DATA PROTECTION OFFICE

Application for Certification Form

Particulars of controller/processor

Name of controller/processor: _____

Please tick whether application is by controller/processor

Name of controller: _____

Please specify name of controller if application is being done by processor

Address: _____

Is the controller/processor registered with the Data Protection Office? _____

Telephone number: _____ Fax number: _____

Email _____

Name of contact person (Mr./Ms./Mrs): _____

Designation of contact person: _____

Telephone number of contact person: _____

Email address of contact person: _____

Date: _____ Signature: _____

OFFICE USE ONLY

Last Certification Date: _____

Forthcoming Audit Date: _____

Auditors: _____

Are all criteria for Certification met?: Yes|No

Can Certfication be granted?: Yes|No

Approval by DPC: _____

Approval Date: _____

Data Protection Certification Asessment

Instructions to controller/processor:

- Please provide clear, factual and accurate answers to the questions in the Data Protection Certification Assessment.
- Please tick Yes, No or N/A as appropriate.
- If the answer is Yes, please attach additional details and evidence as annexure.
- If the answer is No or N/A, please attach the reasons and justifications as annexure.
- Please use the Annexure to provide additional details and evidences.
    - Each question should be labelled as per the Question No. in the document.
    - For e.g Annex for Question 5 should be labelled as Annex 5.
    - Please use the formatting as it is in the document and update the table of content accordingly.
- Please attach a printed copy of the filled Data Protection Certification Assessment Questionnaire and the evidence upon submission of the application for Certification.
- A copy of the filled Data Protection Certification Assessment Questionnaire should be emailed to **dpo@govmu.org** and the email should be titled as "Data Protection Certification Assessment."

	YES	NO	N/A
Registration and Renewal (Sections 17 & 18)			
1. How do you ensure that a change in any of the particulars referred to in your application form for registration as controller /processor is communicated to the Data Protection Office?			
2. Is your registration as controller/processor up to date?			
Lawfulness, fairness and transparency (Section 21a)			
3. Has(ve) the data subject(s) been informed of the processing? *Please annex evidence.*			
4. Has(ve) the data subject(s) been informed of the people or organisations their data may be passed onto? *Please annex evidence.*			
Conditions for consent (Section 24)			
5. Has(ve) the data subject(s) given his/her/their consent to the processing? *Please annex evidence.*			
6. How does the consent (as expressed by the data subject(s)) meet the legal requirements on consent? *Please annex evidence.*			
a. Is the consent freely given, specific, informed and unambiguous, by setting out the purpose of the various phases of the processing?			
b. Is consent easy to withdraw at any time?			
c. Is consent verifiable? Please supply evidence that consent has been obtained as <Annexure>.			
d. Has it been obtained under some form of duress / an offer of advantage/threat of disadvantage?			
7. If the data subject(s) has(ve) not given his/her/their consent, is the processing justified on the basis of necessity (as per Section 28(b))? *Please justify if it is applicable.*			

Purpose limitation (Section21b)			
8. Please provide the lawful grounds for processing.			
9. If applicable, have you informed individuals of any possible 'non-obvious' uses during the processing of their personal information? *Please annex the details.*			
10. Are there procedures in place for maintaining a comprehensive and up-to-date record of the various use/s of personal data? *Please annex the procedures.*			
11. How often is this record checked? *Please annex evidence.*			
12. Does the record include all equipment which can process personal data and data held in relevant filing systems? *Please attach sample records.*			
13. Does the record cover processing carried out on your behalf (e.g. by Mauritius Revenue Authority or Bank)?			
Data minimization (Section21c)			
14. Is each item of personal data limited to what is necessary for the specified purpose(s) for which it is collected? *Please annex evidence.*			
15. Has it been verified that the same outcome could not be achieved, safely and effectively, with less personal data? *Please annex evidence.*			
16. Where personal information is collected, is there any indication given to indicate which information is voluntary or mandatory? *Please annex evidence.*			
17. What are the procedures in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed? How often are these procedures reviewed? *Please annex the procedures.*			

