PROTECTION
OF PERSONAL INFORMATION POLICY (PoPI)

1. Purpose

The purpose of the PoPI Act (Protection of Personal Information Act) is to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise one's personal information in any way.

2. Preamble

The PoPI legislation basically considers one's personal information to be "precious goods" and therefore aims to bestow upon one, as the owner of one's personal information, certain rights of protection and the ability to exercise control over:

- when and how one chooses to share one's information (requires one's consent);
- the type and extent of information one chooses to share (must be collected for valid reasons);
- transparency and accountability on how one's data will be used (limited to the purpose) and notification if/when the data is compromised;
- providing one with access to one's own information as well as the right to have one's data removed and/or destroyed should one so wish;

- who has access to one's information, i.e. there must be adequate measures and controls in place to track access and prevent unauthorised persons, even within the same company, from accessing one's information;
- how and where one's information is stored (there must be adequate measures and controls in place to safeguard one's information to protect it from theft, or being compromised); and
- the integrity and continued accuracy of one's information (i.e. one's information must be captured correctly and once collected, the institution is responsible to maintain it).

Examples of "personal information" for an individual could include:

- Identity and/or passport number;
- Date of birth and age;
- Phone number/s (including mobile phone number(s));
- Email address(es);
- Online/Instant messaging identifiers;
- Physical address;
- Gender, Race and Ethnic origin;
- Photos, voice recordings, video footage (also CCTV), biometric data;
- Marital/Relationship status and Family relations;
- Criminal record;
- Private correspondence;
- Religious or philosophical beliefs including personal and political opinions;
- Employment history and salary information;
- Financial information;
- Education information;
- Physical and mental health information including medical history, blood type, details on one's sex life; and
- Membership of organisations/unions.

It must however be noted that some personal information, on its own, does not necessarily allow a third party to confirm or infer someone's identity to the extent that this information can be used/abused for other purposes. The combination of someone's name and phone number and/or email address for example is a lot more significant than just a name or phone number on its own. As such the Act defines a "unique identifier" to be data that "uniquely identifies that data subject in relation to that responsible party".

We must accept that we now live in a progressive information age and along with this progress comes the responsibility for each person to take care of and protect his/her own information. One cannot accuse someone else / an institution of sharing or compromising one's personal information when one publishes the very same information on social media services such as Facebook, LinkedIn, WhatsApp, Google or public directories etc. Modern technology makes it easy to access, collect and process high volumes of data at high speeds. This information can then be sold, used for further processing and/or applied towards other ends. In the wrong hands such an ability can cause irreparable harm to individuals and companies. To protect one's right to privacy and abuse of one's information, data protection legislation is necessary even if it means imposing some social limits on society to balance the technological progress. The PoPI Act cannot protect one if one does not take care to protect oneself.

It is important to note though that this right to protection of "personal information" is not just applicable to a natural person (i.e. an individual) but any legal entity, including companies and also communities or other legally recognised organisations. All of these entities are considered to be "data subjects" and afforded the same right to protection of their information. This means that while one, as a consumer, now has more rights and protection,

one and/or one's company/organisation are considered "responsible parties" and have the same obligation to protect other parties' personal information. As a company this would include protecting information about one's employees, suppliers, vendors, service providers, business partners, etc.

The PoPI legislation is not a rare or unique phenomenon to South African law. Many countries have similar legislation in place to protect the personal information of their "data subjects", including rules and regulations for international (cross-border) transfer and sharing of data. The general consensus seems to be that the PoPI Act is well thought out and it borrows from the "best of" other similar international laws, learning from their mistakes and shortcomings.

As usual, ignorance of the law is no excuse. Incorporating PoPI into the day-to-day operations of a business will most likely require a significant amount of time and effort, including educating and training staff, updating business processes and implementing or updating technology solutions. Early action is essential, especially if one does not have a business nervous system (BNS) to facilitate this. Consider for example that under the PoPI Act one could be breaking the law if one does something as simple as synchronising one's contacts on one's cellular phone, sending an email with sensitive content, taking/sharing a video or photo, using an international mail provider (like Google…) and so forth.

3. Accountability

3.1. A Personal Information Compliance Officer (the "Officer") must be appointed in writing by the CEO.

3.2. The Officer shall form a Review Committee to attend to any appeals that may be lodged by any person / institution. The committee must consist of personnel who fully understand the Act and the Policy and must consist of at least 3 persons.

3.3. All persons, whether employees, volunteers, or board or committee members who collect, process, or use personal information shell be accountable for such information to the Officer. They must be advised thereof in writing by the Officer together with a copy of this policy.

