

Data Protection Impact Assessment (DPIA) Template

This template is an example of how you can record your DPIA process and outcome.. You may also wish to refer to the guidance “Criteria for an acceptable DPIA” published by the European Data Protection Board (previously the Article 29 Working Party) guidelines on DPIAs.

You should start to fill out the template at the very start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

This template is intended to provide a starting point and should be amended, reordered, and/or added to as necessary and as appropriate for the controller’s organisation and the nature and scope of the issues being considered as part of the DPIA.

Submitting controller details

Name of controller

Subject/title of DPO

Name of controller contact/DPO
(delete as appropriate)

Executive summary

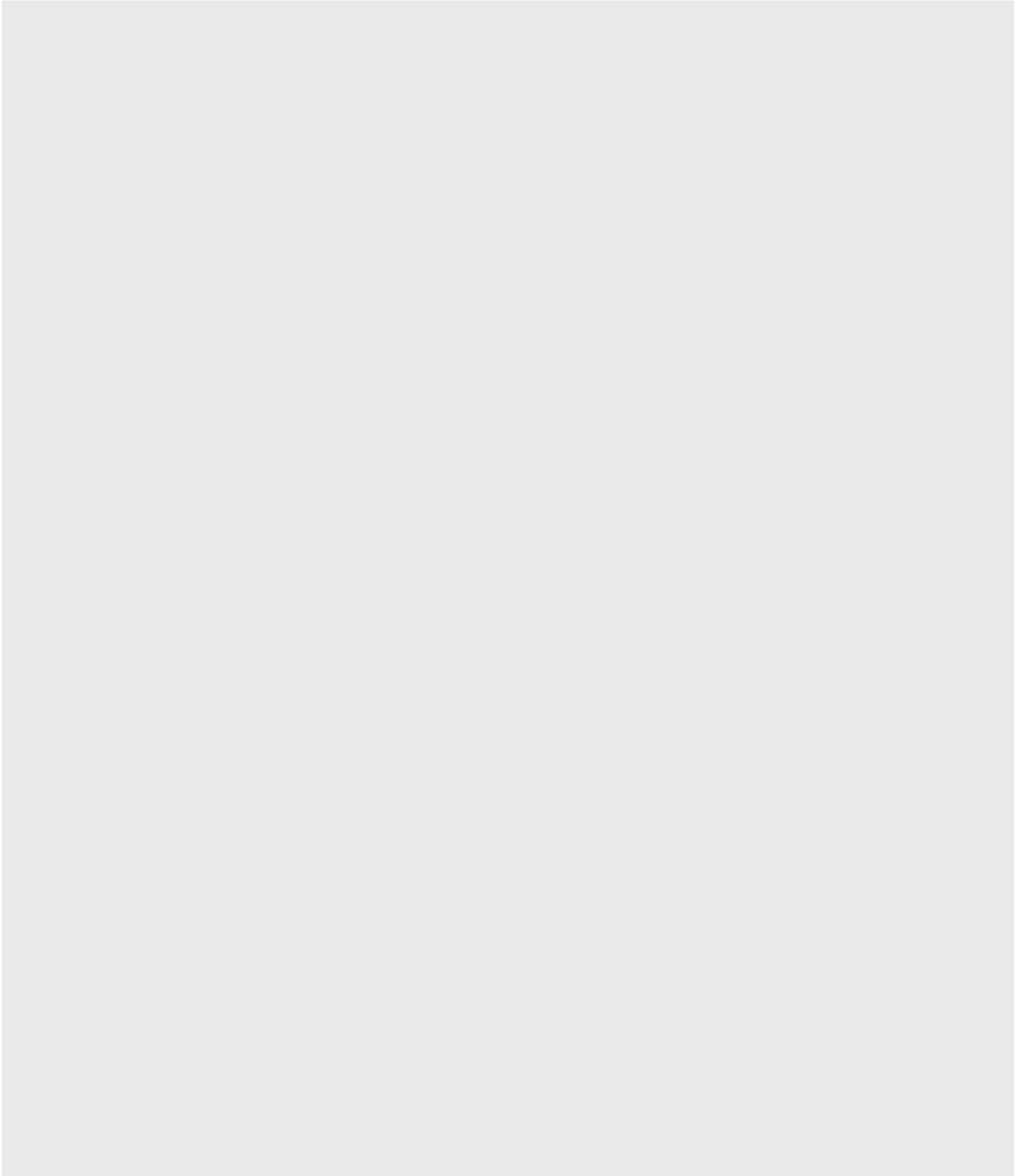
This section should record at a high level the key facts from the assessment as well as the conclusions drawn. The section should include:

- A high-level description of the proposed processing.
- A summary of the processing scope.
- A summary of the purposes for which processing will occur.
- A summary of the intended benefits for data subjects, third parties and the controller.
- A summary of the rationale as to why a DPIA is required.

Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal.

Summarise why you identified the need for a DPIA.



Step 2: Describe the processing

Describe the nature of the processing:

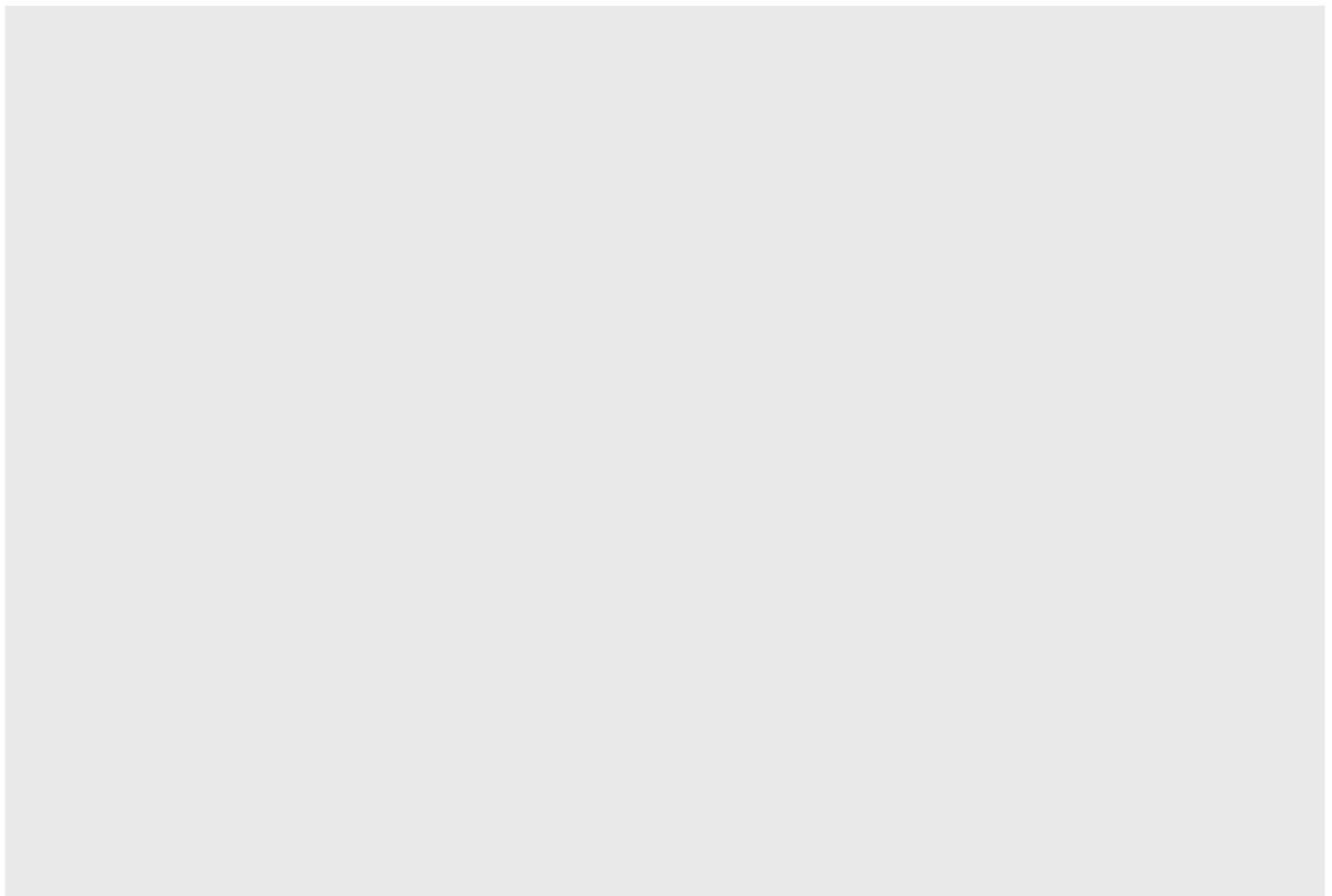
How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

You should consider all aspects of the processing such as the hardware, software, networks, people, paper, paper transmission channel(s), mobile devices and any other relevant medium. Also consider other elements that might be relevant such as the use of cookies and/or whether the solution is cloud-based.

Identify the type(s) of data that is involved - it is important to be clear, in the factual sense, as to what type of data is under consideration.

If you are making disclosure to third parties:

- Where is the recipient located?
- What is the recipient's role (controller or processor) with regard to the data?
- What data is to be disclosed to them and why?
- Does all of the data identified for disclosure need to be disclosed? (In other words, what data minimisation steps can be taken?)
- What agreements need to be put in place with the recipients?
- Is a separate DPIA required?
- What monitoring/contract management arrangements need to be put in place?