Accuracy (Section 21d)			
18. Does your organisation have defined procedures to ensure accuracy of data? *Please annex the steps.*			
19. Are personal data checked for accuracy? *Please specify on what interval checks are done and give examples.*			
20. Are personal data duplicated and held separately at different locations by different departments for backup or other purposes? *Please annex the details.*			
21. If yes, describe how updates or amendments are communicated to all parties with copies of the personal data?			
22. How are inaccuracies of personal data dealt with?			
Storage limitation (Section21e)			
23. Has a retention period and policy been implemented and adhered to in practice?			
24. If yes, please specify the retention period and describe the criteria for determining the retention period of personal data?			
25. How often are these criteria reviewed?			
26. Are there any statutory requirements on retention? *Please give examples.*			
Duty to destroy personal data (Section 27)			
27. When it is no longer necessary to retain personal data which was collected for a particular purpose, is the personal data deleted, retained in an archive or retained in an anonymised format (e.g. if kept only for historical or statistical purposes)? *Please specify how and when is the personal data deleted or destroyed?*			
28. If personal data is held by a processor, is the latter notified about the request to destroy it? *Please specify the procedures.*			

Duties of controller (Section 22)			
29. Are there proper policies regarding implementation of technical and organisational measures in place? *Please annex details.*			
30. Is there a detailed written documentation of processing operations? *Please annex the documentation.*			
31. Is data protection impact assessment/s performed, if applicable? *Please annex the results.*			
32. Has a Data Protection Officer been appointed in line with DPA 2017 to ensure compliance? *Please specify the details.*			
33. On what frequency(ies) are audits conducted in which compliance with the relevant policies, technical and organisational measures and controller's obligations are checked? *Please provide evidence.*			
Collection of personal data (Section 23)			
34. Are personal data collected directly from the data subjects? *Please provide appropriate evidence.*			
a. If personal data are obtained indirectly, please specify the sources from where they are obtained.			
b. If personal data are obtained indirectly, are the sources recorded?			
c. If personal data are obtained indirectly, are the data subjects informed about the collection?			

35. Is the data subject informed as required by DPA 2017 of the following: *Please provide appropriate evidence.*			
a. the identity and contact details of controller, its representative or any nominated data protection officer where one has been appointed			
b. the purpose(s) for which the data are intended to be processed			
c. the intended recipients of the data			
d. whether or not the supply of the data by that data subject is voluntary or mandatory			
e. the existence of the right to withdraw consent			
f. the existence of the right to request from the controller access to and rectification, restriction or erasure of personal data and to object to the processing			
g. the existence of automated decision making, including profiling			
h. the period for which the personal data will be stored			
i. the right to lodge a complaint			
j. the intention to transfer personal data to another country			
k. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair			
Conditions for consent (Section 24) *Applicable where the lawful ground for processing is consent.*			
36. Has the data subject given his/her consent to the processing? *Please annex evidence.*			
37. How does the consent (as expressed by the data subject) meet the legal requirements of consent? *Please annex evidence.*			
a. Is consent freely given, specific, informed and unambiguous, by setting out the purpose of the various phases of the processing?			
b. Is consent easy to withdraw at any time?			
c. Is consent verifiable? Please supply evidence that consent has been obtained in Annexure.			
d. Has it been obtained under some form of duress / an offer of advantage / threat of disadvantage?			
38. If the data subject has not given his/her consent, please provide the lawful basis for processing. *Please justify if it is applicable.*			

