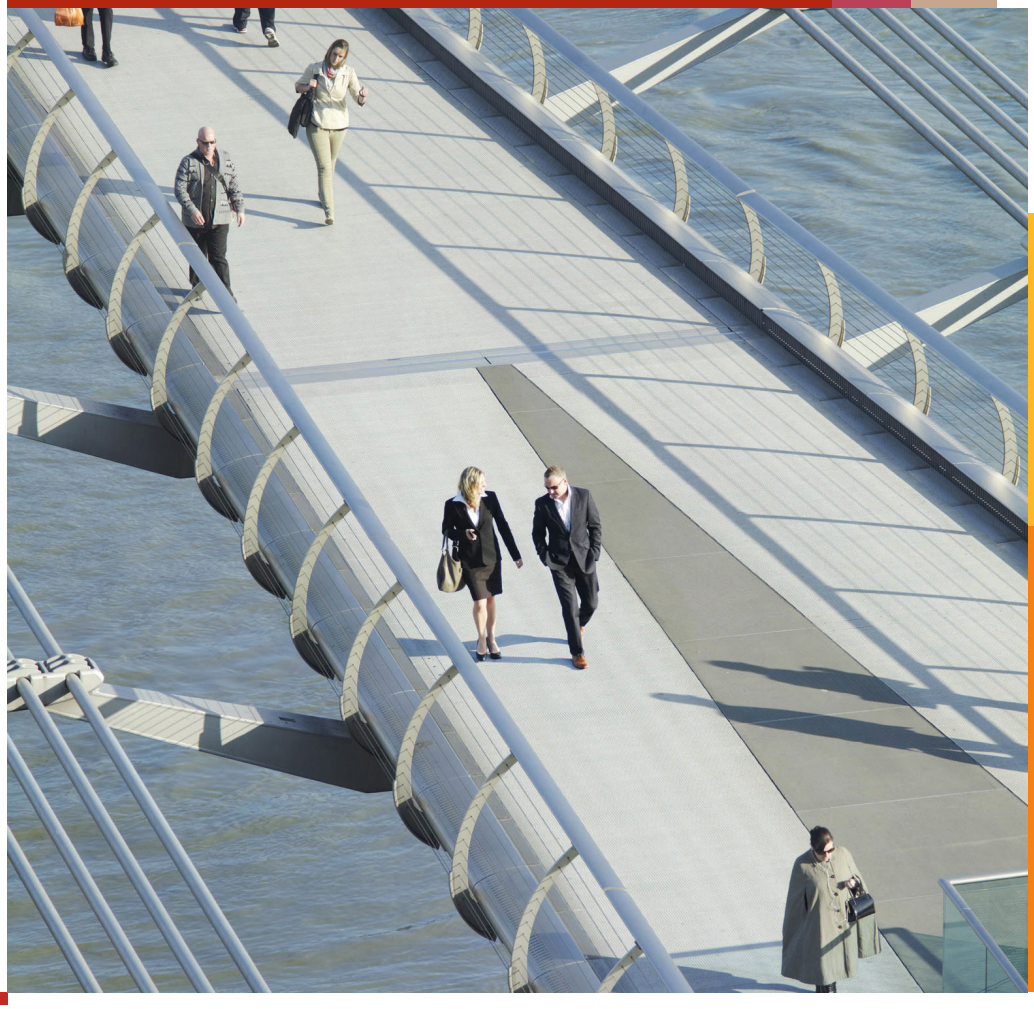
www.pwc.co.za/popi

The protection of personal information bill: The journey to implementation

November 2011



pwc

Table of contents

1. Executive summary

Open any newspaper or news website, and the chances are that you will find a report on someone's right to personal privacy being infringed, or yet another intrusion through an organisation's security systems with credit card or other financial information being stolen. With the rise of free flow of information over the internet, the popularity of social media, increasing identity theft and other intrusions on the privacy of individuals, governments world-wide have become increasingly concerned with the purposes for which organisations collect personal information, why they keep it, and how they protect it. The position in South Africa is no different, and consumers in South Africa should be welcoming the impending Protection of Personal Information Bill (PoPI or the Bill).

Although there are some disadvantages in lagging behind other countries in adopting privacy legislation, one major advantage is that the South African legislators have been able to draw on the models developed and experience acquired in other countries, selecting the best of the best for our privacy legislation. The challenge for organisations, however, is that complying with the requirements of the PoPI Bill is going to have a significant impact on the way they do business. In our discussions with our PwC subject matter experts on privacy in different jurisdictions, the opinion throughout has been that the PoPI Bill is the most comprehensive piece of privacy legislation in the world at the moment, and the burden of complying with it is going to be a difficult one, particularly for small to medium businesses. For organisations with complex business processes who gather multiple types of personal information, the road to compliance is going to be much longer and more challenging. Regardless of the size of the organisation, boards and management need to regard becoming compliant with the Bill as being high on their agendas, and they should be starting their privacy programmes as soon as possible.

The purpose of this white paper is two-fold. We would like to draw attention to some of the potential challenges we have noted in the Bill, as well as to aspects of the Bill that we believe need to be given further clarity, either through changing the language used in the Bill, or through providing guidance in the form of Regulations or other guidance documents. We have surveyed a selection of organisations in South Africa to gather their views on various aspects of the Bill, and it is clear from the responses that we have received that there are some areas in the Bill that should be clarified through the Regulations. As organisations begin their privacy programmes, some areas will start to be viewed as standard business practice, which will further provide meaning to some of the more vague aspects. The second purpose for this white paper is to share with organisations and the Technical Committee responsible for drafting the Bill some of the challenges that are likely to be faced when it comes to operationalising the Bill's requirements. A particularly noteworthy result from our survey is that many organisations face a long journey to becoming compliant with the Bill's requirements. Some of the larger financial institutions and telecommunications organisations have begun with their privacy programmes and a few are relatively advanced, but even these organisations are concerned that they may not be able to complete their programmes in time for the deadline for compliance. The lack of readiness is a major concern, and those organisations who have yet to begin their journey are likely to find themselves facing some unexpected obstacles in the road. The key message for all organisations is that you need to start your compliance process immediately.

2. Research for this white paper

In preparing this white paper, we surveyed selected organisations, who participated from August to October 2011 either by face to face interview, or through completing a questionnaire. The sectors represented include:

- Financial services;
- Public sector;
- Entertainment and gaming;
- Telecommunications;
- Retail;
- Manufacturing; and
- Agriculture.

We also consulted with our PwC colleagues in other jurisdictions who are subject matter experts on privacy in their countries, and included their views in this white paper.

This white paper is based on the draft Protection of Personal Information Bill dated 26 October 2011.

3. Purpose of the Bill

Rampant developments in information and communication technologies, globalisation, and the pursuance of electronic trade across the world have afforded information a strategic value. Moreover, information that is able to profile or identify a person or their interests offers added strategic value as organisations compete for the attention of consumers. Over time, individual rights of privacy and confidentiality have become more and more neglected, giving way to less than acceptable information management practices and rising identity theft, fraud, and other harm stemming from the unauthorised use of an individual's personal information. The constitutional right to privacy in section 14 of the Bill of Rights of the South African Constitution has to date been a largely inaccessible right.