3.4. This policy shall be made available via KLM Empowered Human Solutions Specialists (Pty) Ltd's website (www.klmempowered.com), or a paper copy provided upon written request.

3.5. Any personal information transferred to a third party for processing is subject to this Policy. The Officer shall use the contractual or other appropriate means to protect personal information at a level comparable to this Policy while a third party is processing this information.

3.6. Personal information to be collected, retained, or used by KLM shall be done so only after the Officer gives written approval. This information shall be secured according to the Officer's instruction.

3.7. Any person who believes KLM uses personal information collected, retained, or used for purposes other than those that the person explicitly approved may contact the Officer to register a complaint or to manage any related inquiry.

3.8. Upon receiving a complaint from any person regarding the collection, retention, or use of personal information, the Officer shall promptly investigate the complaint and notify the person who complained about his/her findings and the corrective action taken, if any.

3.9. Upon receiving the response from the Officer, the person who filed the complaint may, if he/she is not satisfied, appeal to KLM's Review Committee to review and determine the disposition of the complaint at issue.

3.10. The determination of the Review Committee shall be final and the Officer shall abide by and implement any of its recommendations.

3.11. The Officer shall communicate and explain this policy and give training regarding it to all employees and volunteers who might be in a position to collect, retain, or make use of personal information.

3.12. The Officer shall prepare and disseminate information to the public which explains KLM Empowered's protection of personal information policies and procedures.

4. Identify Purposes

4.1. The Officer shall document the purpose for which personal information is collected to comply with the openness and individual access principles outlined below.

4.2. The Officer shall determine the information that will be needed to fulfil the purposes for which the information is to be collected which must comply with the limited collection principles below.

4.3. The Officer shall ensure that the purpose is specified at or before the time of collecting the personal information from an individual / institution.

4.4. The Officer shall ensure that the information collected will not be used for any other purpose before obtaining the individual's / institution's approval, unless the new purpose is required by law.

4.5. The Officer shall ensure that a person collecting personal information will be able to explain to the individual why this is being done.

4.6. The Officer shall ensure that limited collection, limited use, disclosure, and retention principles are respected in identifying why personal information is to be collected.

5. Consent

5.1. The Officer shall ensure that the individual from whom personal information is collected consents to this and to it being used and disclosed.

5.2. The Officer shall ensure that the individual can reasonably understand who and how the information will be used when the consent is given.

5.3. The Officer shall ensure that no condition is attached to supplying benefits, because of KLM's activities, requiring the individual to give consent for the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purpose.

5.4. The Officer shall ensure that express consent is obtained wherever possible and appropriate. In rare circumstances where, in the Officer's opinion, having regard to the information's sensitivity and the Policy's purpose and intent, implied consent may be acceptable.

5.5. In obtaining consent, the Officer shall ensure that the individual's reasonable expectations are respected. (For example, a person giving his/her name and address to a charity to receive its newsletter or magazine reasonably expresses that it will use that information about itself. But the individual would not likely expect that the information would be used for fundraising).

5.6. The Officer shall ensure that the express consent obtained from an individual is clear and in an appropriate verifiable format.

5.7. The Officer shall ensure that the individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The individual shall promptly be informed of the withdrawal implications, if any.

6. Limiting Collection

6.1. The Officer shall ensure that personal information will not be collected indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. The Officer shall specify the type of information to be collected.

6.2. The Officer shall ensure that information is collected only by fair and lawful means without misleading or deceiving individuals as to the reason.

6.3. The Officer shall ensure that the identifying purposes and consent principles are followed in identifying why personal information is being collected.

7. Limiting Use, Disclosure, and Retention

7.1. The Officer shall ensure that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law, and any use of personal information shall be properly documented.

7.2. The Officer shall ensure that all personal information is destroyed, erased, or made anonymous as soon as the purpose for which it was collected is no longer relevant, or as permitted by law.

7.3. There shall be an automatic review of the need to continue retaining personal information annually. Except as required to be retained by law, all personal information shall be deleted, erased, or made anonymous no later than 7 (seven) years after the purpose for which it was collected has been completed.

7.4. The information shall be erased or destroyed by way of acceptable erasure and/or destruction methods e.g. a mechanical shredder, permanent deletion of cloud records, etc.

7.5. The Officer shall ensure that all use, disclosure, and retention decisions are made in light of the consent principle, the identifying purposes principle and the individual access principle.

8. Accuracy

8.1. The officer shall reasonably ensure that the personal information is accurate, complete, and up to date, taking into account the individual's interests. The Officer shall ensure that the information is sufficiently accurate, complete and up to date to minimise the possibility that inappropriate information might be used to make a decision about an individual.