Special categories of personal data (Section 29)			
39. If data collection includes special categories of personal data, has the data subject given his/her consent to process such data? *Please annex evidence.*			
Otherwise, please specify on which grounds you have relied on as providing a legal basis for processing such data (as per Section 28(b) or 29(b) in Annexure?			
Personal data of children (Section 30)			
40. If data collection includes the personal data of a child below the age of 16 years, has consent been obtained by the child's parent or guardian? *Please annex evidence.*			
41. Has reasonable effort been made to verify that consent has been given or authorised, taking into account available technology? *Please annex evidence.*			
Security of Processing (Section 31)			
42. Are there security measures in place (for e.g authentication/encryption mechanisms) with regard to the access, storage and transit of personal data on removable media, if applicable? *Please annex the measures.*			
43. Are there measures in place for the administration of access rights to personal data? *Please annex the measures.*			
44. Are there countermeasures in place to prevent users from manipulating data? *Please annex the measures.*			
45. Are you/your organisation using best practices for password management? *Please annex the mechanisms.*			
46. Is a written security policy available? *Please annex policy.*			
47. Are the security objectives effectively pursued by management? *Please describe and annex evidence.*			
48. Are data protection/data security measures being monitored on a regular basis? *Please annex more details.*			
49. Is the erasure of personal data performed in such a manner that they cannot be recovered anymore? *Please annex evidence to illustrate the reliability and effectiveness of the methods.*			
50. Is the process of physical destruction (e.g., for getting rid of paper, media, CD-ROM, chip cards, tokens) regarded as reliable? *Please illustrate the reliability and effectiveness of the methods.*			

51. Are there measures to ensure that no personal data remain if third party equipment is returned or repossessed? (e.g., leased copying machines and their built-in hard disks) *Please annex the measures.*			
52. Are there steps undertaken to remove or sanitize parts of hardware before disposal or withdrawing from service (e.g., removal of hard disks from computers, flash memory from routers, etc.)? *Please annex more details.*			
53. Are personal data automatically anonymised or pseudonymised? *Please annex details.*			
54. Are pseudonymous data secured against too-easy re-identification? *Please annex details.*			
55. Are there measures taken to avoid the unnecessary creation of temporary shadow files (e.g., through unnecessary logging)? *Please annex the measures and provide more details on how well the temporary shadow files are protected against unauthorised access.*			
56. Are measures taken to filter out personal data that are not needed by the recipients when data are passed on to other controllers (or processors)? *Please annex the measures.*			
57. Are there measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services? *Please annex the measures.*			
58. Are there measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident? *Please annex the measures.*			
59. Are there processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing? *Please annex the processes.*			
60. Have the following points been taken into consideration in determining the appropriate security measures whenever the processing involves the transmission of data over an information and communication network:			
a. the state of technological development available;			
b. the cost of implementing any of the security measures;			
c. the special risks that exist in the processing of the data; and			
d. the nature of the data being processed.			

61. Where a controller is using the services of a processor,			
a. Has the processor provided sufficient guarantees in respect of security and organisational measures for the purpose of complying with subsection 31(1)? *Please annex more details.*			
b. Has the controller and the processor entered into a written contract which provides that:-			
(i) the processor will act only on instructions received from the controller and that			
(ii) the processor will be bound by obligations devolving on the controller under subsection 31(1) *Please annex evidence.*			
62. As a processor, is there personal data being processed by you other than as instructed by the controller? *If yes, please annex evidence of registration with DPO as a controller, if applicable.*			
Record of processing operations (Section 33)			
63. Are records of all processing operations maintained? *Please annex evidence.*			
64. Do the records include: *Please annex evidence of the below*			
a. the name and contact details of the controller or processor, and, where applicable, his or its representative and any data protection officer			
b. the purpose(s) of the processing			
c. a description of the categories of data subjects and of personal data;			
d. a description of the categories of recipients to whom personal data have been or will be disclosed, including recipients in other countries;			
e. any transfers of data to another country, and, in the case of a transfer referred to in section 36, the suitable safeguards;			
f. where possible, the envisaged time limits for the erasure of the different categories of data; and			
g. the description of policies and mechanisms to ensure verification of the effectiveness of the measures regarding the duties of the controller as referred to in section 22(3).			

