Step 1: General Information	
1.1 Name of controller/processor	Name.
1.2 Address	Address.
1.3 Telephone Number	Telephone number.
1.4 Name of contact person	Person with whom the Data Protection Office can liaise with for any clarifications on the duly filled DPIA form.
1.5 Is the controller/processor registered with the Data Protection Office?	Registered or not Registered. Note: Registration is a mandatory requirement under section 14 of the DPA.
1.6 Have you designated an officer responsible for data protection compliance issues?	In accordance with section 22(2)(e) of the DPA. Either Yes/No.
1.7 Are you certified ISO/IEC 27701 Privacy Information Management System?	Standard may be purchased at Mauritius Standards Bureau. Either Yes/No.
Step 2: Details of project/envisaged processing	
2.1 Description of project/processing	E.g. This project concerns the setting up of a hospital information system at <*Name of organisation* >.

2.2 Purpose/s of project/processing	Describe what the project/processing aims to achieve. E.g. To implement a new information system to manage all aspects of hospital operations, etc...
2.3 How do you plan to prevent function creep, i.e., preventing the processing of personal data beyond the original context of use?	In accordance with section 21(b) of the DPA. E.g. The purpose/s for processing will be defined and recorded right from the start. The purpose/s will also be specified in the privacy information for individuals.

2.4 Benefit/s of project/processing	Describe the contributions that the project/processing will bring against the existing system/situation. E.g. The benefits of implementing the hospital information system are: 1. Easy and quick access to a patient data 2. Minimise errors 3. Improved traceability and retrieval of patient records4. Enhanced service and patient care 5. Better data security.
2.5 Type/s of processing involved	Please refer to the definition of 'processing' in section 2 of the DPA. E.g. This project involves the following types of processing : (1) Collection of patient data (2) Recording the collected data in a database (3) Storing the data in a local server , etc...

2.6 Reason/s for doing a DPIA	A DPIA is necessary because the project meets the following 3 criteria: 1) Data is processed on a large scale 2) It involves processing data of vulnerable persons (e.g. people with mental illness, asylum seekers or elderly people, patients, etc.) 3) It involves special categories of personal data (physical/mental health and genetic data). Consequently, the processing is considered as high risk to individuals.
2.7 Categories of data subjects whose personal data will be processed	E.g. Patients (citizens, foreigners and employees).

Step 3: Details of processing

Nature of the processing	
3.1 List the types of data which will be processed	E.g. Name, National Identity Card Number, Age, Date of birth, etc..

3.2 (a) Will the processing involve special category/ies of personal data? (b) If yes, (i) List all the special category/ies of personal data that will be involved. (ii) Specify under which condition/s of section 29(1) of the DPA will it/they be processed?	Refer to the definition of special categories of personal data under section 2 of the DPA. Either Yes or No. List the types of special categories of personal data. E.g. Physical or mental health condition, genetic data, etc.. In accordance with section 29 of the DPA. E.g. Special categories of personal data will be processed under section 29(1)(a) of the DPA by satisfying section 28(1)(a).
3.3 (a) Will the processing involve personal data of children below the age of 16 years? (b) If yes, (i) How do you plan to obtain the consent of their parent or guardian? (ii) How do you plan to verify that consent has been given or authorised by the holder of parental responsibility?	Either Yes or No. In accordance with section 30(1) of the DPA. E.g. Consent of parents will be recorded on a form duly signed by the parent. In accordance with section 30(2) of the DPA. E.g. A verification exercise will be carried out by the organisation to cross check consent given by phoning each parent. Note: The above is only an example to facilitate understanding. Other means of verification may be explored.

3.4 What is the source of personal data?	You need to clarify where the data will originate from. E.g. All personal data will be collected directly from individuals.