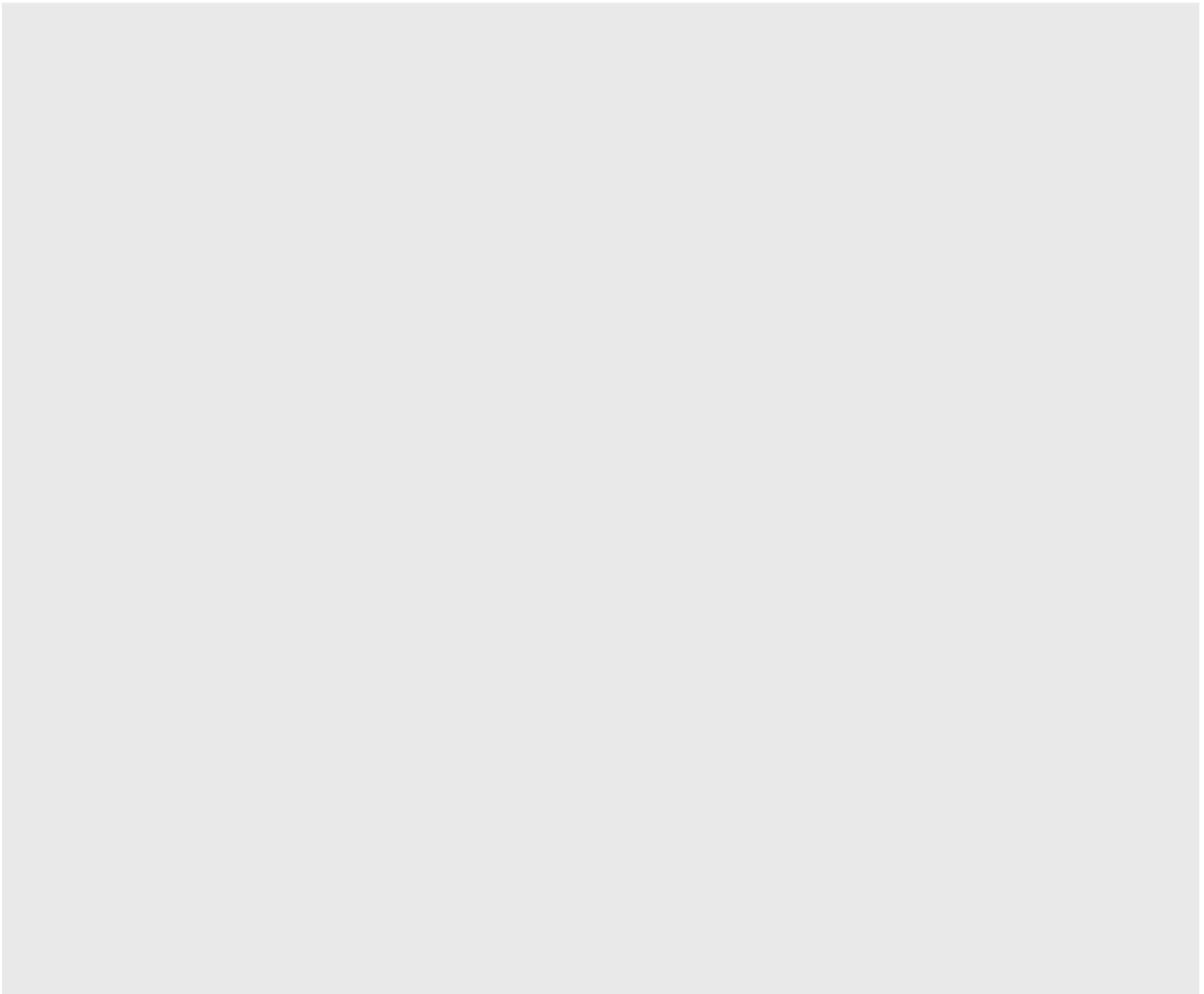


Describe the scope of the processing:

What is the nature of the data, and does it include special category data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

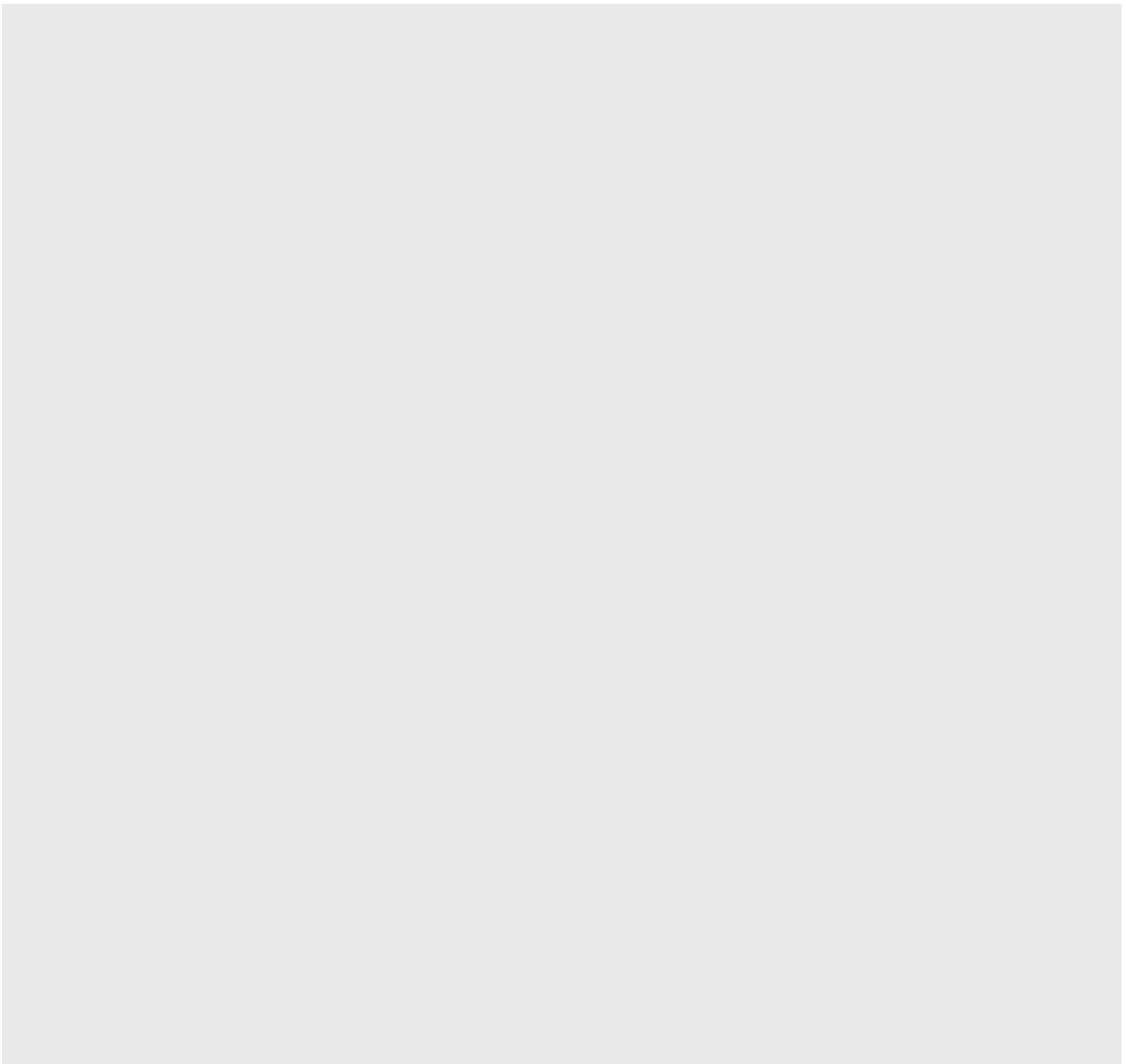
When describing the data processing operations, it is useful to consider:

- The types of personal data.
- The categories of data subject.
- The sources of the personal data (such as whether it is from feeds from internal/external systems, purchased lists or collected directly from data subjects).
- The length and frequency of processing.
- The processing volumes.
- The approach that has been/will be taken to data minimization
- Any cross-border transfers
- Are any cloud solutions being used? Where does storage, backup and disaster recovery occur?



Describe the context of the processing:

- What is the nature of your relationship with the individuals?
- How much control will they have?
- Would they expect you to use their data in this way?
- Do they include children or other vulnerable groups?
- Are there prior concerns over this type of processing or security flaws?
- Is it novel in any way?
- What is the current state of technology in this area?
- Are there any current issues of public concern that you should factor in?
- Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?



Describe the purposes of the processing:

What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The section is intended to focus on the purpose for which personal data is processed and to assess the intended benefits and risks. The [DPJL 2018] does not define “high risk” but does say that “In assessing the risk to the rights and freedoms of natural persons, regard must be had in particular to the use of new technologies, and the nature, scope, context and purposes of the processing” (Art.16(2)). For example:

- Automated processing (including profiling).
- Evaluation or scoring (including profiling or predicting).
- Automated decision-making with legal (or similar) effect.
- Large-scale processing of data.
- Processing of sensitive data or data of a highly personal nature.
- Systematic monitoring of publicly accessible area(s).
- Creation or use of personal profiles.
- Matching/combining datasets.
- Processing in relation to vulnerable data subjects.
- Innovative use or applying new technologies or innovative solutions.

