ Yes ☐ No
		Is the system socially acceptable and understandable for the affected users?	☐ Yes ☐ No
	Evaluation inspired by public policies	What specific problem or need is this AI system intended to solve?	
		Why is this problem relevant or critical to the organisation?	
		What non-algorithmic or traditional solutions are currently available?	
		Explain why “doing nothing” (or maintaining the current situation) is not an option and what specific benefits AI provides (efficiency, accuracy, scalability).	
	Need to use the specific type of AI selected	Are there equally effective alternatives with a lower impact on rights?	☐ Yes ☐ No
		If so, why wouldn't a low-risk AI or a simpler system suffice, or why has the “simpler” technological alternative been discarded?	Justification

		Is the level of automation really necessary to achieve the purpose?	☐ Yes ☐ No

3.1.1 Purpose of the processing

In principle, the data collected is used to fulfil the purpose of the processing for which it was collected. However, in some cases, the Regulation allows the processing of data that has been collected for a different purpose.

Is the data collected used for a purpose other than that of the original processing?	☐ Yes ☐ No

If so,

the following conditions allow data to be processed for a purpose other than that for which it was collected.	
Consent has been obtained from the data subjects for processing for the new purpose.	☐ Yes ☐ No
The processing is based on Union or Member State law that constitutes a measure to safeguard:	
National security.	☐ Yes ☐ No
The defence.	☐ Yes ☐ No
Public safety.	☐ Yes ☐ No
The prevention, investigation, detection and prosecution of criminal offences.	☐ Yes ☐ No
Other important objectives of public interest.	☐ Yes ☐ No
The protection of judicial independence and judicial proceedings.	☐ Yes ☐ No

If so,

The prevention, investigation, detection and prosecution of breaches of professional ethics rules.	☐ Yes ☐ No
The protection of the data subject or the rights and freedoms of others.	☐ Yes ☐ No
The enforcement of civil law claims.	☐ Yes ☐ No

If none of the above conditions apply, the new purpose must be compatible with the purpose that motivated the collection of the data.

Initial purpose.	
Data.	
New purpose.	
Justification of compatibility.	

Initial purpose.	
Data.	
New purpose.	
Justification of compatibility.	

3.1.2 Principles of lawfulness

3.1.2.1 Legal basis for processing

Processing is lawful if one of the following legal bases applies:

The data subject has given consent to the processing of their personal data for one or more specific purposes.	☐ Yes ☐ No
The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps prior to entering into a contract.	☐ Yes ☐ No

The data subject has given consent to the processing of their personal data for one or more specific purposes.	☐ Yes ☐ No
The processing is necessary to comply with a legal obligation applicable to the controller.	☐ Yes ☐ No
The processing is necessary to protect the vital interests of the data subject or of another natural person.	☐ Yes ☐ No
The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	☐ Yes ☐ No
The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child.	☐ Yes ☐ No

Justification of the lawfulness of the processing.

In addition, the processing must not involve any unlawful activity in a broader sense. For example, violating copyright or contractual agreements.

Confirm that the processing does not involve any unlawful activity.

3.1.2.2 Processing of children's data

Children need special protection in the processing of their data, because they may not be aware of the risks involved .

Does the processing offer information society services to children and is it based on consent?	☐ Yes ☐ No
If so, has the minimum age of consent been taken into account?	☐ Yes ☐ No
Is the child's data used for profiling and/or to make fully or partially automated decisions about them?	☐ Yes ☐ No

Does the processing offer information society services to children and is it based on consent?	☐ Yes ☐ No

3.1.2.3 Processing of special categories of data

Are special categories of data processed?	☐ Yes ☐ No

If so,

The processing of special categories of data is prohibited, unless one of the following cases applies.	
The data subject has given their explicit consent to the processing for a specific purpose, unless EU or Member State law does not permit it.	☐ Yes ☐ No
The processing is necessary to comply with obligations or exercise rights in the field of employment law and social security and social protection.	☐ Yes ☐ No
The processing is necessary to protect the vital interests of the data subject or another natural person, in the event that the data subject is not capable of giving consent.	☐ Yes ☐ No
The processing is carried out with appropriate safeguards by a non-profit association with a political, philosophical, religious or trade union aim, provided that it concerns people with whom the association maintains contact in connection with these purposes and the data is not disclosed to third parties without the consent of the data subjects.	☐ Yes ☐ No
The processing relates to personal data which the data subject has manifestly made public.	☐ Yes ☐ No
The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.	☐ Yes ☐ No
The processing is necessary for reasons of essential public interest.	☐ Yes ☐ No
The processing is necessary for the purposes of preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.	☐ Yes ☐ No
The processing is necessary for reasons of public interest in the field of public health.	☐ Yes ☐ No

If so,

The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.	☐ Yes ☐ No
[AI Provider] Is the processing necessary to detect and correct biases associated with high-risk AI systems, in accordance with Article 10(5) of the AI Act?	☐ Yes ☐ No
[Deployer/AI Provider] If so, have measures been put in place to prevent the retrieval of personal data used by the AI system?	☐ Yes ☐ No

Justification of the lawfulness of the processing of special categories of data

3.1.2.4 Processing of crime data

Is data relating to criminal convictions or offences processed?	☐ Yes ☐ No

If so,

Although data relating to criminal convictions or offences are not special categories of data, there is an additional requirement for processing it: processing can only be carried out under the supervision of public authorities or when authorised by Union or Member State law.

Justification of the lawfulness of processing crime data

3.1.2.5 Validity of consent

If processing is based on consent, the following conditions must be met for that consent to be valid:

The controller can demonstrate that consent was obtained.	☐ Yes ☐ No
The consent request is intelligible, easily accessible and in clear language.	☐ Yes ☐ No
The performance of a contract cannot be made conditional on obtaining consent to the processing of personal data that is not necessary for the performance of the contract.	☐ Yes ☐ No
Data subjects have been informed of the possibility of withdrawing consent at any time.	☐ Yes ☐ No
If the data subject does not wish to give consent, they are offered an alternative that does not disadvantage them or result in unfavourable treatment.	☐ Yes ☐ No

3.1.2.6 Data transfers

To prevent data subjects' rights from being diminished, the GDPR imposes particularly strict restrictions on data transfers to countries where it does not apply.