The PoPI Bill is aimed at giving effect to South African citizens' constitutional right to privacy. The Bill achieves this through:

- Providing for the rights of data subjects with regard to their ability to protect their personal information as it is processed by public or private bodies, as well as giving data subjects remedies they can use should those rights be infringed.
- Providing a framework that sets out the minimum conditions that must be met when personal information is processed by organisations, whether they are public or private.
- Establishing an Information Protection Regulator, whose primary purposes will be to promote awareness of the rights of data subjects when it comes to protecting their personal information, as well as enforcing the requirements of the Bill.

The Bill arises from international developments with regard to data protection regulation around the globe. For South Africa to continue trading effectively with other countries, regulation such as this is essential. Consequently, the purpose of the legislation is two-fold, enhancing local privacy regulation as well as prescribing data protection practices in South Africa that are harmonised with international practices.

Drawing from the detail in the Bill, it emerges that the Bill is cognisant of two stark realities of privacy – while privacy is a theme that permeates global society and business endeavour, at the same time variations in industry data protection practices must be accommodated in the regulation of privacy. As a result, the Bill includes conditions for how personal information is shared with third parties (both within South Africa and outside its borders). It also gives authority to industry codes of conduct that will expand and clarify the data protection landscape of unique industries, taking into account the sometimes unique requirements of industries such as healthcare or financial services.

Finally, the Bill pursues a balanced approach to the protection of personal information, mandating due regard for the justifiable limitations of the right to privacy, the need to secure the interests of free flow of information and managing the tensions between the rights of access to information and protection of personal information.

4. Analysis of the conditions for processing

The 8 conditions of the Bill are closely aligned with the principles of data protection that have emerged in the international privacy regulatory setting. These principles are:

1. **Accountability**
   - The responsible party to ensure conditions for lawful processing
2. **Processing limitation**
   - Lawfulness of processing
   - Right to privacy
   - Consent, justification and objection
   - Collection directly from the data subject
3. **Purpose specification**
   - Collection for a specific purpose
   - Appropriate retention of records
4. **Further processing limitation**
   - Further processing to be compatible with the purpose of collection
5. **Information quality**
   - Ensuring quality of information
6. **Openness**
   - Notification to the Regulator
   - Notification to the data subject when collecting personal information
7. **Security safeguards**
   - Security measures on integrity of personal information
   - Information only to be processed by an operator or person acting under authority
   - Security measures regarding information processed by operator
   - Notification of security compromises
8. **Data subject participation**
   - Access to personal information
   - Correction of personal information
   - The manner of access

Historically, the Organization for Economic Cooperation and Development (OECD) compiled "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data". The recommendations contained seven data protection principles for the governance of personal information. These included several principles that correspond with the conditions contained in the PoPI Bill, including, inter alia:

- Purpose specification: the information is only to be used for a specified purpose;
- Security: personal information is to be kept secure to mitigate security incidents that result in unauthorised use of the information;
- Access: provision is made for data subjects to be able access and correct their information; and
- Accountability: collectors of the information are to be held accountable for their data protection practices and failures.

Further to the OECD recommendations, data protection regulation has emerged prominently in Europe and the principles of data protection contained in the European Union's Data Protection Directive remain aligned with the OECD principles which in turn correspond largely with those set out in the Bill. This general approach is also prevalent in the UK and Hong Kong.

In contrast to the general approach, the United States however has opted for an industry specific "sectoral" data protection regulatory approach. The regulation includes legislation, and self regulation. Whilst the US does not have a single data protection law, legislation is linked to the needs of industry and circumstance (e.g. the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act and the 2010 Massachusetts Data Privacy Regulations).

In developing South Africa's legislation, the South African Law Reform Commission looked at the approaches taken primarily in Canada, the European Union, the United Kingdom and the Asia-Pacific region (which includes Australia). In addition to these, the influence of other countries' legislation can also be seen, such as the United States. Thus, South Africa's approach may be described as a hybrid of the pure regulation and the self regulation approaches. The Bill provides for industry codes of conduct that will offer a measure of self regulation of data protection further to the information protection principles.

5. Conditions for processing of information by third parties

Third parties outside South Africa

The Bill establishes requirements for the transfer of personal information to a third party outside South Africa. The responsible party must for instance evaluate whether the third party recipient country's laws are substantially similar to and serve the same purpose as the PoPI Bill, or the third party is subject to a code of conduct that provides adequate protection of the personal information received.

Failing which, the responsible party must show that (i) the data subject has consented to the transfer; (ii) the relevant transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or (iv) the transfer is otherwise for the benefit of the data subject, subject to certain conditions.

The diagram below exhibits the conditions for transferring personal information outside of South Africa. In order to transfer information outside South Africa, at least one of these conditions must be met:

- **A** The foreign organisation is subject to a law, contract or code that offers adequate data protection to data subjects (both in terms of SA principles and the conditions of any further transfer by the organisation of the data subject's information to another cross border party)
- **B** The data subject provides consent to the transfer
- **C** The transfer is necessary for the performance of a contract between the South African organsiation and the data subject (or pre-contract procedures at the data subject's request)
- **D** The transfer is necessary for the performance of a contract between a South African organisation and a foreign organisation in the interest of the data subject
- **E** The transfer benefits the data subject (consent was not obtained but would have been obtained if practicable)

Internationally there have been several debates surrounding such conditions, particularly whether such an approach is overly cumbersome or produces adverse impact on international trade. Locally the practical challenges to enforcing this section are likely to be a matter of inquiry by the Regulator.

Further complications faced by South African organisations concern those relating to cloud computing. Many organisations are considering cloud computing for a number of reasons, but when it comes to the conditions for trans-border flows of information, the cloud computing model provides some challenges. Organisations will need to consider:

- Where the data is being held, in other words, where the servers are physically located. If the servers are in a jurisdiction that does not have similar privacy laws, transacting with the organisation providing the cloud computing services may be problematic, unless the South African organisation is able to draw up a contract with the provider that includes requirements similar to those of the PoPI Bill.

- The Bill requires the responsible party to ensure that there is a "reasonable" level of security over the personal information processed. This does not only refer to the storage of the information, but also its transmission. Therefore, organisations considering cloud computing will also need to consider how the data will be encrypted so that even if it is intercepted during transmission, the interceptor will be unable to access it.

- The service provider will need to be able to provide a level of assurance to the South African organisation that unauthorised persons cannot access the personal information processed by the organisation. This may take the form of, for example, an independent report indicating that the service provider has adequate security measures in place.

Third parties within South Africa

Many organisations in South Africa choose to outsource certain aspects of the processing of personal information to third parties. In such circumstances, organisations need to bear in mind that they still remain the "responsible party", regardless of who is processing the information. While the onus is on the operator to comply with certain requirements laid out by the Bill, oversight of the operator's activities remains with the responsible party.