The above list includes criteria identified by the European Data Protection Board –(EDPB) but is non-exhaustive. However, it provides a useful aid for identifying potential high-risk situations.

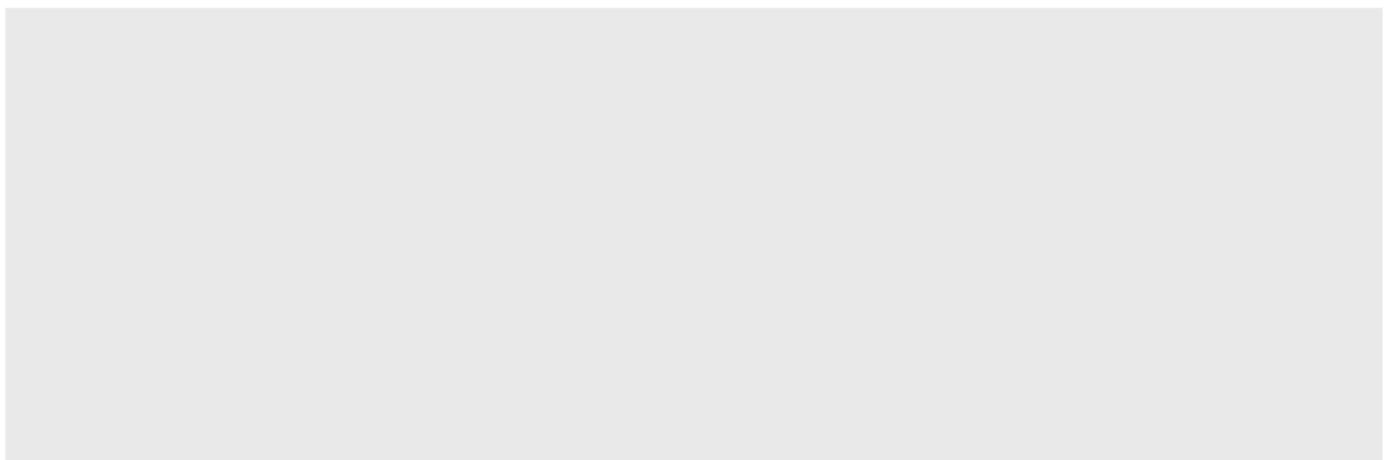
As part of the assessment, you should identify the benefits that may result from the processing.

Benefits could be to:

- (i) individuals (data subjects and users);
- (ii) groups of individuals; and
- (iii) organisations such as the controller/third parties; and/or
- (iv) wider society.

Also consider the risks associated with the processing, including to the data subjects, the controller itself and any other relevant stakeholders. Identify the type of risk, possible threats and sources of risk, the likelihood of risk occurring and the impact of the risk and the type of damage. Within this section, include any risks associated with not proceeding with the processing proposed.

Finally, but of utmost importance, also consider the risk mitigation options. Bear in mind that the quality and sufficiency of the risk mitigation steps that can be taken will impact on the need to consult with the supervisory authority.