Are data transfers made to third countries or international organisations?	☐ Yes ☐ No

If so,

These transfers are permitted if the European Commission considers that the country or organisation offers an adequate level of protection, if appropriate safeguards have been established in accordance with Article 46 or if one of the derogations under Article 49 applies.

Data transferred.	
Country.	
Condition permitting the transfer.	

Data transferred.	
Country.	
Condition permitting the transfer.	

3.1.2.7 Lawfulness of processing to train AI

[AI Provider] If you are reusing publicly available data or data obtained from a third party (e.g. a data provider) to train the AI, have you checked that the dataset was not clearly created unlawfully?	☐ Yes ☐ No
Is the source of the data clearly identified and documented?	☐ Yes ☐ No
Is the dataset the result of a criminal offence or infringement (data leak, theft, etc.), or has it been subject to a public conviction or sanction by a competent authority, resulting in its withdrawal or a prohibition on its use?	☐ Yes ☐ No
Are the conditions under which the data was collected sufficiently documented?	☐ Yes ☐ No
Does the dataset contain sensitive information or information that infringes rights? If so, are thorough checks carried out to ensure that the processing is lawful?	☐ Yes ☐ No

3.1.3. Principle of fairness in processing

Processing is fair if the use made of the data is foreseeable by the data subjects and the processing does not result in unjustifiable adverse consequences for them.

Justification of fair processing

3.1.4 Minimization principle

The data must be adequate, relevant and limited to what is strictly necessary to achieve the purpose of the processing.

Data type.	

Justification of adequacy, relevance and necessity

Data type.	

Justification of adequacy, relevance and necessity

Data type.	

3.1.5 Principle of storage limitation

Personal data must not be kept longer than is strictly necessary to fulfil the purpose of the processing. In the description of the processing, the data retention period was specified. It is necessary to demonstrate that the specified retention periods comply with the principle of storage limitation.

Justification of compliance of the specified retention periods with the principle of storage limitation

The mechanisms established for erasing data must be effective (is erasure automatic or must it be initiated manually? Does the data remain in system backups after erasure? For how long? How is it ensured that the data is not processed?).

Describe the mechanisms established to erase data

Data may be retained indefinitely for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

Data is retained for archiving in the public interest, scientific or historical research, or statistical purposes.	

If so, what measures have been implemented to ensure compliance with the principle of data minimisation?

3.1.6 Principle of accuracy

Processing inaccurate data can negatively affect people. The principle of accuracy requires data to be accurate and appropriate measures to be taken to ensure that inaccurate data is corrected or erased without delay.

Data quality controls[2]

Measures to correct data

3.1.7 Risks to people

The objective of this point is to identify the possible negative effects on people, quantify them and, if necessary, propose measures to mitigate them.

In this section, we will assess the processing as designed. That is, we do not consider cases in which the security of the system fails (whether this failure is accidental or intentional).

When identifying the potential negative effects of processing on individuals, it is advisable to take into account the views of the data subjects and the data protection officer.

Potential negative effects of processing on people

For each of the negative effects identified, it is necessary to estimate the associated risk level. Risk depends on two factors: the impact on people (low, medium, high or very high) and the likelihood of it materialising (low, medium or high). The impact is estimated directly from the potential effects. To determine the likelihood, it is necessary to analyse the circumstances in which the negative effects may materialise (the threats) and estimate their likelihood.

[2] Includes the training phase of AI models

The level of risk is determined on the basis of impact and likelihood, using the following table:

	Impact			
Probability	Low	Medium	High	Very high
Low	Low risk	Low risk	Medium risk	High risk
Medium	Low risk	Medium risk	High risk	High risk
High	Medium risk	High risk	High risk	High risk

First, the risk associated with each threat will be estimated. The overall risk will be the highest risk associated with any of the threats.

Effect on people

Impact:

Threat	Probability	Risk

Estimated risk

Effect on people

Impact:

Threat	Probability	Risk

Estimated risk:

Effect on people

If the risk is not low, measures must be identified to reduce it. This is particularly necessary in cases of high or very high risk. If it is not possible to reduce a high risk, the competent data protection authority must be consulted on the suitability of the processing before it begins.

If the original processing has been modified to make it less harmful to people, the previous sections of the DPIA must be reviewed and updated.

Rights/freedoms affected	Probability	Severity	Overall impact	Measures to prevent/mitigate impacts

3.1.8 Necessity and proportionality of the processing

Based on the information collected in this section, it is necessary to demonstrate that the processing is necessary (the intended purpose cannot be achieved through any other less intrusive measure) and proportionate (it does not cause more harm than good).

Justification of the suitability of the processing for the intended purpose

Justification of the necessity of the processing

Justification that the processing is proportionate

3.1.9 Opinion of data subjects

The GDPR establishes that, where possible, the views of data subjects on the processing must be sought.

Opinion of data subjects on the necessity and proportionality of the processing

If it is not considered appropriate to seek the views of data subjects, this must be justified.

Why have the views of data subjects not been sought?

If the views of data subjects on the processing differ from those expressed by the controller in section 2.7, and the processing is to proceed, the reasons for this must be justified.

Why is the processing being carried out despite the objections of the data subjects?

3.2 Controls to safeguard people's rights

3.2.1 Controls to ensure the right to transparent information

Transparency is a cross-cutting principle and must be reflected in all communications with data subjects.

All communication with data subjects must be concise, intelligible, easily accessible and must use clear and simple language.	☐ Yes ☐ No

The Regulation specifies how this communication must be carried out.

