POPI WHAT CAN WE DO

Policy Review

Entity Wide Gap Analysis

Data Flow Maps

System Changes

Information Security Processes

WHAT CAN WE DO	HIGH LEVEL DETAIL	DELIVERABLE
ENTITY WIDE GAP ANALYSIS	A complete POPI gap analysis of the current level of compliance with the principles of POPI ("the gap analysis") at an entity level and identification of the organisations vulnerabilities and risks from POPI perspective.	A written report detailing • the outcomes of the initial gap analysis at the entity level; • the existing general data governance processes in place regarding personal information processed by the entity, • the general threats to achieving POPI compliance per process; and • our recommendations on proposed amendments to the relevant policies and procedures at an entity level.
IN DEPTH ANALYSIS	An in-depth assessment of the compliance of individual business units/divisions with the requirements of the POPI Act.	A written report dealing with the outcomes of the in depth analysis of the current state of, and required future state, for POPI compliance for each in-scope business unit including: • an analysis of whether employee and customer data is processed according to the conditions; • current data governance processes in place regarding this data; and • threats to achieving POPI compliance per process;
COMPLIANCE RISK MANAGEMENT PLAN	Developing and implementation a compliance risk management plan to assist in: • Managing compliance with POPI; • Development of a privacy and data protection implementation road map to prioritise actions required to close the gaps identified through the gap assessment.	Our key deliverable for this activity will be a customised, consolidated POPI Compliance Risk Mitigation Plan to provide an overall view of POPI Compliance Risk Mitigation across the entity that details the following: • Legislation title; • Reference: Key section/ regulation; • Section wording; • Plain-language Interpretation of applicable sections; • Compliance obligation(s); • Consequences of non-compliance; • Risk Rate / Grade; • Responsible persons / departments; • Existing controls; • Proposed controls / recommendations; and • Management response.
PERSONAL INFORMATION IDENTIFICATION	Identification and analysis of the personal information identified through assessing info stored across the entity and design of a data classification policy, procedure and register.	A written report detailing the personal information identified through the assessment, stored across the entity and design of a data classification policy, procedure and register.
DATA FLOW MAPS	Development of data flow maps to illustrate the flow of personal information within the entity and highlight any significant risks to the flow of personal information throughout its life cycle. (i.e. collection, storage, use, dissemination, retention or destruction.)	Diagrammatic representation of data process flows accompanied by detailed explanations and an assessment of the processing risks and controls of personal info as it is processed by the entitiy.
THIRD PARTY PROCESSING	Third party processing would involve consideration of the following: • Identification of what personal information is processed outside of the organisation and by whom; • Identifying where no third party agreements are in existence, but are required in terms of POPI; • Analysis and review of third party contracts, in terms of which personal information is processed for and on behalf of the organisation; • Advising on contractual amendments which are required to be made to ensure compliance with POPI; • Assesment performance on the third party contract management processes in place pre, post and during third party engagement (i.e. due diligence, vendor selection, contract termination and return of personal information); • Performing third party POPI audits to provide assurance of third party compliance to the POPI Act and agreed contractual obligations; and • Performing an assessment of the security controls in place to ensure the protection of personal information during transmission to third parties and the data protection controls (technical, organisational and physical) in place within the third party environment.	A written report detailing what information is processed, list of identified third parties who process personal information on behalf of the entity, with recommendations relating to: • The adequacy of third party contracts; • Third party contract compliance; • Adequacy of third party controls for the protection of personal information; • Third party contract management.
TECHNICAL / IT POPI ASSESSMENT	An assessment of the IT controls in place to ensure the lawful processing of personal information in respect of the POPI Act, by performing the following: • An assessment of the general IT controls in place (i.e. Access, Change Management, Disaster Recovery and Backup); • A high-level assessment of the IT security controls in place to maintain the protection of personal information; • An assessment of the data quality controls in place to ensure the accuracy and completeness of personal information maintained in the IT environment; • An assessment of the IT enterprise architecture to identify deficiencies or areas for improvement that may be required to comply with the POPI Act; • An assessment of the data classification policies, procedures and controls in place; • Where applicable, an assessment of the cloud environment to ensure the security of personal information stored in the cloud and compliance with POPI and foreign data protection laws (e.g. UK Data Protection Act); • As assessment of the organisation's use of social media against the requirements of the POPI Act; and • An assessment of the organisation's online presence (i.e. website) and its compliance to the POPI.	A written report detailing deficiencies / areas for improvement identified and best practice recommendations for the remediation thereof.

WHAT CAN WE DO	HIGH LEVEL DETAIL	DELIVERABLE
IMPLEMENTATION ASSISTANCE	Assistance with the implementation of any of the corrective measures identified through the POPI gap analysis to enable your organisation to best achieve compliance with the requirements of the POPI Act from an organisational and technical perspective.	Based on the identified gaps within your environment implementation assistance may include inter alia: • Design of organisational structures that enable and foster accountability for POPI within the organisation; • Design, and/or update of policies, procedures, terms and conditions and third party contracts; • POPI training and awareness workshops/programmes; • Assistance with organisational change management; • Security control framework implementation; and • Design and implementation of a POPI compliance management framework.
DATA EXCHANGE	Identification and analysis of the exchange of personal information between organisational entities and partners, cross-border transfers of such information in terms of the POPI Act and foreign data protection laws, where applicable.	A report detailing: • The POPI risk categorisation of the entity counterparts and third parties based on contractual safeguards in place, level of dependency, volume and nature of personal information being exchanged, and/or applicable foreign data protection laws; • Identified personal information exchanged with organisational entities and partners, or through cross-border transfers; • Identified gaps and best practice recommendations for the remediation thereof; and • The organisation's level of compliance to cross-border data protection laws.
IMPLEMENTATION ROAD MAP	Once the POPI compliance gaps have been identified under the initial gap analysis and in-depth assessments, KPMG will identify synergies, initiatives and impacts relating to data protection across the entity. These observations will be used to develop a set of recommendations to prioritise actions required to close the gaps identified through the gap analysis and in-depth assessment.	Our deliverables for this item will be: • A customised set of prioritised risk recommendations, for management's consideration; • A customised POPI roadmap that will detail key activities; and • High level timelines for the remediation of gaps which if adopted and implemented by the entity will enable the business to achieve an acceptable level of compliance with POPI.
MARKETING PRACTICES	An assessment of your organisation's marketing practices to determine your level of compliance in respect of the POPI Act, Consumer Protection Act and Electronic Communications and Transactions Act and other relevant Act(s) detailed in your organisation's Regulatory Universe. This will enable your business to leverage synergies between multiple legislative and regulatory requirements to achieve a holistic level of compliance.	A report detailing the level of compliance of the organisations marketing practices with the relevant Act(s) and best practice recommendations for the remediation of such gaps to enable the organisation to attain a holistic level of compliance.
POLICY REVIEW	Review your organisation's policies to ensure that they cater for the protection of personal information processed by your organisation.	A written report identifying non-compliance and data protection gaps in your organisation's policies, and best practice recommendations and/or model clauses for the remediation thereof.
TRAINING/AWARENESS	Provide training and awareness programmes in respect to POPI, its impact on your organisation and how it will change the way you do business for your clients, employees, management and/or directors.	Training sessions tailored to meet your organisation's needs.
INFORMATION SECURITY ASSESSMENT	Perform a review of your organisation's ability to comply with the POPI Acts requirement for technical and organisation security controls to be in place through the following: • An assessment of the security controls in place to protect personal information, against the requirements of ISO 27001/2; • An assessment of the technical security controls in place (i.e. web application reviews, infrastructure penetration testing, firewall reviews, operating system and database reviews, active directory reviews); and • An assessment of the maturity of the organisations cyber security framework.	A report detailing your organisations gaps in respect to securing personal information from a technical and organisational perspective and detailed best practices for the remediation thereof.
INFORMATION SECURITY INCIDENT MANAGEMENT	An assessment of your organisation's processes to determine your ability to respond effectively and efficiently to information security incidents involving the unauthorised disclosure or abuse of personal information in accordance with the requirements of the POPI Act.	A detailed report and implementation plan for the integration of an effective, POPI compliant information security incident response management framework, that identifies your current gaps and provides best practice recommendations for the remediation thereof.
INFORMATION OFFICER APPOINTMENT	Appoint an information officer who knows and understands their responsibilities under POPI. (Note: The information officer will be responsible, not only for compliance, but also for engaging with the Information Regulator where the organisation is under investigation)	Develop and define the Information Officers roles and responsibilities within the organisation.
POPI EXEMPTIONS	Consider whether your organisation and any of the processes which it undertakes falls within the exemption provisions of POPI.	Legal opinion advising on whether the organisation is exempt under POPI or any part thereof.

Compliance risk mitigation programme

Pesonal information elements

In Depth Analysis