3.5 In the event that data will be collected directly from individuals, do you plan to inform them of the prescribed list of information defined under section 23(2) of the DPA at the time of collection?	In accordance with section 23 (2) of the DPA. Either Yes/ No/ Not Applicable.
3.6 In the event that data will not be collected directly from individuals, how do you plan to inform them of the prescribed list of information defined under section 23(4) of the DPA?	In accordance with section 23 (4) of the DPA. E.g. The organisation will send letters to each individual to inform him/her of the processing and other details defined under section 23(2) of the DPA. Note: Other means of communication may be explored.
3.7 Describe how data will be collected, used, stored and deleted? (Note: You may use Data Flow Diagrams to illustrate same.)	You must describe the flow of personal data during the processing, i.e., how information enters and leaves the system, what changes the information and where information is stored. E.g. Patients will interact with the hospital information system. Patients will first register themselves by submitting their name, National Identity Card Number, age, date of birth, copy of passport where applicable and details of medical problem encountered. Their records are updated in a patient database, etc....

3.8 In what format/s will personal data be collected and stored?	E.g. hardcopy, digital, database, etc...
3.9 Describe any transfer method (internally and externally) of personal data involved in the processing?	E.g. All transmission of personal data will be done through a secured Virtual Private Network, etc...
3.10 What geographical location/s will be involved during the processing?	E.g. Offices located at <*name of locations* > , <*name of cloud system* > with servers located at <name of locations> , third parties located at <*name of locations* >, etc...

3.11 Who will be accountable for the processing of data?	Can be 1 individual or a group of individuals. Also, accountability may change as personal data flows across an organisation.
3.12 Who will have access to the personal data?	Describe the access rights controls you plan for handling the data.
3.13 List all the stakeholders involved in the processing with their respective roles?	Stakeholders include both internal and external stakeholders. E.g. (a) Employees of <*name of departments* > for managing and implementing the system (b) Patients whose data will be inputted in the system (c) <*Name of supplier* > for provision of server (d) <*Name of external information security consultant* > for consultancy purpose (e) <*Name of processor* > for <*description of service* >, etc...

3.14 (a) Do you plan to use the service ged a processor during the envis processi (b) If so, (i) How will the controller that ensure the processor/s comply the with instructions of the controller? (ii) How do you plan to notify the for processor holding the data destruction of the data when purpose of processing lapses?	Please refer to section 31(4) of the DPA. Either Yes or No. E.g. Will there be a contract in place which provides all the conditions (e.g. continuity of service, backups and integrity, safeguards, confidentiality, clauses to ensure that all personal data are returned to the controller upon termination of contract) for processing of data between the controller and the processor? In accordance with section 27(1)(b) of the DPA. E.g. A notice will be sent to the processor for destruction of the data. The processor will be required to confirm in writing to the controller once the destruction is completed.

3.15 Will the data be shared to any third party? If so, for which purpose/s?	Either Yes or No. E.g. <T*ypes of personal data*> will be shared with <*Name of Organisation*> for <*Purpose* >, etc... For instance, Name, gender, age and blood sample of patients will be shared with Organisation A for laboratory analysis.
3.16 Will the disclosure of personal information be considered lawful under the Data Protection Act or other laws?	In accordance with section 42 of the DPA. Refer to section 28 of the DPA which lists the conditions for lawful processing. Either Yes or No.

3.17 Describe the data security and organisational measures that will be implemented to protect data during the processing?	In accordance with section 31 of the DPA. Note: Organisational measures may include amongst others: a) Provision of data security education to all employees including their confidentiality obligations; b) Clear distribution of responsibilities and a clear outline of competences within the organisation in matters of data processing, especially regarding decisions to process personal data and to transmit data to third parties or to data subjects; c) Clear rules within the organisation on the use of personal data according to the instructions of competent person/s or according to laid down policies; d) Policies covering authorisations to access personal data and protection of access to locations and IT processing equipment; e) Regular checks/audits of the internal rules and policies in place; f) Proper documentation where required to demonstrate lawfulness of processing operations.
3.18 Do you plan any special security measures to prevent any potential data breach? If so, list them.	Either Yes or No. E.g. Yes. 2 factor authentication will be used to verify a user's claimed identity as follows: (i) Input password for login (ii) A One Time Password (OTP) sent to the user's phone to input on the system before using it.