The information will be provided in writing, including by electronic means.	☐ Yes ☐ No
In the case of requests made by electronic means, the information will preferably be provided electronically.	☐ Yes ☐ No
If the data subject requests it, the information will be provided orally.	☐ Yes ☐ No

The controller must respond to requests from data subjects to exercise their rights within the prescribed time limits:

Without undue delay and within one month.	☐ Yes ☐ No
If the complexity or number of requests justifies it, the period may be extended by two months. In this case, the reasons for the extension must be communicated within the first month.	☐ Yes ☐ No

If the controller does not intend to act on a data subject's request to exercise their rights, it must:ts from a data subject, it is necessary:

Inform the data subject accordingly without undue delay and within one month at the latest.	☐ Yes ☐ No
Explain the reasons for not acting on the request (for example, because it is repetitive or the controller cannot identify the data subject).	☐ Yes ☐ No
Inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.	☐ Yes ☐ No

A fee may only be charged to cover the costs of handling the request if it is excessive (for example, because it is repetitive).	☐ Yes ☐ No

3.2.2 Controls to ensure the right to information

When collecting personal data, the data controller must inform data subjects of different aspects of the processing.

[Deployer] Has the AI system provider supplied the information needed to fulfil the obligation to inform data subjects appropriately?[3]	☐ Yes ☐ No

Articles 13 and 14 specify that data subjects must be informed of the points detailed in the following table:

The identity and contact details of the controller.	☐ Yes ☐ No
The contact details of the data protection officer (if any).	☐ Yes ☐ No
The purpose of the processing.	☐ Yes ☐ No
The legal basis for the processing.	☐ Yes ☐ No
The legitimate interests pursued by the controller, if these constitute the legal basis for the processing.	☐ Yes ☐ No
The recipients or categories of recipients of the data.	☐ Yes ☐ No
The data retention period or the criterion used to determine it.	☐ Yes ☐ No
The intention to transfer the data outside the EU, where applicable.	☐ Yes ☐ No
The European Commission's decision on the adequacy of the level of protection provided by the recipient country or organisation.	☐ Yes ☐ No
The existence of the right of access to data.	☐ Yes ☐ No
The existence of the right to rectification and erasure.	☐ Yes ☐ No
The existence of the right to limit processing.	☐ Yes ☐ No
The existence of the right to object to processing.	☐ Yes ☐ No
The existence of the right to data portability.	☐ Yes ☐ No

[3] This point is particularly important for ensuring compliance with the obligations established in Article 86 of the AI Act.

The identity and contact details of the controller.	☐ Yes ☐ No
The existence of the right to withdraw consent (if this is the legal basis for the processing).	☐ Yes ☐ No
The existence of the right to file a complaint with a supervisory authority.	☐ Yes ☐ No
That the communication of the data is a legal or contractual requirement, if applicable.	☐ Yes ☐ No
The existence of automated decision-making.	☐ Yes ☐ No
The purpose of using data for a purpose other than that for which it was collected, if applicable.	☐ Yes ☐ No
The origin of the data, if it has not been obtained directly from the data subject.	☐ Yes ☐ No

There are certain exceptions to the obligation to provide information, depending on how the data was collected.

- Where the data has been obtained directly from the data subject, there is no obligation to provide the information if the data subject already has it.
- If the data has not been obtained directly from the data subject, there is no obligation to inform them if any of the following conditions apply: the data subject already has the information; providing the information is impossible or would involve a disproportionate effort; the provision of information is governed by EU or Member State law; or the information is confidential due to an obligation of professional secrecy.

If the information is not provided, this must be justified.

Does the right to information apply to all processed data?	

If any exemption from the right to information applies, it is necessary to specify which exemption applies, which data it concerns and the reasons for applying it

If data subjects are informed, the Regulation determines when this must be done.[4] .

[4] GDPR art. 13(1) and 14(3),

If the data is collected directly from the data subjects, at the time of collection.	☐ Yes ☐ No
If data is collected indirectly, the following conditions must be met:	
Within a reasonable period, but no later than one month.	☐ Yes ☐ No
Where communication with the data subject is envisaged, at the latest at the time of the first communication.	☐ Yes ☐ No
If the data are to be disclosed to third parties, before the disclosure takes place.	☐ Yes ☐ No

3.2.3 Controls to guarantee the right of access

The data subject has the right to obtain confirmation from the controller as to whether their personal data are being processed and, where this is the case, access to the personal data and the following information :

The purpose of the processing.	☐ Yes ☐ No
The categories of data processed.	☐ Yes ☐ No
The recipients of the data.	☐ Yes ☐ No
The data retention period.	☐ Yes ☐ No
The rights to rectify and erase data.	☐ Yes ☐ No
The rights to restrict and to object to processing.	☐ Yes ☐ No
The right to lodge a complaint to a supervisory authority.	☐ Yes ☐ No
If the data has not been obtained from the data subject, the origin of the data.	☐ Yes ☐ No
The existence of automated decision-making, where applicable.	☐ Yes ☐ No
Safeguards for transfers of data outside the EU, where applicable.	☐ Yes ☐ No

In addition to knowing what information must be provided to data subjects, it is necessary to ensure that the conditions for exercising the right of access are met.

Has a standard procedure been established for managing access requests?	☐ Yes ☐ No
Do the staff dealing with data subjects have the necessary training to recognize access requests?	☐ Yes ☐ No

3.2.4 Controls to guarantee the right of rectification

People have the right to have their data rectified if it is inaccurate.

Has a procedure been established for managing requests for rectification?	☐ Yes ☐ No
Do the staff dealing with data subjects have the necessary training to recognize requests for rectification?	☐ Yes ☐ No

If the controller has shared the data, they must inform the recipients about the rectification.

Has a procedure been established to notify the recipients of the rectification?	☐ Yes ☐ No

3.2.5 Right to erasure

People have the right to have their personal data erased in any of the following circumstances:

- The data is no longer necessary in relation to the purpose for which it was collected.
- The data subject withdraws their consent and there is no other legal basis for the processing.
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- The data has been processed without a legal basis.
- The data must be erased to comply with a legal obligation to which the controller is subject.
- The data is used to offer information society services to children.

However, the right to erasure does not apply in the following cases:

- To exercise the right to freedom of expression and information.
- To comply with a legal obligation or to perform a task carried out in the public interest.
- For archiving purposes in the public interest, for scientific or historical research purposes, and for statistical purposes (if the fulfilment of these purposes would be affected by the erasure of the data).
- To file, exercise or defend legal claims.

Are staff qualified to determine whether the right to erasure applies?	☐ Yes ☐ No

It is advisable to establish a standard channel so that data subjects can request to exercise the right to erasure. However, it is necessary to ensure that staff are trained to detect requests made by other means.