65. How often is this record checked? *Please annex evidence.*			
Does the record cover processing carried out by other entities (e.g. by Mauritius Revenue Authority/Bank)?			
Data Protection Impact Assessment (Section 34)			
66. Has a Data Protection Impact Assessment been done for high risks operations? *Please attach the Data Protection Impact Assessment.*			
67. Is a written Risk Analysis available? *Please annex document.*			
68. Does the Data Protection Impact Assessment include the following points:			
• a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest(s) pursued by the controller or processor			
• an assessment of the necessity and proportionality of the processing operations in relation to the purposes			
• an assessment of the risks to the rights and freedoms of data subjects			
• the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with DPA 2017, taking into account the rights and legitimate interests of data subjects and other persons concerned.			
69. Does the documentation provide information on the nature of the data that are being processed, allowing a sufficiently clear classification of data to allow adoption of the appropriate security measures to be taken by the user? *Please annex evidence.*			
Prior authorisation and consultation (Section 35)			
70. Has authorisation been sought from this Office prior to processing the personal data in order to ensure compliance of the intended processing with DPA 2017 and in particular to mitigate the risks involved for the data subjects where a controller or processor cannot provide for the appropriate safeguards referred to in section 36 in relation to the transfer of personal data to another country? *Please attach evidence.*			

Transfer of personal data outside Mauritius (Section 36)			
71. Has the purpose(s) for the transfer of data outside Mauritius been described? *Please attach evidence.*			
72. Is the transfer necessary for the performance of a contract between the data subject and the controller?			
73. Are there appropriate safeguards with respect to the protection of the personal data? *Please attach proof.*			
74. Does the transfer involve the entirety of the personal data or entire categories of the personal data contained in the register? *Please show proof.*			
75. Demonstrate the effectiveness of the safeguards to protect the rights and fundamental freedoms of data subjects.			
Right of access (Section 37)			
76. Following a request for access from the data subject, do you provide confirmation to the data subject as to whether or not his or her personal data are being processed? *Please annex evidence.*			
77. Following a request for access from the data subject, is a copy of the personal data forwarded to him/her within one month and free of charge? *Please provide justification for the cases where reply has not been sent within 1 month.*			
78. Are the following information also provided to the data subject?:- • *the purpose(s) ofprocessing;* • *the categories of personal data concerned;* • *the recipients or categories of recipient to whom the personal data are disclosed;* • *the retention period for storing the personal data or, where this is not possible, criteria for determining how long it is stored;* • *the existence of the right to request rectification, erasure or restriction or to object to such processing;* • *the right to lodge a complaint with the DPO;* • *information about the source of the data, where it was not obtained directly from the individual;* • *the existence of automated decision-making (including profiling); and* • *the safeguards provided if the personal data is transferred to another country.*			

79. Do you inform the data subject in writing of the reasons for any refusal and on the possibility of lodging a complaint with the Commissioner within 1 month? *Please elaborate on the process.*			
Automated individual decision making (Section 38)			
80. Is an individual subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or significantly affects him/her?			
81. If yes, does the decision meet any of the following conditions?			
a. necessary for entering into, or performance of, a contract between the data subject and the controller;			
b. authorized by law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or			
c. based on the data subject's explicit consent.			
82. If yes, has the existence of processing for a decision of the kind and the envisaged effects of such processing on the data subject been specified at the time of collection of personal data? *Please attach evidence.*			
83. If 81 (a) or (c) applies, have appropriate measures been implemented to safeguard the data subject's rights, freedoms and legitimate interests during the automated processing? *Please elaborate on the measures.*			
84. Is any automated processing of personal data intended to evaluate certain personal aspects relating to a data subject based on special categories of personal data?			
Rectification, erasure or restriction of processing (Section 39)			
85. Are there appropriate functionalities and/or processes in place which allow for the rectification, erasure and restriction of processing of personal data? *Please elaborate on the functionalities and processes.*			
86. Do these functionalities and/or processes ensure that inaccurate data are rectified/requested personal data are erased/processing is restricted without undue delay?			
87. What are the time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data?			
88. Do you confirm the identity of the data subject requesting rectification, erasure or restriction of processing? *Please elaborate on the process.*			