3.19 In case of personal data breach/es, (a) How do you plan to notify the Data Protection Office? (b) How do you plan to communicate the data breach/es to any affected individual/s if it is likely to present high risks to him/her?	In accordance with sections 25 and 26 of the DPA. E.g. The Personal Data Breach Notication Form available on the website of the Data Protection Office (DPO) will be duly filled and submitted to the DPO within a time limit of 72 hours. E.g. The organisation will notify each affected individual in writing using clear language on the nature of the personal data breach and relevant information and recommendations defined under section 25 of the DPA. Note: Other means of communication may be explored.
3.20 Do you plan any audit/monitoring exercise to evaluate the effectiveness of technical and organisational measures for the envisaged processing?	Please refer to section 22(3) of the DPA. Either Yes or No. E.g. Yes. Audits will be done by <*name of department* > to verify <*details of verification* > on a quarterly basis starting <*date* > and the results will be reported to top management. All actions will be documented in a file in a folder found at <*name of location* > and approved by top management.
3.21 Will data be encrypted and /or pseudonymised during the processing?	In accordance with section 31(2)(a)(i). Either Yes or No. If yes, kindly describe how.
3.22 Will there be a disaster recovery plan to restore availability and access to personal data during physical/technical incidents?	In accordance with section 31(2)(a)(iii). Either Yes or No.
3.23 Any other information regarding the nature of processing?	Any other relevant information.

Scope of the processing	
3.24 How many individuals' data will be processed?	E.g. Approximately 100,000 individuals.

3.25 What are the boundaries of the envisaged processing?	E.g. Can be a geographical area or a specific group of people such as elderly people, etc...
3.26 How often will the processing be carried out?	E.g. Processing will be carried out on a daily basis.
3.27 How long do you plan to keep the data?	E.g. 10 years. Note: The Data Protection Act does not provide time limits for keeping personal data. This has to be determined by the controller/processor based on the purpose of the processing and taking into account other laws in Mauritius which provide time limits for keeping records.
3.28 Do you plan to delete or anonymise data as soon as the purpose of processing lapses?	In accordance with section 21(e) of the DPA. Either Yes or No.

3.29 (a) Will there be any transfer of personal data abroad? (b) If yes, list the countries? (c) How do you plan to seek authorisation from the Data Protection Office for data transfers abroad in the event where you cannot provide proof of appropriate safeguards with respect to the protection of the personal data, or cannot rely on any of the exceptions provided in section 36(1) of the DPA?	Either Yes or No. If the answer is Yes, then list the names of countries where there will be data transfer abroad. E.g. Ireland, France, etc... In accordance with section 35(1) of the DPA. E.g. The Transfer of Personal Data Form available on the website of the Data Protection Office will be duly filled and submitted.
3.30 Any other information regarding the scope of processing?	Any other relevant information.
Context of the processing	

3.31 What procedures do you plan to have in place to handle requests from individuals regarding their rights to: (a) Access their data? (b) Have their data rectified in case the data processed is inaccurate? (c) Erase their data as appropriate under section 39(2) of the DPA? (d) Temporarily restrict processing of their data as appropriate? (e) Object to processing of their data as appropriate? (f) Not be subject to decisions based solely on automated processing, including profiling, that have legal effects or that significantly affect them?	In accordance with Part 7 of the DPA. (a) E.g. The Rights of Data Subjects form on the website of the Data Protection Office will be made available to individuals at the reception desk and on the website of the organisation. Our privacy policy will also mention the procedures to handle access requests forms. A special unit <*name of unit*> will be responsible for recording and managing the requests.
3.32 How do you plan to inform individuals about their rights on the envisaged processing?	E.g. An information notice will be available on the organisation's website and reception counter which details the rights of individuals for processing their data.

3.33 How far do you consider yourself meeting the expectations of individuals that their personal data will be processed in this manner?	E.g. Given that all processing will be carried out in a transparent and fair manner through : (i) Information notices available at the reception desk and website of the organisation, (ii) ..... etc, the organisation believes that it is meeting the expectations of individuals.
3.34 If the processing entail potential risks to individuals, how do you plan to inform the latter to avoid any unforeseeable negative effects on them?	In accordance with section 21(a) of the DPA on fair processing. E.g Letters will be sent to inform individuals about the risks involved and they will be requested to contact the organisation for any further concern/action. Note: Other means of communication may be explored.
3.35 What is the current state of technological development/s available for the envisaged processing?	Research to be based on the type of processing involved.
3.36 Is there any preceding concern/s or apprehension/s with respect to this type of processing?	Research to be based on the type of processing involved.
3.37 Is there any data protection issue/s which may affect the public regarding the envisaged processing?	Research to be based on the type of processing involved.