Has a procedure been established for managing erasure requests?	☐ Yes ☐ No
Do staff dealing with data subjects have the necessary training to recognize erasure requests?	☐ Yes ☐ No

If the controller shares the data, it must take appropriate measures (taking into account costs and available technology) to notify the recipients of the request for erasure.

Has a procedure been established to notify the recipients of the erasure request?	☐ Yes ☐ No

3.2.6 Right to restriction of processing

Article 18 gives data subjects the right to obtain restriction of the processing of their personal data in the following cases:

- The data subject has requested the rectification of their data and the controller is verifying whether they are accurate.
- The data has been processed without a legal basis.
- The data subject needs the controller to store the data to initiate, exercise or defend a claim.
- The data subject has objected to the processing and the controller is assessing whether the controller's legitimate grounds override those of the data subject.

Are staff trained to determine whether the right to restriction of processing applies?	☐ Yes ☐ No

It is necessary to ensure that staff are trained to recognise requests for restriction of processing.

Has a procedure been established for managing requests for restriction of processing?	☐ Yes ☐ No
Do staff dealing with data subjects have the necessary training to recognise requests for restriction of processing?	☐ Yes ☐ No

When restricting processing, it is necessary to take into account the different forms it can take: data collection, data analysis, dissemination of results, etc.

Are all possible forms of processing taken into account when limiting it?	☐ Yes ☐ No

If data has been shared, the recipients must be informed of requests for restriction of processing.

Has a procedure been established for notifying recipients of requests for restriction of processing?	☐ Yes ☐ No

3.2.7 Right to data portability

Individuals have the right to request the data they have provided to the controller in the following cases:

- If the processing is based on consent or is necessary for the performance of a contract or to take steps prior to entering into a contract.
- The processing is done using automated means.

The right to data portability is not limited to data explicitly provided by individuals; it also covers data collected through observing them.

Are staff trained to decide whether to apply the right to data portability?	☐ Yes ☐ No

The right to data portability must not adversely affect other people. In particular:

- If the personal data contains information about a third party, it is necessary to assess whether that person's rights and freedoms may be affected.
- If the data relates to several people (for example, a joint bank account), the consent of all the individuals concerned must be sought.

Does the procedure for implementing the right to data portability take into account the effect on the rights and freedoms of other people?	☐ Yes ☐ No

Staff must be adequately trained to recognise data portability requests.

Has a procedure been established for managing data portability requests?	☐ Yes ☐ No
Do the staff dealing with data subjects have the necessary training to recognize data portability requests?	☐ Yes ☐ No

The Regulation specifies how data portability must be implemented.

Is a structured format used, commonly used and easy to read mechanically?	☐ Yes ☐ No

3.2.8 Right to object

Individuals have the right to object to the processing of their personal data when the processing is based on:

- The public interest or the exercise of official authority vested in the controller.
- The legitimate interest of the data controller.

In this case, the controller must cease processing unless they can demonstrate compelling legitimate grounds that override the rights of the data subject.

Are staff trained to decide whether to apply the right to object?	☐ Yes ☐ No

Staff must be adequately trained to recognise requests to object to processing.

Has a procedure been established for the management of requests to object to processing?	☐ Yes ☐ No
Do the staff who deal with data subjects have the necessary training to recognize requests to object to processing?	☐ Yes ☐ No

The regulation specifies how to act upon receiving a request to object to processing in various cases.

If the request is to object to processing for marketing purposes, it must be accepted without exception.	☐ Yes ☐ No
If the request is to object to processing for scientific or historical research purposes, or for statistical purposes, it must be accepted unless the processing is carried out in the public interest.	☐ Yes ☐ No

3.2.9 Right not to be subject to automated decisions

Is automated processing carried out that produces legal effects or other similarly significant effects on individuals?	☐ Yes ☐ No
If so, what legal basis allows it?	
It is necessary for the performance of a contract between the data subject and the controller.	☐ Yes ☐ No
It is authorised by Union or Member State law.	☐ Yes ☐ No
The data subject has given their explicit consent.	☐ Yes ☐ No

The data subject always has the right to obtain human intervention, to express their point of view and to challenge the decision.

Is there a procedure allowing individuals to request human intervention, express their point of view and challenge the decision?	☐ Yes ☐ No
Are there staff within the organisation who are qualified to review decisions and change them?	☐ Yes ☐ No

Automated decisions may only use special categories of data if the data subject has given their explicit consent or if the processing is necessary to protect the vital interests of the data subject or another person.

Are special categories of data used in automated processing?	☐ Yes ☐ No
If so, what legal basis allows it?	
The data subject has given their explicit consent.	☐ Yes ☐ No
The processing is carried out to protect the vital interests of the data subject or another person.	☐ Yes ☐ No

3.3. Data security risks

Under the GDPR, the measures used to protect information must be appropriate to the risks to individuals' rights and freedoms. In this section we follow a simple methodology to analyse risks related to data security. That is, the risks associated with the loss of confidentiality, integrity and availability of data.

3.3.1 Impact

We assess the impact of the loss of confidentiality, integrity and availability of personal data on the data subject.

To determine the impact of a data security breach on individuals, the characteristics of the processing must be taken into account. Among others :

- The processing of special categories of data or other particularly sensitive data (financial information, locations, etc.).
- The monitoring of people.
- The processing of data from groups with special needs (minors, authorities, etc.).
- The processing of large amounts of data on each person.

To put the impact assessment into context, different scenarios are considered in which some of these properties are lost.

The impact on individuals of a loss of data confidentiality (i.e. unauthorised access to data).

Examples of breaches of confidentiality:

- Loss or theft of a computer containing personal data.
- Accidentally sending personal data to unauthorised individuals.
- Possibility of unauthorized access to a person's account.
- A configuration error on a website exposes the personal data of its users.
- Theft of information from the premises of the controller or processor.
- An employee at a medical centre accesses a patient's medical records without authorisation.

Impact

Low	Medium	High	Very high

Justification

The impact on individuals of a loss of data integrity (i.e. unauthorised modification of data).

- An employee mistakenly modifies a customer's data.
- An error in the communications network alters data while it is in transit.
- For operational reasons, a company maintains multiple copies of data, but a change in one of the copies is not propagated to the others.
- Loss of part of a file due to a failure in the processing system.