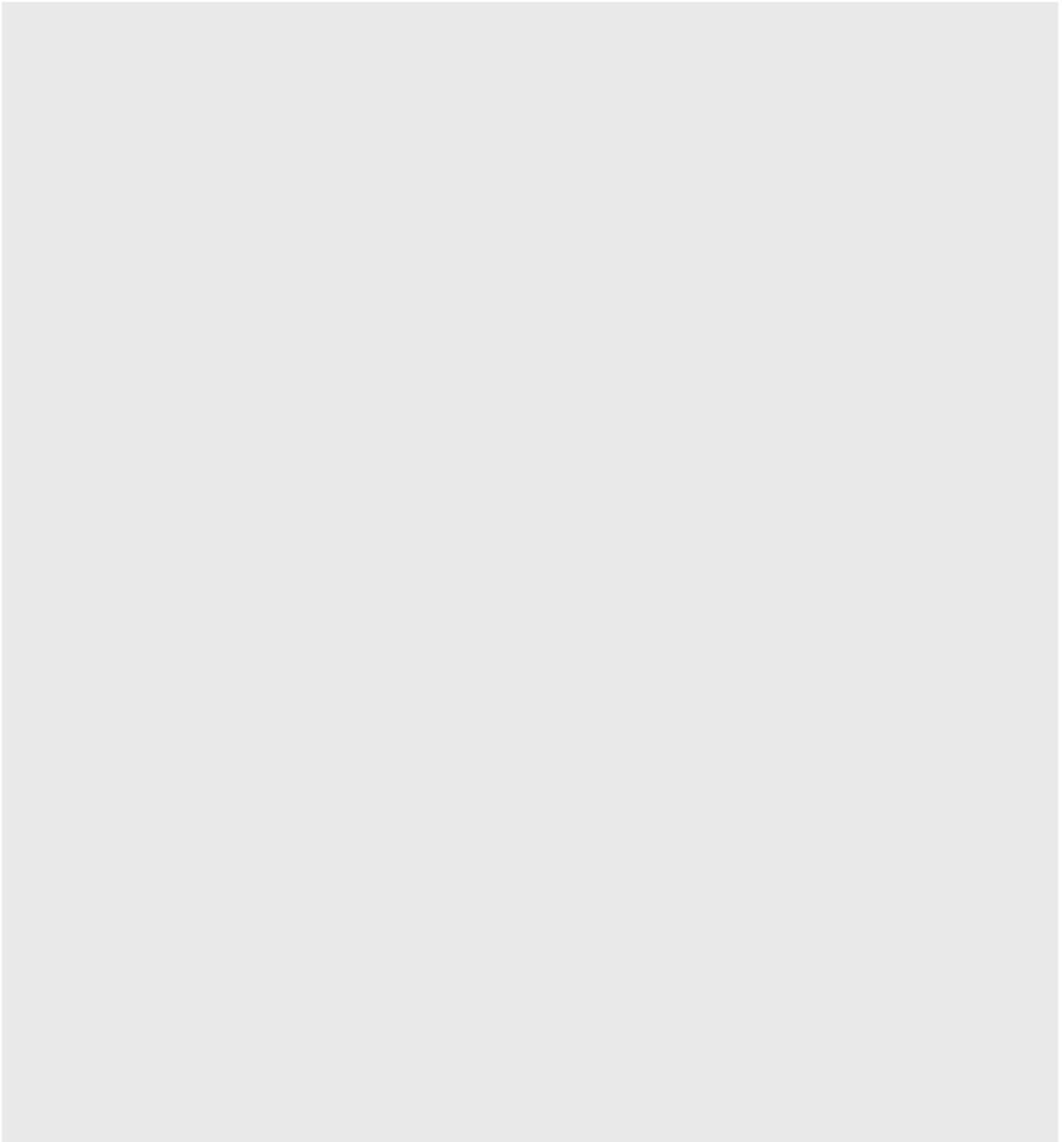


Describe the technical and organisational measures that will be put in place to ensure security of the personal data:

Consider practical measures such as identity and access management arrangements, training, communication and awareness, third party due diligence arrangements and third party contract management and monitoring arrangements.

Consider the range of technical security measures that can be implemented such as encryption, pseudonymisation and two-factor authentication. Ensure that arrangements for data security breach notification have been considered.

Record items such as steps taken for de-identification of data, arrangements for destruction of data and data back up and disaster recovery arrangements. Include records in relation to consents, privacy notices, data flow maps and approvals.



Step 3: Consultation process

Consider how to consult with relevant stakeholders:

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

This section should summarise the advice and input from all stakeholders and interested parties that have been consulted in relation to the DPIA. This will include the functional area/business unit carrying out the DPIA and the DPO (if there is one).

It will also comprise the advice and input of the data subjects, their representatives and other interested stakeholders as well as professional experts such as lawyers, IT experts, security experts, sociologists and ethics experts.

The EDPB advises that this input can be obtained “through a variety of means, depending on the context (for example, an internal or external study related to the purpose and means of the processing operation, a formal question to the staff representatives or trade/labour unions or a survey sent to the data controller's future customers)”.

In this section, therefore, summarise the input received and the decisions taken and consider including a copy of the input received as an annex to the DPIA.

DPO

The controller must also seek the advice of the DPO (where there is one) when completing the DPIA (Article 16(4) of the [DPJL 2018]). Under Article 26(1)(c), the DPO is required to monitor performance of the DPIA so may provide advice on an ongoing basis - the DPIA will need to be updated to take this into account. Advice received during the course of the DPIA should also be included as an annex.

Data subjects

Article 16(8) states the “controller must seek the views of data subjects or their representatives on the intended processing, without limiting the protection of commercial or public interests or the security of processing operations” or EDPB provides the following limited guidance:

- If the controller decides not to seek input from the data subjects, the controller must document its reason for not doing so.
- If the controller's final decision is different to the views of the data subjects, the controller should document the reason for the decision.
- Consent to processing is not a way for seeking the views of the data subjects.

Consultation with the supervisory authority

Under Article 17(1) of the [DPJL 2018], where risks cannot be mitigated, the controller should consult with the Authority. It is the controller's responsibility to determine when the risks cannot be mitigated.