3.38 How do you intend to seek the views of data subjects on the intended processing? Please provide your justifications.	In accordance with section 34 (4) of the DPA. Either Yes or No, with supporting justifications in either case. E.g. A public consultation on the project will be done to address the views of individuals.
3.39 Are employees trained for the envisaged processing?	Either Yes/No/any planned training. E.g. Currently, our staff are not trained and do not have the expertise for the nature of processing involved. However, we have included training of staff as one mandatory requirement when contracting out the tender with the supplier to ensure that our staff are adequately trained prior to going live with the system.

3.40 How do you plan to include the envisaged processing in your record of processing operations carried out by the organisation?	In accordance with section 33 of the DPA. E.g. The Data Protection Officer in the organisation will be responsible to update the record of processing operations kept.
3.41 Any other information regarding the context of processing?	Any other relevant information.

Step 4: Necessity and proportionality of processing

4.1 What is/are your legitimate interest/s for the processing?	Describe the reasonable interests of the controller/processor for the processing?
4.2 What is/are the lawful ground/s for the processing?	List the lawful grounds for the envisaged processing with reference to section 28 of the DPA?

4.3 In the event that you will rely on consent of individuals as your lawful ground to process their data, (a) Will the consent be considered valid, i.e., freely given, specific, informed and unambiguous?	(a) In accordance with the definition of consent in section 2 of the DPA. Either Yes or No. (Freely given: Provide genuine choice; Specific: Concise on the processing operation and purpose/s; Informed: Provide clear information and in plain language , at minimum containing the controller's identity, the purpose/s of the processing, the processing activities, the right to withdraw consent at any time. Amount of information depends on circumstances and context of a case; Unambiguous : To avoid implied form of actions by the data subject such as pre-ticked opt-in boxes.)
(b) How will you keep proof of consent?	(b) In accordance with section 24(1) of the DPA.
(c) What procedures will you keep to handle withdrawal of consent of individuals?	(c) In accordance with section 24(2) of the DPA.
(d) How will you verify that the consent requested is necessary and directly related to the performance of a contract or service related to the project/processing?	(d) In accordance with section 24(3) of the DPA.
4.4 How is the processing demonstrably necessary to meet the specific need/s?	Describe what specific problem has to be solved, and whether the envisaged processing is essential for satisfying the need?

4.5 How is the processing likely to be effective in meeting that need?	Will the envisaged processing actually bring the intended results?
4.6 Are there alternative means for achieving the same outcome?	List whether there are different options to achieve the same result?

4.7 How will you ensure that data collected or processed is adequate, relevant and not excessive?	In accordance with section 21(c) of the DPA. E.g. The organisation will carry out a self testing exercise to ensure that (a) personal information that will be processed is really necessary for the business, (b) people are being asked to provide with just the information the organisation needs, and no more, (c) there is a good reason for asking people sensitive or personal questions.
4.8 How will you ensure that data is accurate and up to date during the processing?	In accordance with section 21(d) of the DPA. E.g. Regular audits will be carried out at <frequency> to ensure data accuracy, etc...
4.9 How will confidentiality, integrity, availability and resilience of data be ensured during the processing?	In accordance with section 31(2)(ii) of the DPA. E.g. Access controls, audit logs, etc...
4.10 Will any loss of privacy be proportionate to the benefit/s gained?	Describe whether the resulting loss of privacy would be proportional to any anticipated benefit. Note: If the benefit is relatively minor, such as a slight increase in convenience or a slight cost saving, then the loss of privacy may not be appropriate.

4.11 How do you plan to provide any additional measures to support the rights of individuals during the processing?	E.g. Yes. A complaints' handling mechanism will be set up to address complaints from the public for the envisaged processing, etc...