Impact

Low	Medium	High	Very high

Justification

The impact on individuals of a loss of data availability.

Examples of loss of data availability:

- A file is corrupted or erased and there is no backup.
- A file for which only a paper copy exists is lost.
- A data access service becomes unavailable (for example, a service providing access to electronic health records).

Impact			
Low	Medium	High	Very high

Justification

The impact on the system will be the highest of the three levels.

Impact			
Low	Medium	High	Very high

Justification

3.3.2 Initial probability

The following table shows processing characteristics that increase data security risks. We will estimate the probability of security failure based on the number of characteristics that are met.

Hardware and software	
Q1. Is the processing system connected to systems external to the organization? Connecting to systems external to the organization increases exposure to threats, as information can be captured or maliciously modified while in transit. This occurs, for example, when cloud services are used, remote workers connect to the organisation's systems, or access to the internal network is permitted via the internet to connect to corporate databases, among other scenarios.	☐ Yes ☐ No

Hardware and software

Q2. Is any part of the processing done online? Interaction with data subjects over the internet exposes the processing system to external threats, such as phishing , SQL injection, man-in-the-middle attacks, DoS and XSS . These threats can compromise the processing system and affect the security of the data (confidentiality, integrity and availability). Allowing staff to access the processing system via the internet also increases exposure to external attacks. It also increases the risk of staff misusing information, whether accidentally or intentionally. Examples include processing activities involving email, systems maintained or monitored over the internet, and the use of cloud services such as Google Drive, Microsoft OneDrive, Amazon Web Services (AWS) and Microsoft Azure.	☐ Yes ☐ No
Q3. Is there a lack of documentation on relevant best practices for the design or configuration of the processing system? If the processing system is not well designed or the elements that make it up are not properly configured, the risks to data security increase. To ensure that the processing system is properly designed and configured, numerous security guidelines are available covering different areas, such as local network design, firewalls, network segmentation, virtual private networks (VPNs), operating system configuration, antivirus software, secure passwords and multi-factor authentication (MFA). Having a best practices document helps ensure that the processing system is appropriately sized to meet computational, communication, security and storage requirements. It also helps ensure that software is correctly configured, a development methodology that prioritises data security throughout the application's life cycle is applied, secure cloud applications are used, and criteria are established regarding the use and types of data that can be managed in this environment, among other measures.	☐ Yes ☐ No
Q4. Is there a lack of a relevant best practices document covering the maintenance, monitoring and incident response of the processing system? Having a best practices document that covers these aspects is essential to ensure proper maintenance, monitoring, and a response plan for system incidents. Maintenance must be carried out on both hardware and software. Monitoring allows incidents to be analysed after they occur and helps detect suspicious behaviour to prevent incidents or reduce their impact. The incident response plan allows for a systematic approach to addressing and managing security incidents. This best practices document can cover important tasks such as applying operating system security updates, performing regular backups, using automated systems to detect or correlate security events, and conducting periodic audits to assess vulnerabilities and overall security, among others.	☐ Yes ☐ No

Hardware and software

Q5. Is there a lack of physical security at the facilities where processing takes place? The physical security of processing facilities is essential. Without this, the security of the processing system (whether electronic or not) cannot be guaranteed. This can occur, for example, when the data centre is not adequately protected against unauthorised access or natural and industrial hazards (electrical failures, fires, etc.); when files are distributed across different locations in a way that compromises their security; or when cloud services are used without adequate guarantees that the provider's facilities are properly protected, among other situations.	☐ Yes ☐ No

Use of the processing system

Q6. Is there a lack of clarity in defining staff roles and responsibilities? A lack of clarity in defining roles and responsibilities can lead to uncontrolled use of data (whether accidental or intentional). For example, a worker should only consult the data they need to carry out their tasks. They must also be responsible for destroying information when it is no longer needed and ensuring its security when it is shared with another organisation or person, among other responsibilities.	☐ Yes ☐ No
Q7. Is there a lack of clarity in the definition of acceptable uses of processing systems? When acceptable uses of processing systems are not clearly defined, the risk of misuse and introducing vulnerabilities into the system increases. For example, installing file-sharing software could lead to the unintentional sharing of information, while accessing malicious websites could allow malware to enter the system or facilitate data theft, among other risks.	☐ Yes ☐ No
Q8. Can staff connect external devices to the system? Connecting external devices (mobile phones, USB drives, etc.) to the processing system can pose a security risk, as this can facilitate the introduction of malware and vulnerabilities, as well as the unauthorised extraction of information. For this reason, it is essential to establish a clear policy that regulates the use of external devices by the organization's staff.	☐ Yes ☐ No
Q9. Is there a lack of an adequate procedure for logging and monitoring processing activities? The lack of an activity log (log file) can encourage poor practices among staff and make it difficult to investigate incidents after they occur due to a lack of traceability,	☐ Yes ☐ No

Use of the processing system

as set out in Spain's National Security Framework (ENS). This compromises the ability to detect, analyse and respond to possible threats. Therefore, an adequate logging system must be in place to identify who accesses information systems and ensure that logged activities are effectively monitored.	

People involved in the processing

Q10. Are staff granted access permissions that are not necessary to perform their assigned tasks? The greater the number of people who have access to data, the greater the likelihood that abuse will occur. To avoid this, it is essential that the system controls staff access and only authorises access that is strictly necessary for staff to perform their assigned tasks.	☐ Yes ☐ No
Q11. Has any part of the processing been outsourced to a processor? The processor is the natural or legal person, public authority, service or body that provides the controller with a service that involves the processing of personal data on behalf of the controller. For example, a company or public entity that provides an information hosting service on its servers or manages a municipal public service, among other examples. The outsourcing of processing or part of the processing to a processor involves a loss of control over the data. It is necessary to choose a processor who offers sufficient guarantees regarding the implementation and maintenance of appropriate security measures, and clearly define their responsibilities.	☐ Yes ☐ No
Q12. Is there a lack of knowledge among staff regarding the proper use of the system, data security or the restrictions on its use imposed by the GDPR? A lack of knowledge about the expected use of the system, information security or the obligations and limitations imposed by the GDPR can give rise to poor practices. For example, staff may be more likely to follow instructions contained in a phishing email or fail to recognise the need to ensure the security of documents when saving them, among other situations.	☐ Yes ☐ No
Q.13. Is there any mechanism for human oversight of the AI system?	☐ Yes ☐ No