89. Does the provider of the service inform the data subjects about the action taken on a request for rectification, erasure or restriction of processing/ the reasons for not taking action without undue delay? *Please elaborate on the process.*			
90. Are all recipients of the personal data informed of the rectification, erasure or restriction of processing? *Please elaborate on how they are informed and whether it depends on certain criteria. Please specify the criteria as well (like time or purpose)?*			
91. Do the functionalities and/or processes ensure that personal data are erased provided that:-			
a. the data are no longer necessary in relation to the purpose/s for which they were collected or otherwise processed?			
b. the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing?			
c. the data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing?			
d. the personal data have been unlawfully processed?			
92. If data are to be destroyed or erased? *Please elaborate on the process and how are unintentional copies avoided.*			
93. Can personal data be selectively erased (e.g., parts of data records that are not needed anymore?			
94. How is erasure affected in respect of backup data?			
95. Do the functionalities and/or processes ensure that processing is restricted when:-			
a. the accuracy of the personal data is contested by the data subject			
b. you no longer need the personal data, but they are required by the data subject for the establishment, exercise or defence of legal claims			
c. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead			
d. the data subject has objected to the processing pending the verification whether your legitimate grounds override those of the data subject			
96. By what technical means are the restriction of the processing ensured (e.g., are the personal data concerned made unavailable for users / secured in a way that they cannot be changed)? How?			
97. Is the fact that the processing of personal data is restricted clearly indicated in the system? E.g., can data be marked (flagged) in such a way as to prevent their use for ordinary processing, while keeping them in the database? *Please elaborate on how this is done?*			

98. How is such restriction of processing logged (date and time, the person responsible for ordering the blocking, etc.)?			
Right to object (Section 40)			
99. Are appropriate functionalities and/or processes in place which allows data subjects to exercise their right to object at any time free of charge? *Please elaborate.*			
100. Do these functionalities and/or processes ensure that the personal data concerned are no longer processed for the said purposes in the event of a reasonable objection of a data subject?			
101. What is the time limit to acquiesce to the objection of the data subject?			
102. Do you inform the data subject about the action taken on an objection request / the reasons for not taking action?			
ISO - IEC - 27701 2019			
103. Is your organisation certified ISO - IEC - 27701 2019? (Privacy Information Management System (PIMS))			
Training			
104. Are the employees made aware of the relevant security measures? *Please annex evidence.*			
105. Is it being ensured that employees are complying with the relevant security measures? *Please annex measures.*			
106. How is the instruction/training carried out: Written material? E-Learning? Presentation? Practical exercises? *Please give details.*			
107. Are the time and attendance of such instruction/training recorded? *Please show evidence of last training.*			
108. Are the duties and undertakings to abide by them formally recorded, in writing? *Please give evidence.*			
109. Is a breach of these duties and undertakings a disciplinary matter and made clear? *Please give details.*			

OFFENCES AND PENALTIES

Offences	Penalties
Section 6: Investigation of Complaints	
Any person who fails to attend a hearing or to produce a document or other material when required to do so.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 7: Power to require information	
Any person who fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 9: Enforcement notice	
Any person who fails or refuses to comply with an enforcement notice of the Commissioner	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 12: Obstruction of Commissioner or authorised officer	
Any person who obstructs or impedes the Commissioner or an authorised officer in the exercise of the power of entry and search or fails to provide assistance or information requested by the Commissioner or authorised officer or refuses to allow the Commissioner or an authorised officer to enter any premises or to take any	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 15: Application for registration	
Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.
Section 17: Change in particulars	
Any controller or processor who fails to notify a change in particulars	Liable to a fine not exceeding 50, 000 rupees.
Section 28: Lawful processing	
Any person who processes personal data unlawfully	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.
Section 29: Special categories of personal data	
Any person who processes special categories of data unlawfully	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

Offences	Penalties
Section 43: Offence for which no specific penalty provided	
Any person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act	Liable to a fine not exceeding 200, 000 rupees and to imprisonment for a term not exceeding 5 years. A Court may also order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence or order or prohibit the doing of any act to stop a continuing contravention.
Section 49: Confidentiality and oath	
Any person who, without lawful excuse divulge any confidential information obtained in the exercise of a power or in the performance of a duty under this Act	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years. Protection from liability also applies.