A particular difficulty is the one faced by organisations whose business model revolves around databases of contact information for the purposes of marketing various products and services. This amounts to "further processing" as defined by the PoPI Bill, and we foresee that this may be the subject of challenges in the courts.

6. Implementation considerations

From the perspective of a Privacy Officer, looking to implement the current (as of this writing) draft of the Bill, we can anticipate a number of challenges. Below we have described some of the challenges as we see them, together with our suggestions of how organisations might go about handling them.

Broad scope of definition of personal information

A key challenge associated with the definition of "personal information" is the extraordinarily broad scope of the definition, the varied nature of the data elements (alpha-numeric characters, text, images, biological material, etc.), and the unstructured nature of some of the data elements (such as images and free text, correspondence, and "views or opinions"). For a Privacy Officer, determining the scope of the organisation's obligations under the Bill, and being able to articulate that scope in a clearly-definable way to one's colleagues throughout the organisation, is extremely important for an effective privacy program.

Recommendation for organisations

Organisations should establish criteria to more specifically identify personal information. For example, in other jurisdictions, the data elements are more explicitly defined, such as requiring a person's name in conjunction with certain other specified information. The Bill currently defines personal information as that relating to an identifiable living natural person, and where applicable an identifiable existing juristic person, including but not limited to the elements listed. Again, in other jurisdictions, where a similarly broad definition exists, the view is taken that any of the elements, in and of themselves, constitute personal information. Organisations will have clarify for themselves which information is considered personal information, whether in conjunction with other elements or not, and under what circumstances. Our understanding of the Bill is that information is personal to the extent that it is able to identify a person, but given that it is possible to come to a different conclusion, it is essential that organisations obtain clarity on this point.

Unstructured information or material, such as images of documents, photos, videos, and paper records, should be stored in designated, secured areas. Alternatively, organisations will need to be extremely disciplined with data classification applied to unstructured data. In developing their privacy programmes, organisations will need to take such information into account and create business processes for managing information of this sort throughout its lifecycle, from the time it is collected or created, used and through to its ultimate destruction.

Definition of personal information relating to living persons

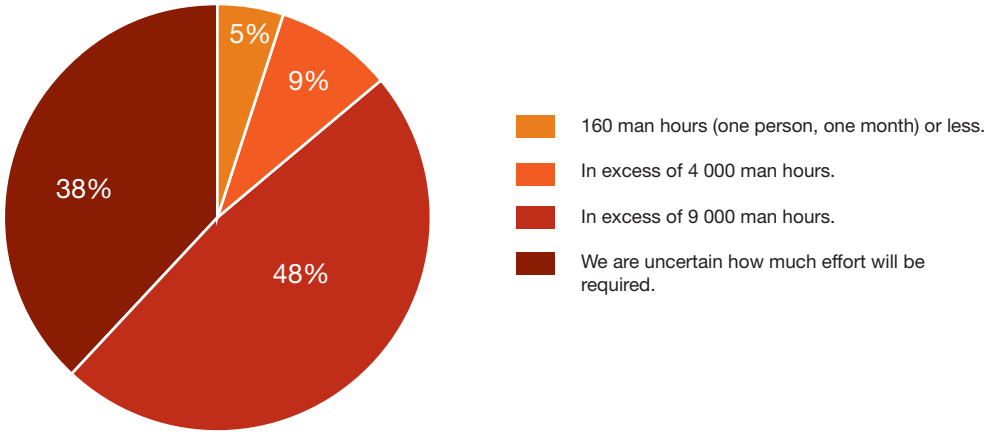
Next, we can direct our attention to the definitions of terms in the Bill. The definition of "personal information" refers to a "living, natural person", which means that as soon as someone dies, their information is no longer safeguarded. While this might provide some relief to some organisations, it is concerning with regards to one of the primary purposes of the Bill, which is to instantiate our constitutional right to privacy.

Recommendation for organisations

This issue would require correction by the legislature; however, in order for organisations to comply with the purposes of the Bill, they should voluntarily adopt periods of time in which to continue to safeguard the information of deceased individuals. These periods would likely vary, based on the sensitivity of the information, and could be included in industry codes of conduct.

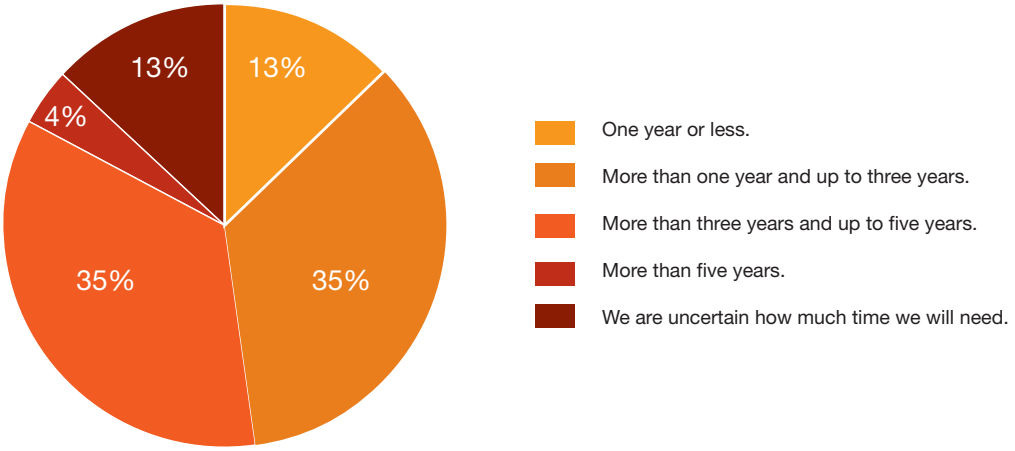
Level of effort required

Our research with organisations in South Africa has shown that many organisations are unsure of the level of effort that will be required of them to comply with the Bill, with others estimating that a considerable amount of work will be needed to in order to become compliant.



At the time of responding to this questionnaire, how much effort do you think your organisation will need to put into becoming compliant with the requirements of the Bill?

Many organisations are also anticipating that becoming compliant with the Bill is going to require a number of years, with the majority believing that they will need more than one year to become compliant. Our experience with our clients both locally and globally shows that compliance can take a great deal longer than one year for larger organisations.



At the time of responding to this questionnaire, how long do you think your organisation will need to become compliant with the requirements of the Bill?