Other features	
Q14. Has the company or other companies in the sector suffered attacks recently? Previous attacks should serve as lessons for identifying vulnerabilities and strengthening security, as well as warnings of potential future attacks.	☐ Yes ☐ No
Q15. Have any complaints been received recently regarding the stability or security of the processing system? The presence of errors in the processing system increases the likelihood of suffering an attack. Similarly, alerts or warnings regarding potential system security failures can also indicate a higher probability of suffering attacks.	☐ Yes ☐ No
Q16. Is data of special interest or data relating to a very large number of users being processed? The processing of large volumes of data or data of special interest provides additional motivation for potential attackers.	☐ Yes ☐ No

We calculate the initial probability based on the number of affirmative answers, according to the following table:

Affirmative Answers	Initial Probability
0 - 4	Low
5 – 9	Medium
10 - 15	High

Number of affirmative answers	
Estimated initial probability	

3.3.3 Initial risk

Once the impact and initial probability have been estimated, we will apply the table in Section 3.1.7 to calculate the initial risk (without security controls).

Impact on confidentiality	
Impact on integrity	
Impact on availability	
Maximum impact	
Probability	
Initial risk	

3.3.4 Security controls

Once the initial risk has been calculated, it is necessary to determine which controls (measures to improve security) should be applied.

There are many lists of security controls. Here we use the controls set out in Spain's National Security Framework (ENS, Royal Decree 311/2024). The ENS controls are quite complex. In the DPIA Guide, you will find guidance and criteria for determining which controls to apply.

Low	Medium	High	Control	Applied
Organizational framework				
Yes	Yes	Yes	Security policy [org.1] (system)	
Yes	Yes	Yes	Security regulations [org.2] (system)	
Yes	Yes	Yes	Security procedures [org.3] (system)	
Yes	Yes	Yes	Authorization process [org.4] (system)	
Operational Framework				
				Planning
Yes	Yes	Yes	Security architecture [op.pl.2] (system)	
Yes	Yes	Yes	Acquisition of new components [op.pl.3] (system)	
Yes	Yes	Yes	Capacity planning [op.pl.4] (D)	
No	Yes	Yes	Certified components [op.pl.5] (system)	
				Access control

Low	Medium	High	Control	Applied
Yes	Yes	Yes	Identification [op.acc.1] (system)	
Yes	Yes	Yes	Access requirements [op.acc.2] (ICAT)	
No	Yes	Yes	Segregation of functions and tasks [op.acc.3] (ICAT)	
Yes	Yes	Yes	Access rights management process [op.acc.4] (ICAT)	
Yes	Yes	Yes	Authentication mechanism for external users [op.acc.5] (ICAT)	
Yes	Yes	Yes	Authentication mechanism for internal users [op.acc.6] (ICAT)	
				Operations
Yes	Yes	Yes	Asset inventory [op.exp.1] (system)	
Yes	Yes	Yes	Security settings [op.exp.2] (system)	
Yes	Yes	Yes	Security configuration management [op.exp.3] (system)	
Yes	Yes	Yes	Maintenance and security updates [op.exp.4] (system)	
No	Yes	Yes	Change management [op.exp.5] (system)	
Yes	Yes	Yes	Malicious code protection [op.exp.6] (system)	
Yes	Yes	Yes	Incident management [op.exp.7] (system)	
Yes	Yes	Yes	User activity record [op.exp.8] (system)	
Yes	Yes	Yes	Incident management record [op.exp.9] (system)	
Yes	Yes	Yes	Cryptographic key protection [op.exp.10] (system)	
				External services
No	Yes	Yes	Contracting and service level agreements [op.ext.1] (system)	

Low	Medium	High	Control	Applied
No	Yes	Yes	Daily management [op.ext.2] (system)	
No	No	Yes	Supply chain protection [op.ext.3] (system)	
No	Yes	Yes	Systems interconnection [op.ext.4] (system)	
				Cloud services
Yes	Yes	Yes	Protection of cloud services [op.nub.1] (system)	
				Continuity of service
No	Yes	Yes	Impact analysis [op.cont.1] (D)	
No	No	Yes	Continuity plan [op.cont.2] (D)	
No	No	Yes	Periodic tests [op.cont.3] (D)	
No	No	Yes	Alternative means [op.cont.4] (D)	
				System monitoring
Yes	Yes	Yes	Intrusion detection [op.mon.1] (system)	
Yes	Yes	Yes	Metrics system [op.mon.2] (system)	
Yes	Yes	Yes	Surveillance [op.mon.3] (system)	
Protective measures				
				Protection of facilities and infrastructures
Yes	Yes	Yes	Separate areas and access control [mp.if.1] (system)	
Yes	Yes	Yes	Identification of people [mp.if.2] (system)	
Yes	Yes	Yes	Environmental control of premises [mp.if.3] (system)	
Yes	Yes	Yes	Electrical power [mp.if.4] (D)	
Yes	Yes	Yes	Fire protection [mp.if.5] (D)	
No	Yes	Yes	Flood protection [mp.if.6] (D)	

Low	Medium	High	Control	Applied
Yes	Yes	Yes	Equipment entry and exit logging [mp.if.7] (system)	
				Personnel management
No	Yes	Yes	Characterization of the workplace [mp.per.1] (system)	
Yes	Yes	Yes	Duties and obligations [mp.per.2] (system)	
Yes	Yes	Yes	Awareness [mp.per.3] (system)	
Yes	Yes	Yes	Training [mp.per.4] (system)	
Equipment protection				
Yes	Yes	Yes	Clear desk [mp.eq.1] (system)	
No	Yes	Yes	Workstation locking [mp.eq.2] (system)	
Yes	Yes	Yes	Laptop protection [mp.eq.3] (system)	
Yes	Yes	Yes	Other devices connected to the network [mp.eq.4] (C)	
				Communications protection
Yes	Yes	Yes	Secure perimeter [mp.com.1] (system)	
Yes	Yes	Yes	Confidentiality protection [mp.com.2] (C)	
Yes	Yes	Yes	Authenticity and integrity protection [mp.com.3] (IA)	
No	Yes	Yes	Segregation of information flows [mp.com.4] (system)	
				Protection of information storage media
Yes	Yes	Yes	Labelling [mp.si.1] (C)	
No	Yes	Yes	Cryptography [mp.si.2] (IC)	
Yes	Yes	Yes	Custody [mp.si.3] (system)	
Yes	Yes	Yes	Transport [mp.si.4] (system)	

