#### [TO BE PLACED ON CLIENT’S LETTERHEAD]

To: [NAME OF ACCOUNTANT]

##### [SAIBA DESIGNATION AND MEMBERSHIP NUMBER] [NAME OF MEMBER’S FIRM]

##### [ADDRESS OF FIRM [DATE]

Dear Sirs,

#### ENGAGEMENT ON POPIA COMPLIANCE CHECKLIST

This representation letter is provided in connection with your engagement to declare the compliance status of [**NAME OF CLIENT]** (“the Company”) with the Protection of Personal Information Act, 3 of 2013 (“POPIA”), by way of the completion of the compliance checklist.

I confirm that I have performed such internal assessment as I considered necessary to enable me to assess the Company’s compliance with the applicable sections of POPIA.

I also confirm to the best of my knowledge and belief the following representations made to you in relation to the Company, the board of directors of the Company (“the Board”), the Company’s information officer, policies and procedures during the performance of your engagement for the purposes of compiling your report on factual findings. Where I know such representation to be incorrect or not-applicable, I have disclosed this to you by ticking the relevant column below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Question | Yes | No | NA |
| 1. | Accountability: Information Officer and Employees | Do you have a POPIA compliance framework? |  |  |  |
| 2. | Does your Information Officer have the requisite capacity, knowledge and |  |  |  |
|  | ability to discharge the duties required of the Information Officer in terms of |
|  | POPIA and the Regulations? |
| 3. | If not, have you appointed deputy Information Officer(s) to assist the |  |  |  |
|  | Information Officer? |
| 4. | Has the Information Regulator been notified of the appointment of the |  |  |  |
|  | Information Officer? |
| 5. | If the Information Officer has other responsibilities, have they been |  |  |  |
|  | assessed to avoid conflicts of interest? |
| 6. | Has the Information Officer developed and completed a personal |  |  |  |
|  | information impact assessment to ensure that adequate measures and |
|  | standards exist in order to comply with the conditions for the lawful |
|  | processing of personal information? |
| 7. | Has the Information Officer developed, monitor, maintain and made |  |  |  |
|  | available a manual as prescribed in sections 14 and 51 of the Promotion of |
|  | Access to Information Act, 2 of 2000? |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 8. |  | Has the Information Officer developed internal measures together with adequate systems to process requests for information or access thereto? |  |  |  |
| 9. | Does the Information Officer conduct regular internal awareness sessions regarding the provisions of POPIA and the Regulations? |  |  |  |
| 10. | Processing Principles: Collection and Retention of Personal Information | Is personal information collected for specified, explicitly defined and lawful purpose, and not further processed in a manner incompatible with those purposes? |  |  |  |
| 11. | Is personal information relevant, limited and minimised to what is necessary in relation to the purposes for which they are processed? |  |  |  |
| 12. | Are there documented principles to justify retention of personal information periods? |  |  |  |
| 13. | Have Data Subjects consented to the retention of personal information? |  |  |  |
| 14. | Is personal information kept only for as long as is necessary for the purposes for which it is processed? |  |  |  |
| 15. | Do you have a process for the destruction or declassification of personal information? |  |  |  |
| 16. | Are there security systems in place, whether electronic or not, to ensure that all retained personal information is appropriately secured, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? |  |  |  |
| 17. | Systems and Software | Has there been implemented processes to ensure privacy by design and default is embedded into projects, to include measures that ensure data minimisation, pseudonymisation, encryption and the processing of only personal information necessary for specified purposes? |  |  |  |
| 18. | Are systems and services frequently audited and tested to ensure ongoing confidentiality, integrity, availability and resilience? |  |  |  |
| 19. | Are records of processing activities maintained in writing and available to the Information Regulator on request? |  |  |  |
| 20. | Processing of Personal Information | Where a data subject exercises their right of access, do you have the appropriate policies and procedures in place to: |  |  |  |
|  | (a) confirm, free of charge, whether or not you hold personal information about that data subject; |  |  |  |
|  | (b) within a reasonable time, at a prescribed fee (if any), in a reasonable manner and format and in a form that is generally understandable, provide the data subject with the record or description of the personal information about that data subject held by you, including the identities of all third parties (or categories of third parties) who have, or have had, access to the information? |  |  |  |
| 21. | Are processes maintained for rectifying inaccurate personal information and having incomplete personal information completed? |  |  |  |
| 22. | Where a data subject requests the erasure of personal information, is every reasonable step to erase all data, links and copies without undue delay? |  |  |  |
| 23. | Where data subjects object to having their data processed for direct marketing, is the data no longer processed and removed? |  |  |  |
| 24. | Is it ensured that data subjects have the right not to be subject to legal or similarly affecting decisions based on automated processing? |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 25. |  | Are you able to demonstrate that data subjects have consented to the processing of their data? |  |  |  |
| 26. | Are consent requests clearly distinguishable from other matters, in an intelligible and accessible form, and written in clear and plain language? |  |  |  |
| 27. | Are data subjects asked to positively opt-in? |  |  |  |
| 28. | Do data subjects have the right to withdraw consent at any time? |  |  |  |
| 29. | If yes, to 29: Is withdrawing consent as easy and giving consent? |  |  |  |
| 30. | Where processing data of subjects below the age of 16 years, is consent given and authorised by the holder of parental responsibility? |  |  |  |
| 31. | If yes to 31, are reasonable efforts made to verify this consent? |  |  |  |
| 32. | Are privacy notices and policies clearly provided to data subjects with processor and Information Officer contact details, purposes of processing, legal bases for processing, recipients of personal information, international transfers, data retention periods and data subject rights? |  |  |  |
| 33. | Where personal information is not obtained directly from data subjects, are categories of personal information provided and the originating sources and whether those are publicly accessible? |  |  |  |
| 34. | Are privacy notices and policies provided to data subjects at the time of collection from data subjects or within one month when not obtained from data subjects? |  |  |  |
| 35. | Are all communications with data subjects provided in writing using clear, concise and transparent language? |  |  |  |
| 36. | Security Compromises | Are breach incident and notification policies and procedures kept? |  |  |  |
| 37. | Are security measures implemented and appropriate for data risks? |  |  |  |
| 38. | Is there a data breach response plan for employees? |  |  |  |
| 39. | Are investigations conducted and corrective action implemented for all personal information breaches? |  |  |  |
| 40. | Are employees aware that the Information Regulator must be notified without undue delay after becoming aware of a data breach? |  |  |  |
| 41. | Is a data breach register maintained which includes:* including facts related to the breach; and
* the effects and remedial actions taken?
 |  |  |  |
| 42. | Do you communicate breaches to affected data subjects without undue delay and in clear and plain language? |  |  |  |
| 43. | Transfer of Personal | When transferring or disclosing personal information, is the data encrypted? |  |  |  |
| 44. | When transferring or disclosing personal information, is the data sent only what is necessary and relevant? |  |  |  |
| 45. | Are secure data transfer methods for all communications utilised? |  |  |  |

Yours faithfully,

 **\_ [NAME OF SIGNATORY]**