Data Protection Impact Assessment

Project: [name of project]

Assessment undertaken by: [insert name of relevant person]

Date: [Date]

Data Controller: [Name of Entity] _____

(signature)

Data Protection Officer: [insert name of relevant person] _____

(signature)

General Overview	
1.	**What are your reasons for conducting a DPIA?**
2.	**Describe the nature, scope, context and purpose of envisaged processing. Does the project involve new/additional technology which will have a substantial privacy risk (e.g. smart cards, RFID tags, mobile phone locations, applications of GPS, visual surveillance, digital imaging and video recording)? If yes, justify why it is needed.** **(Attach any relevant supporting documentation such as a project proposal, data flow diagrams, images, related systems documentation, etc.).**
3.	**Describe the processing operations related to the envisaged processing.**
4.	**Is the DPO involved in the process?**
5.	**Contact details of DPO**
6.	**Has a previous DPIA been carried out? (Attach any relevant supporting documentation)**

Legal Basis for Processing	
7.	**Identify the proper legal ground(s), on the strength of which, the processing activity will be legitimised.**

Categories of Personal Data Processed	
8.	**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.**

Data Protection Principles	
The First Principle: Lawfulness, Fairness and Transparency	
9.	**Will any decisions affecting individuals be made solely on processing by automatic means (i.e. a computer will make the decision rather than a human being)? If yes, specify how data subject will be notified.**
10.	**Is there a Data Protection Policy in place? If yes, include link or attach document.**
11.	**Is there a Data Protection statement present on application forms/documents related to this process that need to be filled in by the data subject?**
12.	**Are measures in place for the data subjects to exercise their rights (including right of access, right to object, right to restrict processing, right to rectification, and right to erasure)?**
13.	**Does the new processing allow you to respond to data subject requests easily? Are there any restrictions to the rights of the data subjects in relation to this process?**
14.	**Does the project involve the use of an identifier as a reference number? If yes, justify why it is needed.**
15.	**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).**

The Second Principle: Purpose Limitation	
16.	**Are the purposes of the processing operation specific and explicit?**
17.	**Does the processing actually achieve the intended purpose?**
18.	**Will the personal data collected be used for other purposes? If yes, is it compatible with the original purpose?**
19.	**In this project, will you be receiving personal data from other existing processes (e.g. CdB, other Public Authorities)? If yes, will you take note of the sources of such data?**
20.	**Is the purpose for this process related to public safety and security (e.g. CCTV cameras, controlled access to premises, etc.)?**
21.	**Is there another way to achieve the same outcome in a more privacy friendly manner?**

The Third Principle: Data Minimisation	
22.	**Will the data collected be adequate, relevant and limited to what is strictly necessary in relation to the purposes for which the data will be processed?**
23.	**Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database? If Yes, explain why this processing is necessary?**
24.	**Does the project involve new or significantly changed handling of personal data about a large number of individuals? If Yes, explain why this processing is necessary?**

The Fourth Principle: Accuracy	
25.	**How do you ensure that the personal data provided are accurate and kept up to date (e.g. by contacting the data subject)?**

26.	**Will personal data be evaluated to establish the degree of damage that they may cause the data subject and/or data controller if they are inaccurate?**

The Fifth Principle: Storage Limitation	
27.	**Is there a retention policy in place? If yes, include link or attach document.**
28.	**What are the data retention periods, in particular, where different categories of personal data are processed? Will the project include the facility to set retention periods (manual or automated)?**
29.	**What measures are in place to ensure that the personal data are deleted once the retention period has expired?**
30.	**Are there to be any exceptional circumstances for retaining certain data for longer than the normal period? If yes, justify why.**

The Sixth Principle: Integrity and Confidentiality	
31.	**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 (e.g. access to limited personnel, password protected, locked cabinets for manual documents, etc.)?**
32.	**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)?**
33.	**Are there procedures 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?**
34.	**Does the project involve new or significantly changed consolidation, interlinking, cross-referencing or matching of personal data from multiple sources?**
35.	**Will a processor and/or sub-processor be engaged to process data on your behalf?**

36.	**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?**
37.	**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.**
38.	**Will this project involve the disclosure of personal data to third parties? If yes, will a record be kept of the data that are going to be disclosed to third parties?**
39.	**Is disclosure to third parties ruled by any particular policy, procedure, or legal obligation? If yes, is this reflected in the Data Protection policy?**
40.	**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.**
41.	**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.**
42.	**Is there or will there be a higher degree of security with regards to special categories of personal data? If yes, specify how.**
43.	**Is there or will there be a contingency plan in place to manage the effect/s of an unforeseen event, such as human error, computer virus, network failure, theft, fire, flood, or other disaster? If yes, explain how.**

The Seventh Principle: Accountability	
44.	**Did you provide training and instructions to your staff on how to safeguard the personal data?**
45.	**Are approved information security policies in place to provide the necessary internal guidelines as part of information security and risk management?**
46.	**Do you follow any approved codes of conduct or internationally applicable standards?**
47.	**Will you keep formal records of this processing?**

Risk Assessment (minimum requirements)	
48.	**Identify the threats and the likelihood that such threats materialise into risks.**

Possible threat	Risk level	Security Measure

49.	**Identify all the possible risks.**
50.	**Establish the number or potential number of affected data subjects by the processing activity.**
51.	**Identify adverse effects and impact on the data subjects.**
52.	**Identify mitigations measures appropriate to the risks.**

53.	**Identify residual risks, if any.**

Outcome	
54.	**Comments by the DPO**
55.	**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?**
56.	**Devise an implementation plan of the necessary measures identified in the DPIA and target dates.**
57.	**Comments of the Lead Supervisory Authority**
58.	**Any additional actions to take post-notification to the Lead Supervisory Authority**