Low	Medium	High	Control	Applied
Yes	Yes	Yes	Erasure and destruction [mp.si.5] (C)	
				Protection of computer applications
No	Yes	Yes	Application development [mp.sw.1] (system)	
Yes	Yes	Yes	Acceptance and commissioning [mp.sw.1] (system)	
				Information protection
No	Yes	Yes	Information classification [mp.info.2] (C)	
Yes	Yes	Yes	Electronic signature [mp.info.3] (IA)	
No	No	Yes	Timestamps [mp.info.4] (T)	
Yes	Yes	Yes	Document sanitisation [mp.info.5] (C)	
Yes	Yes	Yes	Backups [mp.info.6] (D)	
				Protection of services
Yes	Yes	Yes	Email protection [mp.s.1] (system)	
Yes	Yes	Yes	Protection of web services and applications [mp.s.2] (system)	
Yes	Yes	Yes	Web browsing protection [mp.s.3] (system)	
No	Yes	Yes	Denial-of-service protection [mp.s.4] (D) (impact, probability)	

3.3.5 Residual impact

Security controls can reduce the impact of a security incident. For example, encrypting certain information can limit the extent of a loss of confidentiality; a backup can limit the

impact of a loss of information availability; and electronic signatures can help detect a loss of integrity and thus reduce its impact.

Impact that the loss of confidentiality of data (i.e. unauthorised access to data) has on people

Impact

Low	Medium	High	Very high

Residual impact

Low	Medium	High	Very high

Justification

Impact that the loss of integrity of data (i.e. unauthorised modification of data) has on people

Impact

Low	Medium	High	Very high

Residual impact

Low	Medium	High	Very high

Justification

Impact that the loss of availability of data has on people

Impact

Low	Medium	High	Very high

Residual impact

Low	Medium	High	Very high

Impact that the loss of availability of data has on people

Justification

Impact that the loss of availability of data has on people

Impact			
Low	Medium	High	Very high

Residual impact			
Low	Medium	High	Very high

Justification

The residual impact of the system will be the highest of the three preceding values.

Residual impact of the system

Low	Medium	High	Very high

3.3.6 Residual probability

To reduce the probability, it is necessary to eliminate the underlying circumstances that lead to affirmative answers to the questions in section 3.2.2.

In many cases, it is not feasible to eliminate the circumstances associated with the questions in section 3.2.2. In this case, to change an affirmative answer to a negative one, it is necessary to demonstrate that, in the context of the processing system, the implemented controls mean that the factor addressed by the question has a negligible influence on the occurrence of security incidents.

The answers provided when calculating the initial probability must be reviewed, taking into account the controls implemented.

Answer only those questions for which the answer has changed as a result of the controls implemented. Examples of security measures have been provided to justify this change, although other controls may also reduce the probability.

Hardware and software

Q1	Is the processing system connected to systems external to the organization?	
	Controls implemented and justification for reducing probability	
	Any measure related to access control, external services, cloud services or system monitoring.	
Q2	Is any part of the processing done online?	
	Controls implemented and justification for reducing probability	
	Any measure related to access control, external services, cloud services or system monitoring.	
Q3	Is there a lack of documentation on relevant best practices for the design or configuration of the processing system?	
	Controls implemented and justification for reducing probability	
	Any measure related to organisational matters or staff training.	
Q4	Is there a lack of a relevant best practices document covering the maintenance, monitoring and incident response of the processing system?	
	Controls implemented and justification for reducing probability	
	Any measures related to staff training, monitoring or record-keeping.	
Q5	Is there a lack of physical security at the facilities where processing takes place?	
	Controls implemented and justification for reducing probability	
	Any measure related to monitoring or record-keeping.	

Procedures related to processing

Q6	Is there a lack of clarity in defining staff roles and responsibilities?	
	Controls implemented and justification for reducing probability	
	Any organisational measure and/or measure related to staff training.	
Q7	Is there a lack of clarity in the definition of acceptable uses of processing systems?	
	Controls implemented and justification for reducing probability	
	Any measure related to staff training.	
Q8	Can staff connect external devices to the system?	
	Controls implemented and justification for reducing probability	
	Any measure related to access control, external services, cloud services or system monitoring.	
Q9	Is there a lack of an adequate procedure for logging and monitoring processing activities?	
	Controls implemented and justification for reducing probability	
	Any measure related to access control, external services, cloud services or system monitoring.	

People involved in the processing

Q10	Are staff granted access permissions that are not necessary to perform their assigned tasks?	
	Controls implemented and justification for reducing probability	
	Any measure related to access control and user training.	
Q11	Has any part of the processing been outsourced to a processor?	
	Controls implemented and justification for reducing probability	

People involved in the processing

	Any measure related to access control, external services, cloud services or system monitoring.	
Q12	Is there a lack of knowledge among staff regarding the appropriate use of the system, data security or the restrictions on use imposed by the GDPR?	
	Controls implemented and justification for reducing probability	
	Any measure related to staff training.	

Other features

Q13	Has the company or other companies in the sector suffered attacks recently?	
	Controls implemented and justification for reducing probability	
	For example, improvements have been made to the authentication of internal and external users, incident management, and the surveillance and monitoring of systems or the corporate network itself.	
Q14	Have any complaints been received recently regarding the stability or security of the processing system?	
	Controls implemented and justification for reducing probability	
	For example, improvements have been made to internal security procedures, security configuration management or the system of metrics.	
Q15	Is data of special interest or data relating to a very large number of users being processed?	
	Controls implemented and justification for reducing probability	
	For example, improvements have been made to security configuration management, redundant systems have been introduced, or other systems have been implemented to improve confidentiality, integrity or authenticity.	