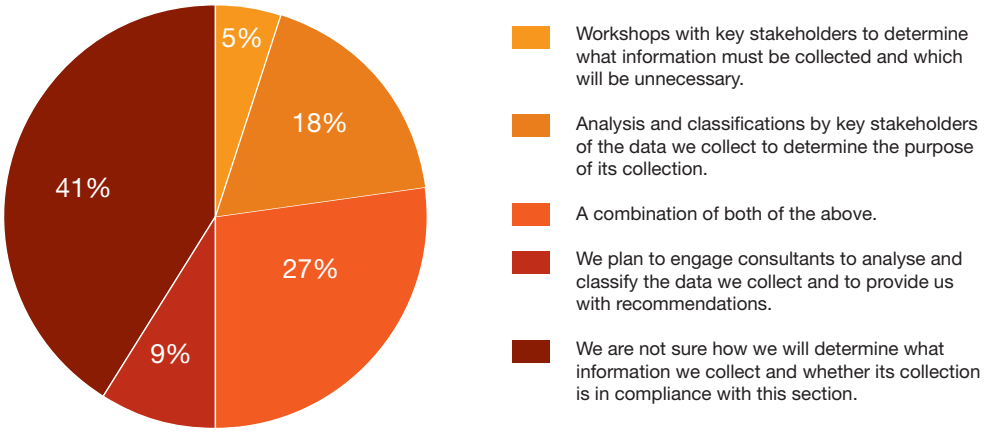
Recommendation for organisations

When the data protection laws came into effect in the United Kingdom, organisations were given three years to work towards compliance. During that time, the Information Commissioner worked with affected organisations to educate and inform, without enforcing the requirements of the Data Protection Act at that stage. In the United States, most organisations handling health-related information were given two years to become compliant with the requirements of HIPAA, with smaller organisations being given three. The experience in these countries demonstrates that given the extent of the changes required not only to systems and processes, but also to the mindset of employees, it may be somewhat impractical for the legislature to expect South African organisations to become compliant in just one year.

While we hope that our white paper will sensitise the legislature to the fact that compliance with the Bill is not likely to be a task that can be completed within a short space of time, at the same time we advise that organisations should not expect that there will be an extension to the one year that has been allowed for becoming compliant in the current draft of the Bill, and should not develop their programmes based on the expectation of an extension. We are also aware that many organisations are currently adopting a "wait and see" approach, arguing that there may be changes to the draft Bill before it is enacted. We noted that there were no significant changes to the conditions that organisations must comply with in the last two drafts of the Bill (namely February 2011 and October 2011), and based on the latest draft, we believe that the legislation is close to finalisation. We therefore believe that if organisations begin acting on the present draft of the Bill as if it were law, it is unlikely that they will have to make considerable changes to their programmes to accommodate further amendments to the legislation. With this in mind and the fact that, based on experience, it will take significant time to comply we strongly advise that organisations begin their privacy compliance programmes as a matter of urgency.

The minimality requirement

One of the principles of the Bill is that organisations should collect only the minimum information required, and should not collect any excessive information. The challenge that many organisations face is that they are not only unsure of what personal information is being collected, but they are also unsure of whether the personal information they are collecting is excessive.



At the time of completing this questionnaire, has your organisation considered how you will ensure that the information your organisation collects will be in compliance with this principle? That is, collecting only adequate and relevant information or only that information that is objectively necessary for the completion of the transaction.

Recommendation for organisations

An important step in an organisation's journey to compliance will be determining what information is collected, and whether it is absolutely necessary that it is collected. As can be seen from the above, organisations are taking a variety of means to determine this. Regardless of how each organisation goes about determining what information is collected, the question that must be asked at all stages and at all levels within the organisation is: "Why are we collecting this?" If there is no clear purpose for collecting a particular data element, then it should not be collected. The less personal information an organisation collects, the less effort will be required to protect it.

In our experience, we have seen that using a combination of interviews and questionnaires to determine what personal information is collected is most effective. Questionnaires allow for quantitative measurements, while interviews or workshops provide the qualitative background as to why certain information is collected.

Pre-emption provisions

The "pre-emption" provisions of the Bill in section 3, which state that any other legislation that is stricter than the Bill must still apply mean that a Privacy Officer cannot rely solely on the Bill for the development of their privacy program. Organisations need consider the requirements of legislation such as the Consumer Protection Act, the Promotion of Access to Information Act, the Companies Act, to name just a few of the other pieces of legislation that make up the South African regulatory universe. Multi-national organisations who are subject to privacy legislation from other jurisdictions will also need to factor the requirements of those jurisdictions into their privacy programmes.

Recommendation for organisations

Organisations should take a holistic approach to the regulatory universe, and consult with legal advisors to ensure that all applicable privacy legislation is contemplated, and apparent conflicts between such legislation are interpreted and resolved within organisational policy.

Clarity of terminology

In a number of key areas, strongly subjective terminology is used in the Bill, such as "reasonable", "unnecessarily", "legitimate interests", and "reasonably practicable". Given that privacy is such an inherently subjective notion, and that one cannot predict how the Regulator will interpret these subjective terms, it is difficult for organisations to establish policies and train their staff.

Recommendation for organisations

Organisations should determine for themselves what the terminology means and how it will impact them, and look to the purposes of the Bill for guidance. They can also research case law and enforcement actions in other jurisdictions to determine how the Regulator may interpret such provisions. Having done this, organisations can then develop their own internal policies and information handling controls with guidance in line with the sensitivity of the personal information they process, the risks involved and the consumer base expectations. Organisations can then develop employee training to integrate the terms in daily operations. They should additionally clarify the subjective terms through industry codes of conduct defining and applying standards relative to the industry and technological standards relative to the industry.

Communicating the uses of personal information

Section 17 of the current draft of the Bill requires organisations to explain to a data subject what his/ her information is being used for, but given the many purposes for which organisations use personal information once it has been collected, how will this be meaningfully communicated to the data subject at the time of collection?

Recommendation for organisations

Organisations will have to examine their data flows quite carefully, in order to determine whether to create a single, large privacy notice for the entire organisation (which runs the risk of not being helpful to the data subject and therefore deemed non-compliant by the Regulator), or creating specialised privacy notices for different areas of the organisation.

The purpose of this provision is primarily to ensure that the data subject is aware of the purpose of the processing of their personal information. As with the content of contracts, organisations will be measured not only by whether a statement that informs the data subject is in place but on the quality of the communication. The statements should be clear, should not be vague or ambiguous. Questions as to language of communication and literacy of data subjects may be raised as future inquiries.

The uses of personal information

The Bill requires that if information is collected for a specific purpose, it cannot then be used for a different purpose. For example, if a customer's mobile phone number is collected by an organisation as part of completing a transaction, the organisation cannot then use that mobile phone number to send the customer text messages to promote the organisation's goods or services, as that would then be a change from the purpose for which it was originally collected.

