DATA PROTECTION COMPLIANCE AUDIT FORM		
Form No: QMS14	**Revision No: 01**	**Date of Issue: 20.04.2022**
Title: DATA PROTECTION COMPLIANCE AUDIT FORM		**Ref:**

1. Introduction

The purpose of a data protection compliance audit is to obtain a complete picture, as far as possible, of the structure of personal information flows within an organisation so that the appropriate compliance procedures are in place in accordance with the Data Protection Act and best practices.

For large-scale and complex organisations, the first stage is to obtain an organisational chart showing the operational, managerial and departmental structure of the organisation.

2. General Information

Name of Controller or Processor:
Address:
Telephone Number:
Name of Data Protection Officer:

	Audit Question	*Yes*	*No*	*N/A*	*Description of measures and mechanisms in place to protect personal data*
Collection	***1. Does your organisation process personal data?***				
	2. Are personal data collected for explicit, specified and legitimate purpose(s)?				
	3. Are personal data collected in paper format?				
	4. Are personal data collected digitally?				
	5. Are personal data collected directly from individuals themselves?				
	6. Are personal data collected indirectly from third parties, intermediaries, financial advisers, joint venture partners, etc?				
	7. Is a form of data protection notice given to individuals when personal data is collected as per section 23(2) of the DPA?				

	8. Is the data protection notice(s) concise using clear language(s)?				
	9. Is the data protection notice(s) reviewed?				
	10. Is there someone responsible to review the data protection notice(s)?				
Consent	***11. Do you rely on consent for any processing of personal data?***				
	12. Do you ensure that consent is freely given, specific, informed and unambiguous?				
	13. Do you provide individuals with the option to withdraw consent at any time where the lawful ground of processing is based on consent?				
	14. When processing a child's (below age of 16 years) personal data, do you ensure that you obtain authorisation of the child's parent or guardian?				

	15. Do you keep evidence to demonstrate consent?				
Accountability and governance	***16. Have you designated a data protection officer for managing data protection compliance issues?***				
	17. Are the roles and responsibilities of the data protection officer clearly defined in the organisation?				
	18. Do you have a data protection policy in place?				
	19. Are all staffs aware of the data protection policy?				
	20. Do individuals (e.g. staff) who process personal data understand their data protection obligations associated with that processing?				
	21. Do you keep a record of processing operations?				
	22. Have you identified all repositories of personal data in the organisation (e.g.				

	employee/customer/ supplier databases)?				
Storage, Processing and Disclosure	***23. Is personal information stored in physical files in the organisation?***				
	24. Is information stored digitally in the organisation?				
	25. Is information stored digitally by third parties?				
	26. Do you process personal data lawfully, fairly and transparently?				
	27. Are any of your processing activities carried out by third parties?				
	28. Is there any officer(s) in the organisation who is responsible for all processing activities carried out?				
	29. Are there defined roles and responsibilities to view, change, add or delete data?				

	30. Are there well-defined access control rights to personal data within the organisation?				
Storage, Processing and Disclosure	***31. Is there someone who authorises such access?***				
	32. Does your organisation hold any special categories of personal data?				
	33. Do you process special categories of personal data lawfully as per section 29 of the DPA?				
	34. Do you disclose personal data to recipients outside the organisation?				
Rights of Data Subjects	***35. Are there procedures in place for handling rights of data subjects to their personal data?***				
	36. Are those procedures readily available within the organisation?				
	37. Are those procedures readily available to data subjects?				

	38. Are data subjects aware where to address their request for access, rectification, objection or erasure of their personal data?				
	39. Is there any officer(s) who authorises requests pertaining to rights of data subjects?				
	40. Do you process personal data for direct marketing purpose(s)?				
	41. If your answer to question 40 is 'yes', do you have procedures in place to ensure that personal data is no longer processed for direct marketing when a data subject objects?				
Data Quality	***42. Is there officer(s) in the organisation who is responsible for reviewing personal data for relevance, accuracy and keeping personal data up to date?***				

	43. Are these reviews carried out often?				
Security of processing	***44. Are there appropriate security and organisational measures to keep all information secure?***				
	45. Is access to personal data repositories controlled?				
	46. Do you have an audit log of activities performed on these personal data repositories?				
	47. If there are contracts, associated with the processing of personal data, which allow third parties access to personal data, for example data processors, do these contracts specify data protection requirements?				
	48. Do security controls or procedures include measures to ensure pseudonymisation and encryption of personal data?				

	49. Do security controls or procedures include measures to the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services?				
	50. Do security controls or procedures include measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident?				
	51. Do security controls or procedures include a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures?				

Data Breach and DPIA	***52. Do you carry out DPIA for high risks processing operations?***				
	53. If Answer is Yes above, have you filled the DPIA Questionnaire?				
	54. When there is a personal data breach, do you notify the Data Protection Office using the available form?				
	55. If you are a processor, do you notify the controller without undue delay after becoming aware of a data breach?				
	56. When there is a personal data breach, do you notify affected data subjects when there are high risks to their rights and freedoms?				
	57. Do you implement procedures to prevent the re-occurrence of personal data breaches?				

Data Transfer	***58. Is personal data transferred outside Mauritius?***				
	59. Are you aware of the country(ies) the data is transferred to?				
	60. Do you ensure that all transfers of personal data outside Mauritius are lawful in accordance with section 36 of the DPA?				
	61. Have you filled the Transfer of personal data form if you rely on section 36(1)(a) for the transfer?				
	62. Do you use Standard Contractual Clauses or Binding Corporate rules to ensure that appropriate safeguards are applied when transferring/receiving data to/from parties abroad?				
Destruction	***63. Have you defined the retention period for personal data processed in the organisation?***				
	64. Is there any officer(s) who authorises the				

	destruction of personal data?				
	65. Is there a specific location where personal information is archived?				
	66. Do you use a specific format or medium to store archived information?				
Training	***67. Does the organisation train its employees on data protection law?***				
	68. Do you assess the effectiveness of the training provided?				
Future Business Requirements	***69. Do you foresee in the next twelve months a change in any of the answers you have given?***				