General Overview

What are the reasons for conducting a DPIA?

- New processing activity
- Due to changes that occurred to the existing processing activity

Note: A processing activity includes both manual and electronic operations.

Is the DPO involved in the DPIA process?

Describe the nature, scope, context and purpose of envisaged processing.

E.g.: Does the processing include: solely automated and automated processing, including profiling, with legal or similar significant effect; systematic monitoring and evaluation of personal aspects including online behaviour, processing that would exceed the reasonable expectation of the data subjects, use of new technologies, processing of data on a large scale, processing for which the exercise of data subjects rights will prove to be impossible or result disproportionate, processing for which the notification of a breach will result disproportionate? Indicate the methods used for the processing operation.

Attach any relevant supporting documents, such as a project proposal, data flow diagrams, related systems documentation, etc.

Describe the processing operations related to the envisage processing.

E.g.: How will the personal data be collected, used, stored and deleted?

Legal basis for processing

Identify the proper legal ground(s), on the strength of which, the processing activity will be legitimised.

Article 6 GDPR sets out the legal criteria to process personal data.

Whereas the rule provides for a prohibition of the processing of special categories of data, the provisions of Article 9 foresee a list of derogations on which the controller can rely to justify the processing of sensitive data.

Categories of personal data processed

Identify the categories of personal data that will be processed, in particular, where special categories or data of a highly personal nature such as criminal offences or convictions or related security measures, or data concerning vulnerable data subjects such as children, location data, will be processed.

Security of processing

Identify and describe the technical and organisational measures adopted to protect the data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Did you consider the implementation of data protection by design and by default measures to enhance the security of personal data (such as pseudonymisation and encryption techniques, automated deletion of personal data on expiry of retention period and system's capabilities and functionalities to accede to data subjects' rights)?

Did you implement preventive measures to safeguard the personal data and ensure that procedures are in place to detect and report data breaches (e.g. incident response plans) to the supervisory authority within 72 hours from becoming aware of the breach?

Did you provide training and instructions to your staff on how to safeguard the personal data?

Are approved information security policies in place to provide the necessary internal guidelines as part of information security and risk management?

Additional safeguards

Do you follow any approved codes of conduct or international/industry applicable standards?

Processors

Will a processor and/or sub-processor be engaged to process data on your behalf?

If yes, have you carried out the necessary due diligence on the processor/sub-processor to ensure that they provide sufficient guarantees to implement appropriate technical and organisational measures that the processing will meet the requirements of the GDPR?

Is the relationship with the processor/sub-processor governed by means of a contract or other legal act under Union law. Take into account the minimum requirements set out under Article 28(3) GDPR.

Transfer of personal data to third countries or international organisations

Will the personal data be transferred to a third country?

If yes, will the transfer rely on:

- the basis of an adequacy decision;
- appropriate safeguards, including but not limited to, BCRs, standard data protection clauses adopted by the Commission, approved code of conduct and approved certification mechanism;

Authorisation from the supervisory authority shall be required if the transfer will be carried out on the basis of:

- contractual clauses entered into between data exporter and data importer in the third country;
- provisions to be inserted in administrative arrangements between public bodies.

Necessity and proportionality

Are the purposes of the processing operation specific, explicit and legitimate (purpose limitation principle)?

Does the processing actually achieve the intended purpose?

Is there another way to achieve the same outcome in a more privacy friendly manner?

Are the data collected adequate, relevant and limited to what is strictly necessary in relation to the purposes for which the data are processed (data minimisation principle)?

How do you ensure that the data provided are accurate and kept up to date (accuracy principle)?

What are the data retention periods, in particular, where different categories of personal data are processed (storage principle)?

What measures are in place to ensure that the data are deleted once the retention period has expired?

Data subject rights

Are measures in place for the data subjects to exercise their rights (transparency, right of access and to data portability, right to objects and to restrictions of processing, right to rectification and erasure)?

If applicable, how is consent obtained? Ensure that consent is freely-given, specific and informed. Consider opt-in mechanisms in online systems where required. Provide the data subject with an easy manner how to withdraw consent (e.g. opt-out).

Does the new processing allow you to respond to data subject access requests easily?

Risk Assessment (minimum requirements)

Identify the threats and the likelihood that such threats materialise into risks.

Identify all the possible risks.

Establish the number or potential number of affected data subjects by the processing activity.

Identify adverse effects and impact on the data subjects.

Identify mitigations measures appropriate to the risks. Identify residual risks, if any.
Outcome
Comments by the DPO. In the case of residual high risks, do you have a procedure in place to consult the supervisory authority pursuant to the requirements of Article 36 GDPR? Devise an implementation plan of the necessary measures identified in the DPIA and target dates. Approvals, signatures of responsible officers (including the DPO where applicable) and date.