Record any interaction with the Authority and identify whether a consultation is required or not. If a consultation is required summarise the output and the decisions made. Include any advice from the Authority as an annex to the DPIA.

Advice of DPO:

A large, solid gray rectangular area intended for providing advice from the Data Protection Officer (DPO).

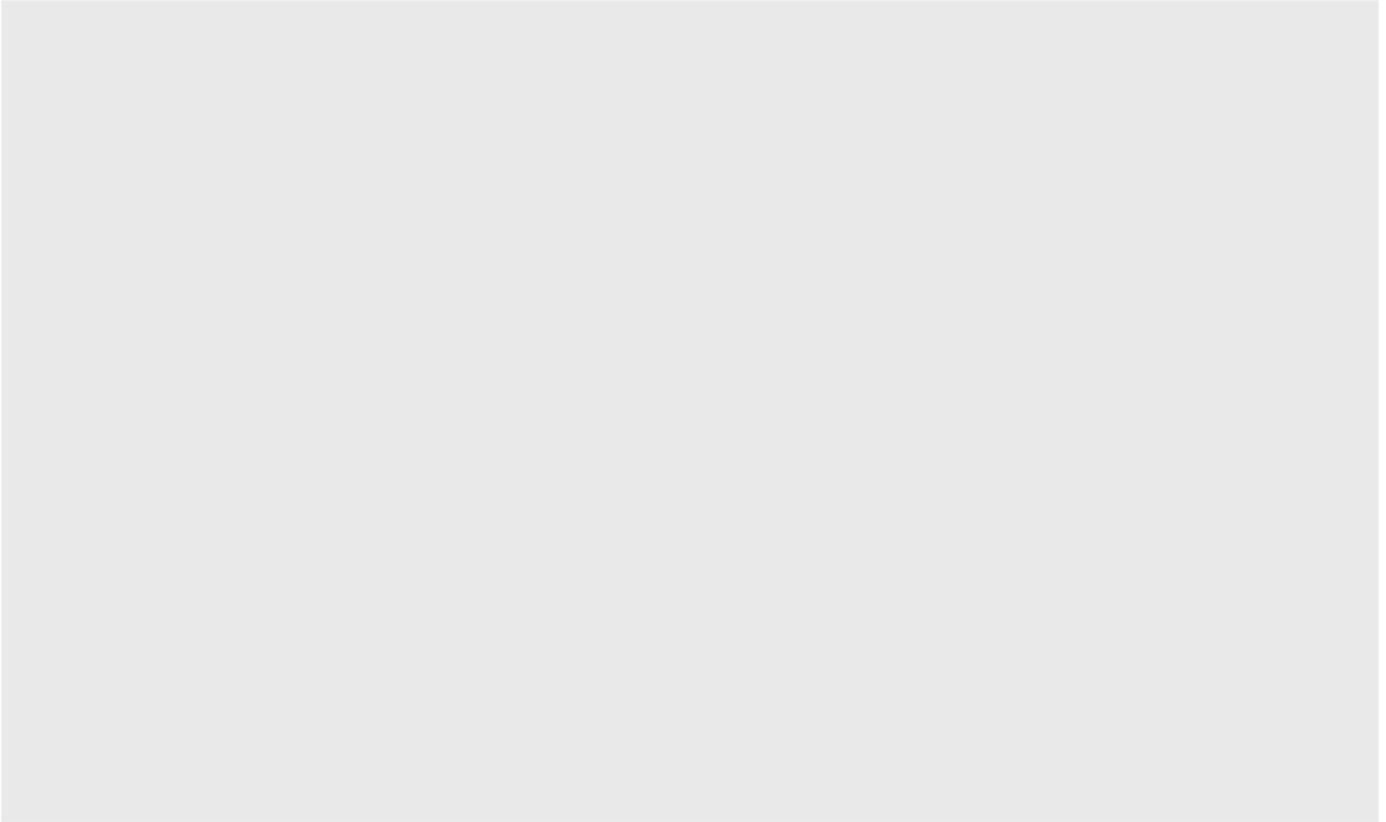
Input of specific business functions:

A large, solid gray rectangular area intended for providing input from specific business functions.