Step 5: Risk Assessment (See further guidance at end of document)

Description /Nature of Risks	List the risks to the rights and freedoms of data subjects which may result in physical, tangible or intangible damage/harm to data subjects such as discrimination, loss of confidentiality, availability or integrity of data, etc… E.**g.:** 1. Interception of data during transmission 2. Physical access to patient data stored in server 3. Failure of backup leading to permanent loss.
Likelihood of damage/ harm	Probability of risk occurring. Evaluation has to be done by the controller/processor. May be classified on a scale 'Frequent' ,'Occasional' or 'Unlikely'. You may adapt the scale in your context of operation with a brief legend explaining each representation of the scale.
Severity of damage/ harm	Determine the significance of the risk in terms of degree or amount of damage/harm. Evaluation has to be done by the controller/processor. May be classified on a scale 'Critical', 'Moderate' or 'Insignificant'. You may adapt the scale in your context of operation with a brief legend explaining each representation of the scale.

Overall Risks	Taking into consideration both the likelihood and severity of the risk, you need to assess whether the overall risk is low/ medium/ high in your context of operations.

Step 6: Measures to mitigate risks (See further guidance at end of document)

Measures to mitigate risks	Describe the technical and organisational measures to protect against the risks.
Effect of Measures on risks	Will the risks be eliminated or reduced after applying the envisaged measures?
Residual Effect	Evaluate the remaining significance of the risk in terms of 'high', 'medium' and 'low' after mitigations are applied.

Step 7: Documentation

DPIA carried out by	Details of the controller's or processor's officer/s who carried out the DPIA.

DPIA reviewed by	Details of the controller's or processor's officer/s who reviewed the DPIA.
DPIA approved by	Details of the controller's or processor's officer/s who approved the DPIA.
Submission of a copy of DPIA to Data Protection Office	Details of the controller's or processor's officer/s who submitted the DPIA to the Data Protection Office.

Further guidance on steps 5 and 6

1. The risk matrix is a simple tool to help organisations understand and explain the level of privacy risk arising from personal data processing activities.
   Step 1: Identify the Risk
   Begin by clearly stating the privacy risk. This should describe what could go wrong, for example, unauthorised access to personal data.

   Step 2: Assess the Likelihood
   Decide how likely it is that the risk could occur:

   - Frequent: The event is expected to occur regularly.
   - Occasional: The event is possible but not frequent.
   - Unlikely: The event is rare or improbable.

   Step 3: Assess the Severity (Impact)
   Consider how serious the impact would be on data subjects if the risk occurred:

   - Critical: Causes significant impact (e.g., severe financial, operational or reputational damage).
   - Moderate: Causes noticeable but manageable impact.
   - Insignificant: Minimal or negligible impact.

   Step 4: Determine the Overall Risk Level
   Using the risk matrix, combine the likelihood and severity to determine the overall risk:

Likelihood \ Severity	Critical	Moderate	Insignificant
Frequent	**High**	**High**	**Medium**
Occasional	**High**	**Medium**	Low
Unlikely	**Medium**	Low	Low

   - High: Requires immediate action or control.
   - Medium: Needs monitoring and mitigation.
   - Low: Acceptable with minimal or no additional action required.

Example:

Risk No.	Description /Nature of Risks	Likelihood of damage/ harm (Frequent/ Occasional/ Unlikely)	Severity of damage/ harm (Critical/ Moderate/ Insignificant)	Overall Risks (High/ Medium/Low)
1.0	Unauthorised access to personal data	Occasional	Critical	High

Step 5: Describe Existing and Planned Controls
For overall risks classified as "High" or "Medium", briefly explain what measures are in place and whether additional measures are planned to reduce the risk.

Example:

Risk No.	Measures to mitigate risks	Effect of Measures on risks (Eliminated/Reduced)	Residual Effect (High/Medium/Low)
1.0 (Unauthorised access to personal data)	Access rights management implemented. Regular review of logs to detect any unauthorized access. Internal audit checks. ISO 27001 certified with third party audit yearly.	Reduced	Low

Step 6: Review Residual Risk

After considering the controls, reassess whether the risk remains high, medium or low.