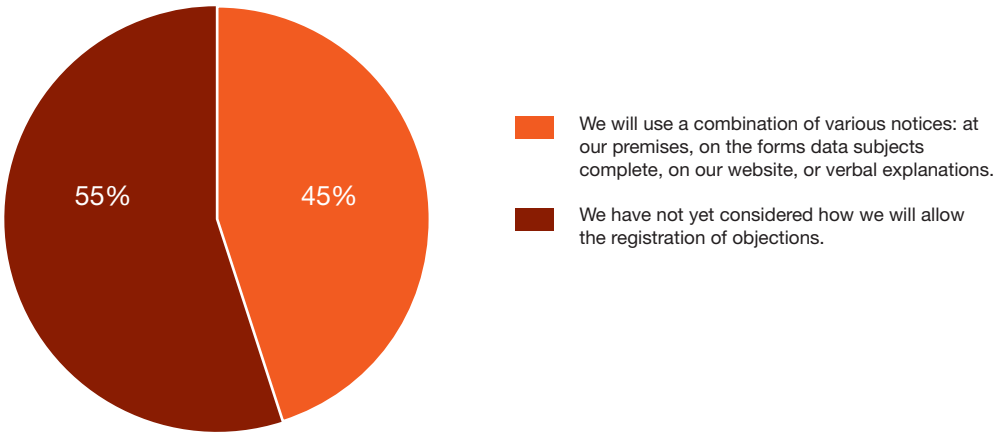
Recommendation for organisations

In developing privacy programmes, organisations will need to consider the processes around collection of personal information and how the purpose of collection is identified. In developing processes, the organisation will need to bear in mind the life cycle of data, the data elements being collected and most importantly, when personal information will need to be destroyed as it is no longer needed. Training of employees will be essential, as the best-designed privacy programme is likely to fail if employees do not understand their responsibilities when it comes to the handling of personal information. Organisations will have to have a holistic approach to purpose specification and management within the organisation and consider automating some of the processes to minimise usages of personal information for other purposes. (Bear in mind, however, the challenge associated with objections, below.)

The right to object to processing of personal information

Individuals have the right to object to the processing of their information. How will this objection be honoured throughout the entire organisation?

Our research has shown that many organisations are currently unsure how they will handle objections to the processing of personal information.



At the time of completing this questionnaire, has your organisation considered how you will allow data subjects other than employees to register their objections to the processing of personal information?

Recommendation for organisations

Experience in other countries has shown that the majority of complaints regarding the handling of personal information are based on the data subject's perceptions. Once these perceptions have been changed, the complaint is easily resolved. This underscores the reality that more often than not it is the way that the organisation's employees manage complaints and objections that will ultimately determine whether the affected data subject registers a formal complaint with the Regulator. As has already been mentioned, training of employees will be essential, especially those who are customer-facing, such as call centre agents or front-desk agents. Organisations will need to implement dispute resolution procedures to provide for and efficiently manage objections to the use of personal information.

This is not to say that all objections will simply be a matter of discussing them with the data subjects concerned and placation of the data subjects. There will be other objections that indicate that there are problems within the systems and processes, and organisations will need to develop objection-handling processes that will allow the organisation to determine the cause of the problem and resolve it to prevent further occurrences. They will have to develop mechanisms to track and check for objections in all their business processes at key points. Organisations also need to bear in mind that the Regulator may insist on evidence of how the objection has been resolved, so processes will need to take this into account as well.

Access to personal information

Section 22 of the Bill implies that data subjects will be able to ask organisations whether the organisation stores or processes any of their personal information, and can submit a request to have that information deleted. Most personal information is spread throughout multiple disparate systems (both paper and electronic) within an organisation. How will organisations be able to identify where all the information is located?

Recommendation for organisations

As far as is practically possible, organisations should normalise their electronic information to ensure that it is stored the minimum number of times across applications, databases, end user applications, third parties and in various other electronic or paper formats. The quality of personal information can be questioned if it is spread across systems. Wherever feasible, organisations will have to ensure that a single view of customer records is possible and that the information is consistent across the organisation. Records management systems will need to be established for paper and electronic records. However, normalisation may only be possible for new systems that are in development. It is therefore important that organisations review their system development processes and change management processes to ensure that they include considerations for the requirements of the Bill.

For older legacy systems where normalisation may be difficult, it would be wise to determine what data elements are being stored in those systems, and ensure that appropriate protection is in place.

Section 22 gives additional weight to the existing requirements of the Promotion of Access to Information Act, in terms of which organisations must compile a manual detailing the procedures for gaining access to information. Over and above this, organisations will need to engage in data classification in order to distinguish personal information from other information, and to further distinguish "special personal information", the processing of which is covered in sections 25 to 32 of the Bill.

Outsourcing of information processing

Organisations are required to "ensure" that third parties who process personal information on their behalf also safeguard the information, and to have contractual terms in place with such parties, especially if the outsource partner is located outside of the Republic (unless they are in a jurisdiction covered by comparable legislation).

Recommendation for organisations

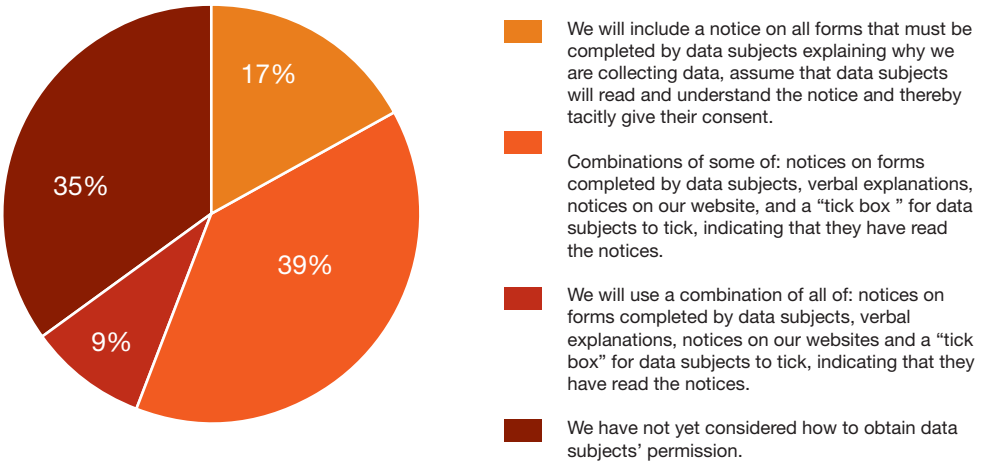
Organisations will need to thoroughly review their existing contracts, as well as identify and evaluate any trans-border data flows, and ensure that appropriate contractual language and terms and conditions are in place. In addition, organisations may need to consider requiring that their outsource providers supply them with evidence that the provider has adequate security measures in place and that these are regularly and independently evaluated. Organisations should maintain rights of auditing the practices of third party organisations in order to ensure meaningful compliance with the terms and conditions of the contracts.

Over and above this, we recommend that organisations both evaluate the operators they are currently dealing with, as well as developing processes to evaluate operators that they may contract with in the future. In evaluating operators, organisations should establish, for example:

- Whether the operator has sufficient controls (people, process and technology) in place to ensure that the personal information being processed is protected; and
- Whether the operator is in turn outsourcing the processing of personal information to yet another party.

Obtaining consent from data subjects

Section 10 requires responsible parties to obtain consent from a data subject prior to processing his information. Organisations who participated in our research have generally indicated that they will use a variety of means to obtain consent from data subjects to collect and process their information.



At the time of completing this questionnaire, have you considered how will you obtain consent from data subjects other than employees (i.e. customers, suppliers, etc.)?