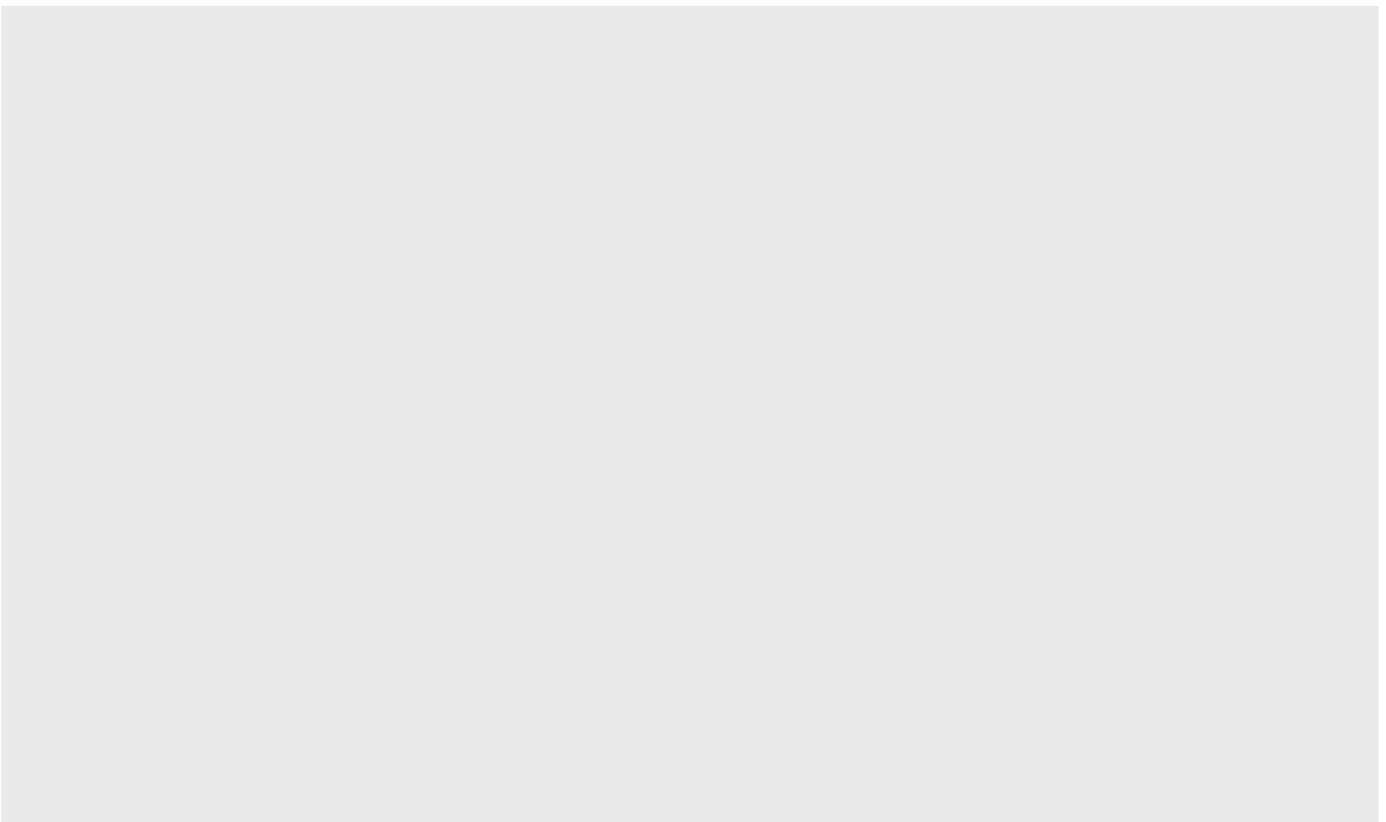
Input of data subjects and/or their representatives:

A large, solid gray rectangular area intended for providing input from data subjects and/or their representatives.

Input of experts and other interested stakeholders:

A large, solid grey rectangular area intended for providing input from experts and other interested stakeholders. It is currently empty.

Consultation with the JOIC:

A large, solid grey rectangular area intended for providing input from the JOIC. It is currently empty.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

- What is your lawful basis for processing?
 - Does the processing actually achieve your purpose?
 - Is there another way to achieve the same outcome?
 - How will you prevent function creep?
 - How will you ensure data quality and data minimisation?
 - What information will you give individuals?
 - How will you help to support their rights?
 - What measures do you take to ensure processors comply?
 - How do you safeguard any international transfers?
- 

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step 5.

Risk	Options to reduce or eliminate risk	Effect on risk Eliminated reduced accepted	Residual risk Low, medium or high	Measure approved Yes/no

Step 7: Sign off and record outcomes

This section records the final decision taken in relation to the DPIA. This should be completed by individual(s) with sufficient overall authority to make the decision to carry out the processing that is the subject of the assessment.

The controller may decide to:

- proceed on the basis of the findings of the DPIA;
- not proceed; or
- in the absence of measures taken by the controller to mitigate the risk, seek approval from the Authority (and/or other relevant supervisory authority) for the processing.

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the JOIC before going ahead
DPO advice provided:		Measures approved by:
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Step 8: Document history

Version No.	Summary of change	Date