PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT) – DEVELOPMENT OF IMPLEMENTATION AND COMPLIANCE OFFERING PROJECT			
Document:	**BANK OF FREQUENTLY ASKED QUESTIONS REFERENCE DOCUMENT**	**Version:**	13.10.20
Purpose:	Frequently Asked Questions to be referred to in case of uncertainty as part of the personal information Act compliance and effective Data Privacy Management journey		

1. INTRODUCTION

The frequently asked questions listed below are aimed at supporting the personal information Act compliance and effective Data Privacy Management journey, as one of the quick reference guides as part of the Masthead solutions. It addresses certain practical questions that may arise in the compliance management process. It is not meant for general information purposes regarding the personal information Act, which can be accessed in the personal information Act and regulations and Regulator's Guidelines, or forms part of other Masthead webinars, online training and compliance project presentations and information shared. It is also not meant to address how specific compliance activities need to be implemented.

This document is a living document that needs to be updated as legal requirements, guidelines or circumstances may change. It is a guideline reference tool with standardised answers and does not fulfil the function of or replace formal professional advice on any matter.

Keep an eye on the Masthead website, newsletters, webinars and training courses for answers to future additional frequently asked questions.

2. FREQUENTLY ASKED QUESTIONS

TYPICAL QUESTION	STANDARD ANSWER
What is the real purpose of the POPI Act?	*Section 2 of the POPI Act specifies its purpose:* ***2.** The purpose of this Act is to—* *(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—* *(i) balancing the right to privacy against other rights, particularly the right of access to information; and* *(ii) protecting important interests, including the free flow of information within the Republic and across international borders;* *(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that* *prescribe the minimum threshold requirements for the lawful processing of personal information;* *(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and* *(d) establish voluntary and compulsory measures, including the establishment of*

TYPICAL QUESTION	STANDARD ANSWER
	an Information Regulator, to ensure respect for and to promote, enforce and *fulfil the rights protected by this Act.*
How is an Information Office appointed?	The Information Officer is not appointed, it is a legal function bestowed on the 'head' of an organisation or business. The personal information Act defines the Information Officer as: ***''information officer''*** *of, or in relation to, a—* *(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or* *(b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;* Section 1 of the Promotion of Access to Information Act (PAIA) defines it as such: *in relation to, a private body means-* *(a) in the case of a natural person, that natural person or any person duly authorised by that natural person;* *(b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;* *(c) in the case of a juristic person-* *(i) the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or* *(ii) the person who is acting as such or any person duly authorised by such acting person* Deputy Information Officers can be appointed by the business as per section 56 of the personal information Act. The details of both Information Officers and Deputy Information Officers must be registered with the Regulator as prescribed by the regulators Guidelines issued in this regard.
What is the most effective way of mitigating the risk of non-compliance with the POPI Act?	Ensure that at the point of collection of the personal information the specific and informed consent of the data subject is obtained voluntarily. This means the data subject must be informed of what personal information will be processed for what purpose/s as well as any possible third party recipients and the purpose for sharing with such third party, and the data subject must explicitly agree. In other words, there must be full notification/disclosure followed by consent. As long as there are openness and transparency with the data subject about the processing and the data subject agrees, risks would be substantially mitigated.
Can an Information Officer be personally liable for data breaches or non-compliance to the personal information Act	If the Information Officer is the Responsible Party (in the case of a sole proprietor, for example), then yes. If the Information Officer is an employee of a Responsible Party then the Responsible Party will be liable, but employees who do not comply to the personal information Act can be held responsible by their employers and if an employee commits a criminal offence in the process (for example to steal and sell account numbers of clients), he/she can be personally prosecuted.

TYPICAL QUESTION	STANDARD ANSWER
What is the need and purpose of the Privacy Policy	It conveys the commitment and principles regarding personal information compliance and good Data Privacy Management to clients, business partners, suppliers etc. It is aimed at building trust and showing commitment.
Can questions or information that has personal information Act implications be shared verbally with clients, Operators or Third Parties?	Yes, but it needs to be confirmed in writing.
Will attending training on the POPI Act ensure compliance and reduce breach risks	Not on its own. Implementing all compliance activities effectively and continuously is the only way to ensure compliance and breach risk reduction.
Why are awareness and training so important?	A great part of breach risk reduction is to 'think privacy' on a constant basis and be aware of possible risks and gaps. Capacitating the mind to do so greatly enhances risk reduction.
What is an automated decision system?	It is a statistical model or tool built into an electronic system to enable an automated/electronic decision, in other words, the decision is made in a purely automated way without human intervention.
Is it necessary to implement a separate Privacy Risk Management System	Depending on the size of the business, Data Privacy Management and Information Security are normally addressed as a component of the overall business risk management system.
Can the Responsible Party appoint a third party to process personal information on its behalf?	Yes, the third party is known as an Operator, will act under the authority and specific instructions of the responsible party, and must be appointed in terms of a written contract that ensures that the operator is bound by the POPI Act.
Can the Responsible Party share personal information with a third party?	Yes in terms of a contract, whereby the third party warranties that it will fully comply with the POPI Act in the processing of the personal information from the point of receipt of the personal information from the responsible party, and the Responsible Party confirms that the POPI Act was fully complied with up to the point of transfer to the third party.
Is it sufficient just to have a data privacy and security agreement in place with Operators or Third Parties	Although such an agreement is a minimum requirement of the POPI Act, it's advisable to do a proper due diligence and as far as possibly responsibly ensure that Operators and Third Parties are indeed compliant and secure.
Which automated decision systems are governed by the POPI Act and must be compliant with the Act?	Any automated decision system that will have legal consequences for the data subject or affect the data subject substantially.
What is the minimum requirement for processing personal information for the purpose of direct marketing via electronic communication to a non-existing client?	The data subject must provide specific and informed, express consent before the processing.
What is the minimum requirement for processing personal information for the purpose of direct marketing via non-electronic communication to an existing client?	The data subject must be given the right/opportunity to object to the processing of personal information for the purpose of direct marketing (right to opt-out) and be afforded this opportunity each time direct marketing communication is sent.

TYPICAL QUESTION	STANDARD ANSWER
When can personal information be sent from South Africa to a third party in a foreign country?	If the foreign country has a law that is similar to and consistent with the POPI Act, which the recipient in the foreign country is subject to; if there is a binding agreement between recipient and sender that ensures full compliance the POPI Act; or if the recipient and sender, are part of the same corporate structure, and are bound by binding corporate rules that ensure full compliance with the POPI Act.
What is meant by Privacy by Design	It means that data privacy and security is considered when any new process or system is developed and compliance and breach risk reduction is taken into account in the design of the new process or system
When it comes to information security, is it critical to be ISO27001, 27002 and 27701 certified.	No, not certified, unless a specific contract or business relationship requires it. But procuring, reading and implementing the principles and guidelines in such international standards is advisable and can greatly contribute to breach risk reduction.
What to do when a breach occurs	Refer to the Guideline document in this regard.
When does the POPI Act not apply and/or what are the exemptions	Sections 6, 7 37 and 38 of the POPI Act specifically address certain exclusions or exemptions to the Act. Sections 11 and 12, for example also address conditional exclusions from specific provisions of the Act, including reference to the 'legitimate interest' of the data subject, Responsible Party or Third Parties. These exclusions should however not be seen as opportunities not to comply with the Act and will probably be interpreted and treated limitedly by the regulator and courts.
Can I update and change any of the templates provided to me by Masthead	You may and should tailor and update templates to your business circumstances and requirements, but it is advisable to check in with Masthead if you are uncertain about the implications of significant changes.