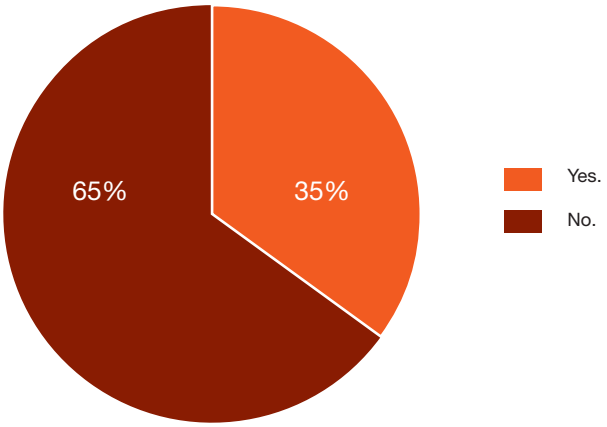
Recommendation for organisations

Obtaining consent for the processing of personal information needs to be an aspect that will be considered by organisations, depending on their business and how they transact with stakeholders. Privacy notices on websites and on contracts will need to be developed, giving data subjects clear information regarding why the entity is collecting their personal information, and what it will be used for, including the option to object if the data subject wishes to – which will need to be accompanied by appropriate processes and procedures for personnel to follow should this occur. Consent choices and objectives must be recorded in systems and data subjects who consented for specific processing options or objections must be flagged and their information excluded in the specific processing or alternative procedures will need to be defined and followed.

Deletion of information that is no longer required or that is excessive

Section 13 requires organisations to delete personal information that is no longer required, unless it needs to be retained by law, for the purposes of a contract between the organisation and the data subject or if the data subject has given his/ her consent to the information being retained. The requirement to delete information that no longer needs to be retained is an issue that many organisations are finding difficult to manage, given the multitude of legislation that requires records to be kept for differing periods of time.

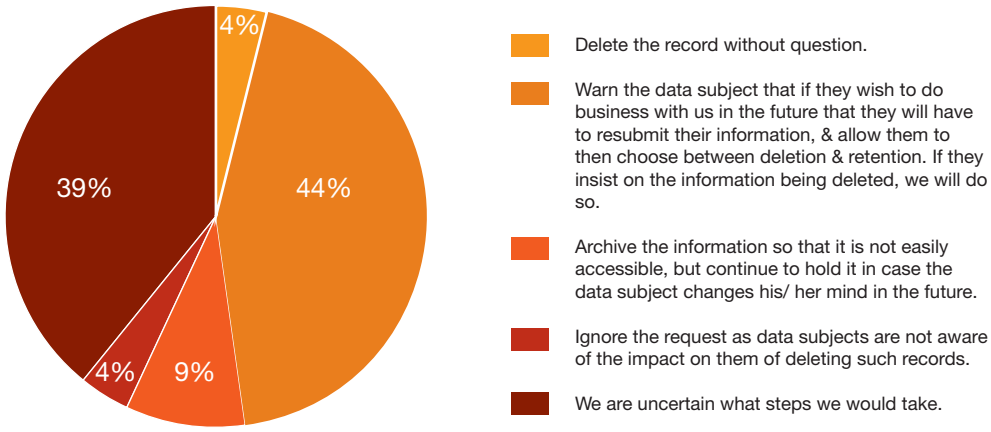
Our research with organisations shows that many entities do not yet have records retention policies that include policies regarding the deletion of personal information.



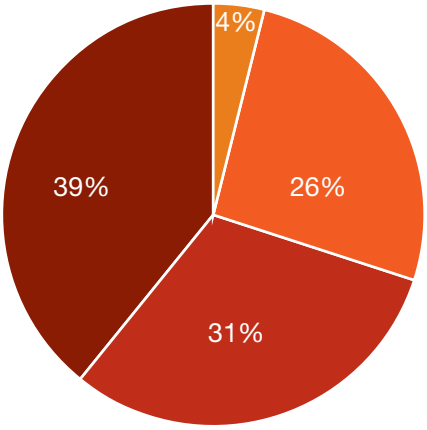
At the time of completing this questionnaire, does your company have policies and procedures governing when and how personal information is to be deleted?

In conjunction with the requirements of Section 13, Section 23 gives data subjects the right to request an organisation to delete his/ her record if the organisation is no longer authorised to retain the record or the record is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully", or to request an update to the record.

However, many entities are not yet certain how they will manage such requests.

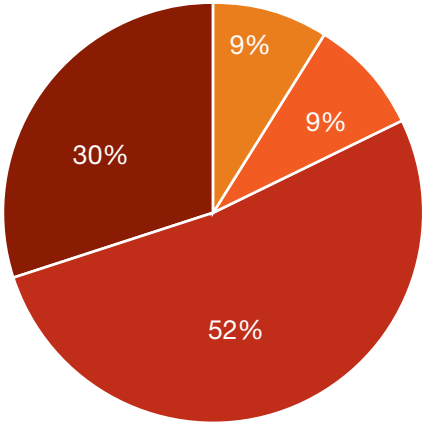


If a data subject claims that the record your organisation holds should be deleted because your organisation is no longer authorised to retain the information or for any of the other reasons listed in the Bill (inaccurate/ out of date information, etc.), what steps is your organisation likely to take?



- Delete the information the data subject claims is "excessive" without further question.
- Explain why the information is collected and what it is used for, and continue to hold all the information collected.
- Explain why the information is collected and what it is used for, but if the data subject continues to insist that the "excessive" information be deleted, do so after the data subject has been warned of the impact of deleting the information.
- We are uncertain what steps we would take.

If a data subject claims that the personal information your organisation holds is "excessive" and requests that the "excessive" information be deleted, what steps is your organisation likely to take?



- By completing a secure form on our website.
- By completing a paper form that can be submitted to any of our branches/offices.
- Any of: completing a form on our website, calling our call centre, completing a form to be submitted at one of our branches/ offices, or sending us a fax.
- We have not yet determined what process data subjects should follow to update their records.

If a data subject requests an update to the records your company holds about him/ her, in what manner will you ask for the updated information?

Recommendation for organisations

Processes that organisations will need to consider as part of their privacy programmes will include those regarding allowing data subjects to update their information, as well as how to handle requests from data subjects to delete their personal information. In addition organisations will have to ensure that their Records Management Policy details the retention periods of the various personal information categories with related processes and mechanisms to destroy it in all formats once the retention period is met. These policies will need to take a holistic approach to records retention that takes into account the multitude of legislation that makes reference to records retention periods. In developing a policy regarding update of information by data subjects and the deletion of such information once it is no longer needed, organisations need to consider the following, amongst others:

- Back-up tapes;
- Information stored off-site for disaster recovery purposes;
- Spreadsheets of information extracted onto individual laptops or PC's;
- Data warehouses;
- Footage from closed circuit cameras.

Systems that inadvertently store information will also need to be more carefully managed. Such systems may include records of visitor details to the organisation's premises, as a simple example.

