PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT) – DEVELOPMENT OF IMPLEMENTATION AND COMPLIANCE OFFERING PROJECT			
Document:	**DATA PRIVACY RISK IMPACT ASSESSMENT CONSIDERATIONS GUIDELINE REFERENCE DOCUMENT**	**Version:**	13.10.20
Purpose:	To provide guidance on how to consider and implement Data Privacy Risk Management for an SMME FSP		

1. INTRODUCTION

In considering risks about Data Privacy Management and the POPI Act, sections 19 and 109(3)(g) are specifically relevant. These sections are quoted below and the relevant wording is highlighted for ease of reference.

Security measures on integrity and confidentiality of personal information
19
(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
(a) loss of, damage to, or unauthorised destruction of personal information; and
(b) unlawful access to or processing of personal information.
(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—
(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Administrative fines
109
(3) When determining an appropriate fine, the Regulator must consider the following factors:
(g) any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information.

It should be noted that although section 19 refers to “security measures” it is self-evident and in line with international best practices in Data Privacy Management (of which Information Security Management is a subset) that considering risks pertaining to data, breaches involve much more than only security considerations.

Data Privacy Risk (and Risk Impact) Assessment can be done as part of:

- an overall business risk assessment taking compliance to the POPI Act and good Data Privacy Management principles (which integrates with good Governance and best business practices) into account;
- recording personal information data flows and related risks; and
- assessing data privacy risks relating to procedures, systems, projects, or products, referred to as Data Privacy Impact Assessments [DPIAs] – incorporating the concept of ‘Privacy by Design’.

2. AS PART OF OVERALL BUSINESS RISK ASSESSMENTS

The purpose of this guideline document is not to address or reconfirm the standard (enterprise) risk assessment process should follow, typically addressing the elements indicated below, as per the existing Masthead Risk Management Plan template below:

Risk Assessment				Risk Treatment					Risk Monitoring	
Likelihood	Impact	Risk Rating	Risk Category (See guideline)	Existing Control	Adequate (Yes /No)	Action Plan	Responsible Person	Target Implementation Date	Review Comment	Review Date

The following business risk-related considerations, specifically relevant to compliance to the POPI Act and good Data Privacy Management, can however be highlighted:

- Due to the legislative and reputational risk implications of data breaches, it is advisable to prioritise risk mitigation regarding compliance to the POPI Act.
- Ensuring compliance with the POPI Act and implement effective Data Privacy Management (especially when establishing an effective system in this regard) often takes more dedicated time and resources than initially estimated.
- Considering compliance to the POPI Act and implement effective Data Privacy Management as a 'tick box' exercise or that completing certain templates will be sufficient, is a very risky paradigm. Effectively implementing all relevant activities and maintaining the management system and risk-based thinking approach is the only way to effectively reduce the risk of non-compliance or breaches.
- Data breaches often occur in the simplest of business processes and hence all business processes need to be considered.

3. AS PART OF THE INFORMATION FLOW AND RISK MITIGATION ASSESSMENT

Kindly refer to this relevant template – and specifically the requirement to highlight risky elements in red and the last columns in it, addressing risk and mitigation measures identified per relevant business function and process.

4. DATA PRIVACY IMPACT ASSESSMENTS (DPIAs)

The POPI Act does not make specific reference to DPIAs and the regulator has not yet issued guidelines in this regard. International best practices and established guidelines can hence be quoted and followed in this regard.

According to the European Union's "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"* ", a DPIA is defined as: "*a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.*". It should be noted that the European Union's General Data Protection Regulation (GDPR) only addresses personal information of private individuals ("*natural persons*") and the POPI Act applies to both private and juristic persons.

The Information Flow and Risk Mitigation Assessment template can be used for DPIAs on current and new business processes and initiatives. For more details, or for bigger projects or planned initiatives the following guidelines and templates can be followed:

- The European Union's "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"* can be downloaded by following this link: **http://ec.europa.eu/newsroom/document.cfm?doc_id=47711;**
- A template (developed by the UK Information Commissioner's Office) to conduct a comprehensive specific DPIA can be accessed here: **https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf**