Detailed POPIA Compliance Checklist

|  | **Procedure** | **Yes** | **No** | **N/A** | **Done by** | **Date** | **Comments** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Step 1 - Formalise your POPIA compliance project** |
|  | Did you identify your relevant stakeholders (clients, suppliers, individuals etc.)? |  |  |  |  |  |  |
|  | * *Go through your client contracts & appointment letters, invoices, ID documents etc. Do not forget that this includes both natural and juristic persons. Go as far back as possible (use the financial services regulation requirements on how long you should keep data).*
* *Save all these / file them where they can easily be found should you need to provide evidence of them.*
* *Create a spreadsheet where you can list to have a quick reference of how old the data is, who has access to it and where it is stored.*
 |  |  |  |  |  |  |
|  | Did you identify your project sponsor? |  |  |  |  |  |  |
|  | * *Depending on the size of the organization or where the Information Officer is the CEO, this can be an additional support to assist the Information officer in preparing for &maintaining compliance. This is a senior role player. This is not the same as a Deputy Information officer who needs to be officially delegated the duties of the Information Officer as dictated by the Act.*
 |  |  |  |  |  |  |
|  | Did you identify your project manager? |  |  |  |  |  |  |
|  | * *Project manager is also optional, depending on the size of the organization. Reports to the Project sponsor and handles the day to day “tick box” exercises of ensuring compliance.*
 |  |  |  |  |  |  |
|  | Did you set high level scope, timescale, budget, etc.? |  |  |  |  |  |  |
|  | * *This is role is usually appointed to the Project Sponsor.*
* *Based on the results of (a) above, as well as the 8 conditions of compliance, draw up a scope of work, when deliverables are expected, who will do it and how frequently it will be reviewed to maintain compliance e.g. who will train staff of POPIA? How much will the training cost if outsourced? How frequently will refresher training be held? How will new staff be training on ad-hoc?*
 |  |  |  |  |  |  |
|  | Did you identify security safeguards applicable to your industry / business? |  |  |  |  |  |  |
|  | * *Draw up a list of all internal risks and external risks. E.g. Filing cabinets containing client information is in the printing room where all staff have access to it. OR Ensure that my IT service provider is aware of the risks & penalties I face should they accidentally delete / lose my client information.*
* *Along each risk, identify a reasonable mitigating action, e.g. move filing cabinets to a secure area and provide access to a few identified individuals. OR Revise IT services contract to reflect data protection obligation.*
 |  |  |  |  |  |  |
| **Step 2 - Appoint an Information Officer (Legal requirement – Default is highest ranking officer)** |
|  | Did you ensure alignment between your Promotion of Access to Information Act (PAIA) and POPIA Information Officer (IO)? |  |  |  |  |  |  |
|  | * *When drawing up the Job description or KPI’s for the Information Officer, ensure that you include all the duties / responsibilities stipulated in both Acts.*
 |  |  |  |  |  |  |
|  | Did you decide whether the CEO can fulfil the IO function or needs a Deputy/Deputies (DIO)? |  |  |  |  |  |  |
|  | * *After listing the responsibilities as stipulated by the 2 ACTs, it will be clear how much will be required of the Information Officer e.g. taking calls for complaints / having to keep regular updates from the Regulator – Should this be too much for the CEO, a formal delegation, signed by both parties should be drawn.*
* *Deputy should be senior enough to represent the organization should they need to be in court and should be aware of the penalties associated with the role.*
* *Information Officer may be outsourced to an expert service provider.*
 |  |  |  |  |  |  |
|  | Did you agree IO/DIO roles and responsibilities? |  |  |  |  |  |  |
|  | * *All parties are required to sign a written document of the delegation which includes responsibilities and penalties for non-compliance as well as how the role will be performance managed.*
 |  |  |  |  |  |  |
|  | Did you complete the formal appointment process? |  |  |  |  |  |  |