"De-identification" of personal information

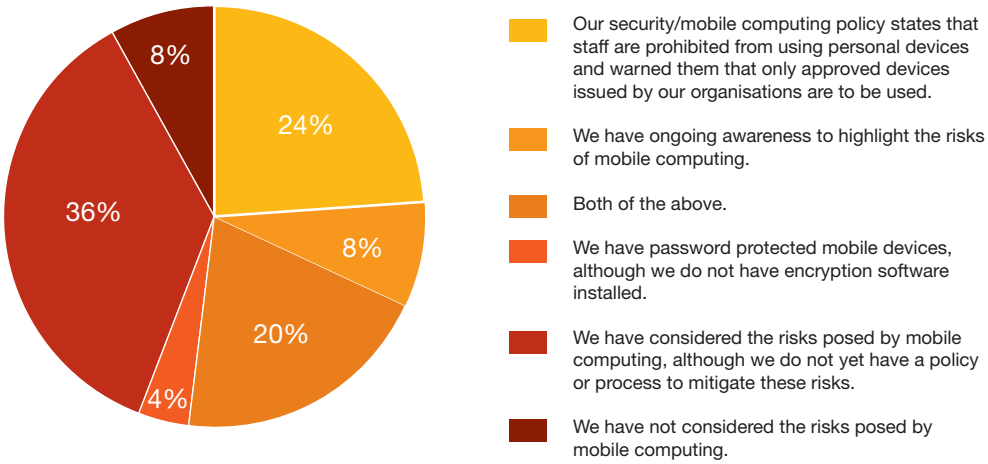
Another definition that is likely to pose challenges is "de-identify". Section 4 of the Bill excludes information "that has been de-identified to the extent that it cannot be re-identified again", using any "reasonably foreseeable method". However, in other jurisdictions there have been several well-publicised reports of re-identification of individuals within large data sets using publicly-available information. As a result, organisations may find it challenging to use de-identification as an effective business mechanism. It remains to be seen whether the South African Regulator will view organisations as having been negligent if information is re-identified using publicly-available information.

Recommendation for organisations

Organisations will need to familiarise themselves with the various techniques available for de-identification. They will also need to implement a re-identification risk assessment for each situation. The outcome of the risk assessment will determine whether de-identification is acceptable, given the circumstances, and which technique(s) to use.

Removable devices

Experience both locally and overseas indicates that the greatest number of compromises of personal information is due to the loss of removable devices, such as laptops, USB memory sticks, PDA's, etc. Paper records have also proved problematic, as many of the more recent compromises relate to personal information stored on paper that was either deliberately or inadvertently removed from the organisation's premises, with inadequate precautions then being taken to protect it. However, many organisations in South Africa, while aware of the risks both from a security and privacy perspective, have not yet determined how to address this risk.



At the time of completing this questionnaire, has your organisation implemented any special security safeguards for removable computing devices (e.g. laptops, USB flash drives/ memory sticks, external hard drives, PDA's)?

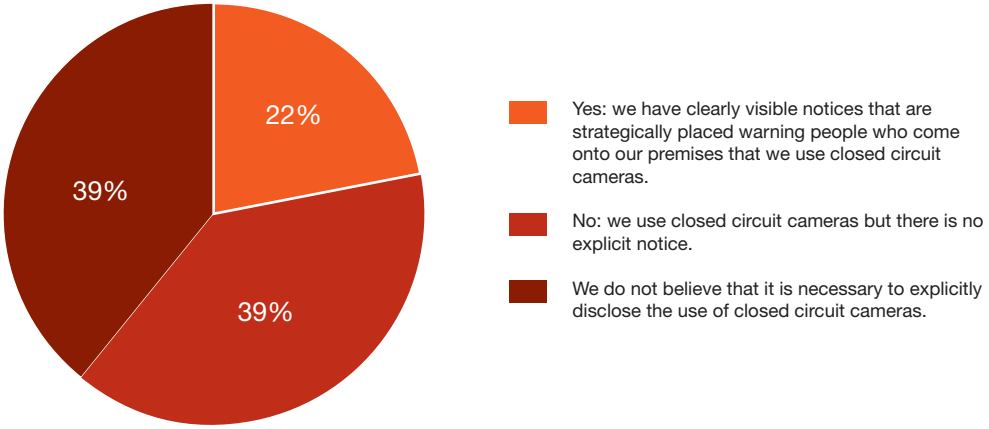
Recommendation for organisations

Addressing the risks of mobile computing is essential in developing a comprehensive privacy programme. The answers to mitigating these risks are likely to lie in a combination of technical solutions (such as encryption software) as well as having ongoing education and awareness programmes so that staff are constantly reminded of their responsibilities when it comes to removable devices.

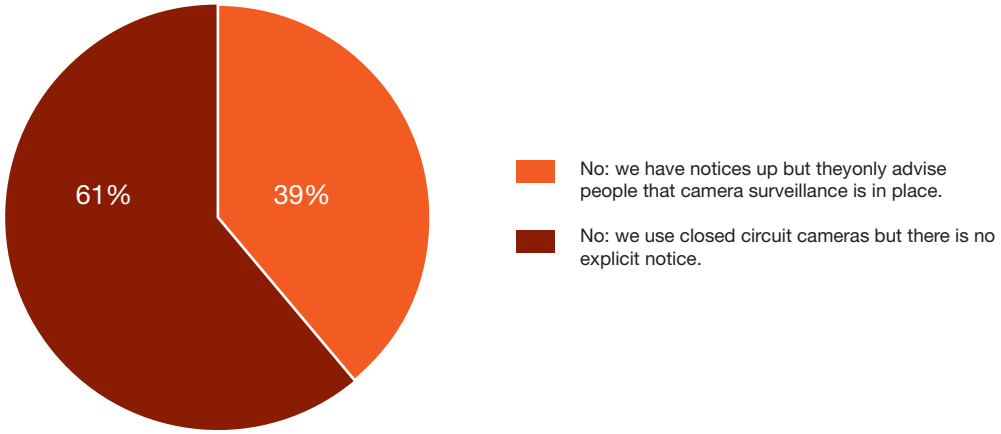
In addition to preventative measures, organisations will also need to determine what the response will be in the event of a compromise of personal information due to a removable device being lost or paper records inadvertently being left in a public place. Strategies to respond will need to include how to determine which data subjects were affected, how to manage notifications to the affected data subjects, the handling of any complaints that may arise as a result, as well as investigation of how the breach occurred in the first place. Once again, organisations need to remember that the Regulator may well demand evidence of how the compromise was responded to, and therefore documentation of the actions taken will be important.

Closed circuit cameras

One aspect that many organisations have not considered are the privacy notices that will be required if they use closed circuit cameras. The responses to our survey indicate that this is generally something that many organisations have not yet considered.



At the time of completing this questionnaire, does your organisation disclose to stakeholders (e.g. customers, suppliers, employees, visitors, etc.) that they are being recorded by closed circuit cameras?



At the time of completing this questionnaire, if your organisation does disclose to stakeholders that they are being recorded by closed circuit cameras, does the disclosure also include information regarding what is done with the video surveillance footage?

Recommendation for organisations

As the definition of "records" extends to photographs and video footage, organisations will need to determine whether the notices they have up (if they have them up) will be sufficient for the purposes of the Bill. In the long term organisations will need to seek guidance from the Regulator as to the parameters on balancing the rights of the organisation vis-à-vis the rights of the data subject. In some cases they may also need to take into account other legislation that requires such surveillance.