8.2. The Officer shall ensure that KLM does not routinely update personal information, unless it is necessary to fulfil the purposes for which the information was collected.

8.3. The Officer shall ensure that personal information used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up to date, unless limits to the requirements for accuracy are clearly set out.

9. Safeguards

9.1. The Officer shall ensure that KLM has security safeguards to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification. The Officer shall do this regardless of the format in which KLM holds the information.

9.2. Depending on the information's sensitivity, the Officer may permit reasonable discretion regarding the information that has to be collected: the amount, distribution, format, and the method of storage. A higher level of protection shall safeguard more sensitive information according to the consent principle's considerations.

9.3. The Officer shall ensure that the protection methods include,

9.3.1. Physical measures, for example, locked filing cabinets, controlling access to keys, key registers and restricted access to offices;

9.3.2. Organisation measures, for example, security clearance, and limiting access on a "need-to-know" basis; and

9.3.3. Technological measures, for example, the use of passwords and encryption.

9.4. The Officer shall ensure that all employees and volunteers know the importance of keeping personal information confidential.

9.5. The Officer shall ensure that care is taken when personal information is disposed of or destroyed to prevent unauthorised parties from gaining access to it.

10. Openness

10.1. The Officer shall ensure that KLM is open about its policies and practices regarding the management of personal information. The policies and information about the related practices shall be available without unreasonable effort in a format that is generally understandable.

10.2. The Officer shall ensure that the information available shall include:

10.2.1. The name or title and address of the Officer who is accountable for KLM's policies and practices and to whom complaints or inquiries can be forwarded;

10.2.2. The means of gaining access to personal information held by KLM;

10.2.3. A description of the type of personal information held by KLM including a general account of its use;

10.2.4. A copy of any brochures or other information that explain KLM's policies, standards, or codes; and

10.2.5. What personal information is made available to related organisations (e.g. organisations that are affiliated).

10.3. The Officer shall ensure that the information that must be provided according to section 10.2 of this policy is available either in a brochure at the locations KLM operates, online, or through the mail.

11. Individual Access

11.1. The Officer shall ensure that upon request KLM shall inform an individual whether KLM holds personal information about him/her. If possible, the information's source shall also be given. KLM shall also account for the use that has been made or is being made of this information and give an account as to the third parties to whim it has been disclosed. (Note, if the Officer believes for valid reasons that access to personal information should be denied, the Officer shall consult legal counsel before making such a decision).

11.2. A person requesting his/her personal information may be required by the Officer to give sufficient information to permit KLM to provide an account of the existence, use, and disclosure of personal information. Information shall be used only for the purpose for which it was obtained.

11.3. If KLM has supplied personal information about an individual to third parties, the Officer shall ensure that an attempt is made to be as specific as possible. When it is impossible to give a list of organisations to which KLM has actually disclosed information about an individual, KLM shall provide a list of organisations to which it might have disclosed information about the individual.

11.4. The Officer shall ensure that KLM responds to an individual's request within a reasonable time, but no later than 7 days from the date of receipt of the request, and at minimal or no cost to the individual. The requested information shall be made available in a generally understandable form. For example, the organisation shall explain abbreviations or codes it uses to record information.

11.5. The Officer shall ensure that when an individual successfully demonstrates the inaccuracy or incompleteness of personal information, KLM shall amend the information as required. Depending on the information challenged, amendment involves the correction, deletion, or addition of information in question.

11.6. The Officer shall ensure that when a challenge is not resolved to the individual's satisfaction, KLM shall record the unresolved challenge's substance. When appropriate, the unresolved challenge's existence shall be transmitted to third parties having access to the information in question.

12. Challenging Compliance

12.1. The Officer is authorised to address a challenge concerning compliance with the above principles.

12.2. The Officer shall develop procedures to receive and respond to complaints or inquiries about the policies and practices regarding the handling of personal information. The compliance procedures shall be easily accessible and simple to use.

12.3. The Officer shall inform individuals inquiring about lodging complaints that the relevant complaint procedures exist.

12.4. The Officer shall investigate all complaints. If a complaint is found to be justified, the Officer shall take appropriate measures, including, if necessary, amending this Policy and general policies and practices pertaining to personal information entrusted to KLM.

13. Discipline

13.1. Any employee or manager failing to adhere to this policy and procedure may be subjected to disciplinary action in terms of the Disciplinary Code and Procedures of KLM.

Prepared on behalf of KLM Empowered
Human Solutions Specialists (Pty) Ltd
10 October 2017