The residual probability is calculated by counting the affirmative answers.

Affirmative answers	Initial probability
0 - 4	Low
5 – 9	Medium
10 - 14	High

3.3.7 Estimation of residual risk

Once the residual impact and residual probability have been estimated, we calculate the residual risk following the table in Section 3.1.7.

	Impact			
Probability	Low	Medium	High	Very high
Low	Low risk	Low risk	Medium risk	High risk
Medium	Low risk	Medium risk	High risk	High risk
High	Medium risk	High risk	High risk	High risk

Residual impact on confidentiality Residual impact on integrity Residual impact on availability	
Maximum residual impact Residual probability	
Residual risk	

If the residual risk is high, new controls must be proposed to reduce it. If the residual risk cannot be reduced, the competent data protection authority must be consulted before processing begins to determine whether the processing is appropriate.

4. Fundamental Rights Impact Assessment

This section examines the impacts on fundamental rights and freedoms other than the right to data protection, which have already been the subject of the DPIA.

4.1 Planning and scoping questionnaire

Section A[5] Complementary description of the AI system, including the related data flows	What are the main objectives of the AI system? What types of data are processed (personal, non-personal, special categories)?
Section B Fundamental rights context	What fundamental rights are potentially affected by the use of the AI system? What international/regional legal instruments for the protection of human/fundamental rights have been applied at the operational level? What are the most relevant courts or bodies in the field of fundamental rights in the context of use? What are the most relevant decisions and provisions on human/fundamental rights?
Section C Controls in place	What policies and procedures have been implemented to assess the potential impact on fundamental rights, including stakeholder engagement? Has an impact assessment been carried out, developed and implemented in relation to specific issues (e.g. data protection) or certain features of the system (e.g. the use of biometrics)?
Section D Stakeholder engagement and due diligence	What are the main groups or communities potentially affected by the AI system, including its development? In addition to individuals or groups that may be affected by AI systems, which other stakeholders should be involved (e.g. civil society,

[5] In Section A of the DPIA-FRIA integrated model, questions relating to the main characteristics of the system, the countries in which it will be offered, and the identification of those affected and of those responsible have been moved from the FRIA model to the general evaluation section (1.3 'Description and analysis of the AI system').

	international organisations, experts, industry associations and journalists)? Are there other duty bearers who should be involved, apart from the AI provider and deployer (e.g. national authorities, government agencies)? Have business partners, including service providers (e.g., subcontractors on AI systems and datasets) been involved in the assessment process? Has the AI provider conducted an assessment of its supply chain to identify whether the activities of suppliers/subcontractors involved in AI development may affect fundamental rights? Has the provider promoted fundamental rights standards or audits to ensure respect for fundamental rights among suppliers/subcontractors? Have the AI provider and deployer publicly communicated the potential impact of the AI system on fundamental rights? Have the AI provider and deployer provided training on fundamental rights standards to the personnel responsible for the management and procurement of the AI system?

4.2 Risk matrices

Table 1. Probability

Low	The risk of prejudice is either improbable or highly improbable.
Medium	The risk of prejudice is possible.
High	The risk of prejudice is expected to occur.
Very high	The risk of prejudice is almost certain to occur.

Table 2. Exposure

Low	Few or very few individuals in the identified population of rights holders are potentially affected.
Medium	A substantial part, but not the majority, of the identified population of rights holders is potentially affected.

High	The majority of the identified population of rights holders is potentially affected.
Very high	Almost the entire identified population of rights holders is potentially affected.

Table 3. Likelihood of harm occurring

		Probability			
		Low	**Medium**	**High**	**Very high**
Exposure	**Low**	L	L/M	L/H	L/VH
	Medium	M/L	M	M/H	M/VH
	High	H/L	H/M	H	H / VH
	Very high	VH/L	VH/M	VH/H	VH

Probability			
Low	Medium	High	Very high

Table 4. Severity of the harm

Low	Affected individuals and groups may experience only minor harm in the exercise of their rights and freedoms.
Medium	Affected individuals and groups may experience moderate harm in the exercise of their rights and freedoms.
High	Affected individuals and groups may experience serious harm in the exercise of their rights and freedoms.
Very high	Affected individuals and groups may experience severe harm in the exercise of their rights and freedoms.

Table 5. Effort required to overcome harm and reverse adverse effects

Low	The harm suffered can be overcome with little or no difficulty (e.g. time spent modifying information, inconvenience, irritation, etc.).
Medium	The harm suffered can be overcome despite some difficulties (e.g. additional costs, fear, misunderstanding, stress, minor physical ailments, etc.).
High	The harm suffered can be overcome only with considerable difficulties (e.g. significant economic losses, material damage, deterioration of health, etc.).
Very high	The harm suffered is extremely difficult, if not impossible, to overcome (e.g. long-term psychological or physical ailments, death, etc.).

Table 6. Severity

		Severity of impact			
		Low	**Medium**	**High**	**Very high**
Effort	**Low**	L	L/M	L/H	L/VH
	Medium	M/L	M	M/H	M/VH
	High	H/L	H/M	H	H/VH
	Very high	VH/L	VH/M	VH/H	VH

Severity			
Low	Medium	High	Very high

Table 1A. Data collection and risk analysis

Rights/ Potentially affected freedoms	**Description of the impact**	**Probability**			**Severity**		
		Probability of adverse outcomes	**Exposure**	**Probability**	**Severity of impact**	**Effort**	**Severity**

Table 7. Overall risk impact

		Severity			
		Low	Medium	High	Very high
Probability	Low				
	Medium				
	High				
	Very high				

Overall risk			
Low	Medium	High	Very high

Table 2A. Risk management (I)

Rights/freedoms affected	Probability	Severity	Overall impact	Measures to prevent/mitigate the impacts

Table 3A. Risk management (II)[6]

Rights/freedoms affected	Probability (residual)	Severity (residual)	Residual impact

[6] In this table, a reference must be included to the final result of the DPIA in terms of residual probability and severity. This can be done by linking to the specific page of the DPIA where the measures adopted are described.