POPI compliance checklist

Companies can assess the amount of preparation needed to ready themselves for the implementation of the Protection of Personal Information Bill ("POPI") by considering the following minimum requirements:

1. Audit the processes used to collect, record, store, disseminate and destroy personal information: in particular, companies must ensure the integrity and safekeeping of personal information in their possession or under their control. They must take steps to prevent the information being lost or damaged, or unlawfully accessed.
2. Define the purpose of the information gathering and processing: personal information must be collected for a specific, explicitly defined and lawful purpose that is related to a function or activity of the company concerned.
3. Limit the processing parameters: the processing must be lawful and personal information may only be processed if it is adequate, relevant and not excessive given the purpose for which it is processed.
4. Take steps to notify the 'data subject': the individual whose information is being processed has the right to know this is being done and why. The data subject must be told the name and address of the company processing their information. In addition, he or she must be informed as to whether the provision of the information is voluntary or mandatory.
5. Check the rationale for any further processing: if information is received via a third party for further processing, this further processing must be compatible with the purpose for which the data was initially collected.
6. Ensure information quality: the company processing the information must make sure the information is complete, accurate, up to date and not misleading.
7. Notify the information Protection Regulator: when the POPI is enacted and a Regulator established, organisations processing personal information will have to notify the Regulator about their actions.
8. Accommodate data subject requests: the POPI allows data subjects to make certain requests, free of charge, to organisations holding their personal information. For instance, the data subject has the right to know the identity of all third parties that have had access to their information. A data subject can also ask for a record of the information concerned.
9. Retain records for required periods: personal information must be destroyed, deleted or 'de-identified' as soon as the purpose for collecting the information has been achieved. However, a record of the information must be retained if an organisation has used it to make a decision about the data subject. The record must be kept for a period long enough for the data subject to request access to it.
10. Cross border data transfer: there are restrictions on the sending of personal information out of South Africa as well as on the transfer of personal information back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned, as the case may be.