|  | * *Appointment process must include training of appointee & should be included in performance management process should it not be the CEO who is appointed as Information officer.*
 |  |  |  |  |  |  |
| **Step 3 - Perform a gap analysis versus the ACT (POPIA)** |
|  | Did you set interim and final targets for compliance – Compliance within reasonable practicality? |  |  |  |  |  |  |
|  | Did you engage with stakeholders in the assessment? |  |  |  |  |  |  |
|  | Did you use an evidence-based approach? |  |  |  |  |  |  |
|  | Remember to use the assessments for ongoing compliance monitoring. |  |  |  |  |  |  |
| **Step 4 - Analyse what and how Personal Information is processed (status quo)** |
|  | Did you use a broad definition of record types as per the POPIA (e.g. CCTV, biometric)? |  |  |  |  |  |  |
|  | Did you Identify Special Information (e.g. Biometric data, Gender information etc.)? |  |  |  |  |  |  |
|  | Did you look at various aspects as required by the POPIA (including consent, purpose, source, sharing, destruction, etc.)? |  |  |  |  |  |  |
|  | Did you consider user rights and their management? |  |  |  |  |  |  |
|  | Did you think broadly in terms of the types of devices where data is stored – and represents a security compromise risk? |  |  |  |  |  |  |
| **Step 5 - Review / draft POPIA compliance policies based on findings** |
|  | Did you review existing relevant policies? |  |  |  |  |  |  |
|  | Did you ensure your policies are reasonable and appropriate? |  |  |  |  |  |  |
|  | Did you make sure your policies are enforceable? |  |  |  |  |  |  |
| **Step 6 - Review your websites & online platforms** |
|  | Did you refer to your PAIA Manual availability? |  |  |  |  |  |  |
|  | Did you consider and refer to data security notices? |  |  |  |  |  |  |
|  | Did you implement “best practice”, such as Cookie notifications? |  |  |  |  |  |  |
|  | Did you develop and implement your remediation plan? |  |  |  |  |  |  |
| **Step 7 - Update / create your PAIA manual** |
|  | Did you confirm whether your organisation needs a Promotion of Access to Information Act (PAIA) manual? |  |  |  |  |  |  |
|  | Did you confirm whether you are a Public or Private Body as per the PAIA? |  |  |  |  |  |  |
|  | Did you review the proposed contents of your manual? |  |  |  |  |  |  |
|  | Did you ensure your PAIA manual follows the prescribed layout and includes the necessary details? |  |  |  |  |  |  |
| **Step 8 - Implement POPIA compliant PI management processes** |
|  | Did you look at the Personal Information lifecycle: including acquisition, processing, retention, and destruction practices? |  |  |  |  |  |  |
|  | Did you develop reasonable and appropriate measures to ensure ongoing compliance (e.g. Procedure document, self-assessments, health-checks, formal audits)? |  |  |  |  |  |  |
|  | Did you develop your dashboard for monitoring? |  |  |  |  |  |  |
| **Step 9 - Train internal stakeholders on their roles in POPIA compliance** |
|  | Did you design on-going training according to their needs? |  |  |  |  |  |  |
|  | Did you look to special needs such as the IO/DIO roles? |  |  |  |  |  |  |
| **Step 10 - Adopt POPIA compliance as “Business-As-Usual”** |
|  | Did you recognise that POPIA compliance is the “new normal” and work that way? |  |  |  |  |  |  |
|  | Did you build compliance into your products, services and processes – adopt “Privacy By Design”? |  |  |  |  |  |  |
| **Step 11 - Information security Safeguards** |
|  | Did you consider generally accepted information security practices and procedures for both local and international data flows? |  |  |  |  |  |  |
|  | Did you consider electronic data protection tools i.e. Cybersecurity against Ransomware? |  |  |  |  |  |  |
|  | Did you consider means for secure data transfer, storage & recovery? |  |  |  |  |  |  |
|  | Did you revise processes for non-electronic data storage / filing? |  |  |  |  |  |  |
|  | Did you agree on safety practices for both operators and processors of data and manage these through contractual agreement where necessary? |  |  |  |  |  |  |

Information Officer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Important Note:*** *Remember to attach proof of the above steps to this checklist, where appropriate.*