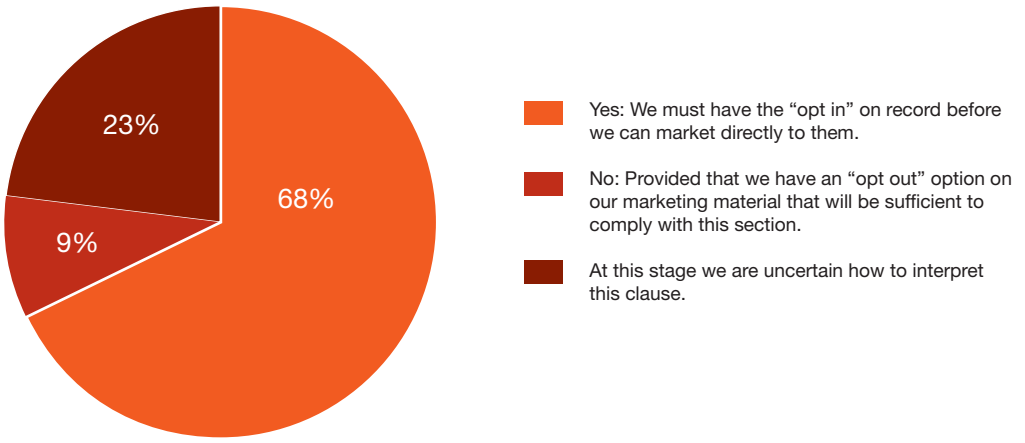
Over and above providing notices regarding camera surveillance, organisations will need to include in their policies who will be permitted to access such information, how it will be protected, and when it will be destroyed in accordance with legislative requirements.

One aspect that we believe that the banks in particular will need to discuss with the Regulator is the matter of hidden cameras in the vicinity of automated teller machines (ATM's). It is clear that such cameras are needed in the event of criminal activity around ATM's, and therefore providing notification that cameras are being used may be counter-productive. It will be important that the need for security and crime prevention is balanced against the need for the protection of personal information, and finding this balance is likely to need input from the Regulator.

Section 71 – Unsolicited electronic communication

Although s71(1) prohibits using electronic communications for direct marketing unless the data subject has given his/ her consent or is a customer of the responsible party, s71(2) permits an organisation to approach a data subject once in order to obtain their consent to be obtained. This may be interpreted by organisations as being allowed to add data subjects' contact information to mailing lists, and only removing the customers if the customer chooses to "opt out". In the case of marketing campaigns conducted by SMS, the data subject who receives the message often has to reply to the SMS to be removed from the contact list, which is generally at his/ her expense. If the data subject ignores the initial contact and does not specifically opt out from the marketing communication, the organisation may continue to send marketing communication on the assumption that "silence indicates consent".

Our research with South African organisations indicates that there is some confusion with regard to the interpretation of this particular clause, as shown below.



Does your organisation view this clause as a requirement for customers to specifically give their consent before marketing to them via email or other electronic means, i.e. customers must "opt in"?

While most organisations seem to be fairly clear that they regard this as a requirement for customers to "opt in" before they start marketing to them using electronic communications, there are still a number of organisations who seem to be uncertain as to the meaning of this requirement, or see having an "opt out" mechanism as being sufficient for compliance. In additional, anecdotal evidence from media reports and discussions on websites indicates that there are a number of people who interpret this clause as being a requirement to have an "opt out" mechanism, rather than specifically asking for permission from customers to contact them ("opt in").

Consideration for the Regulator

The uncertainty over the interpretation of this clause is likely to be an indicator that organisations may take some latitude in how they believe they should comply. We therefore recommend that greater clarity be given, either through rewording of this clause, or through the Regulations.

7. The Regulator

The governance and structure of the Regulator

The most recent version of the Bill outlines a structure for the Regulator that comprises a commission-style Regulator, rather than an individual. The commission would be comprised of relatively few individuals (currently five people), including a Chairperson. The individual members are likely to be responsible for different functions of the Regulator, such as the protection of personal information and the promotion of access to information. The current draft of the Bill calls for the members to be appointed by the President, based on recommendations from the National Assembly. The National Assembly must recommend the members via a committee comprised of members of parties represented in the National Assembly, and the nominees to the President must be approved by a majority vote of the National Assembly. Although the Regulator will be formed under the auspices of the Department of Justice and Constitutional Reform, the Regulator itself will be an independent juristic person, subject only to the Constitution and the law. This holds promise for the independence and impartiality of the Regulator.

The structure of the Regulator will be aligned with its functions (see below).

The Regulator itself, as a juristic person, would be "... independent, and is subject only to the Constitution and to the law ...". In other words, the Regulator will not be under the authority of government.

The powers and duties of the Regulator

The Bill provides for the establishment of an Information Protection Regulator with institutional characteristics common to counterpart regulators in other countries – independence, impartiality, a juristic entity comprising a sound governance structure that performs its functions and exercises its powers without fear, favour or prejudice. The duties of the Regulator shall include:

- Monitoring and enforcing compliance with the Bill (on enactment);
- Promoting understanding and acceptance of the information protection principles and objects of principles;
- Input to revisions to laws impacting the protection of personal information;
- Monitoring developments in technology in order to limit foreseeable negative impact on the protection of personal information;
- Conducting educational programmes and making public statements pertinent to protection of personal information; and
- Auditing public and private bodies' personal information practices.

As such the Regulator is tasked with administrative, supervisory and promotional roles. Day to day functions of the Regulator will include receipt and investigation of complaints, issuing of directions for compliance with the legislation and maintaining a strong research function that is able to position the adequacy of South Africa's data protection regulation against rampant opportunities for abuse of personal information.

Equally noteworthy, the Regulator is tasked with the performance of its functions and powers in accordance with this Bill and the Promotion of Access to Information Act (PAIA). The arrival of the Regulator spells therefore the arrival of due enforcement of PAIA which came into effect in 2000. Another challenge for the Regulator will be the facilitation of the interplay between rights of access to information in PAIA and protection of information in the PoPI Bill.

As with regulatory bodies in other countries, we would like to anticipate that in the beginning much of the Regulator's activity will relate to educating organisations about their responsibilities when it comes to protecting the personal information of the data subjects that they transact with. We would further anticipate that the Regulator's early activity will also include educating the general public about their rights when it comes to their personal information. While the Regulator will have wide powers, and hopefully sufficient resources to enforce the requirements of the Bill, at the end of the day the Regulator will also need to rely on the public to assist with enforcement.

8. Applying experience from other countries in South Africa

Section 1 – Definitions

The current draft of the Bill has described fairly lengthy description of what is meant by "personal information". On first reading this definition one would assume that there is little room for misinterpretation, until the reader realises that there are certain elements that are somewhat subjective. For example, one of the data elements included is that of "preferences". Does this then mean that Mrs A's preference for tea rather than coffee should be protected? We therefore submit that certain of the elements included are difficult to interpret and impractical to protect.

We reviewed the definitions of personal information from a number of other countries.

The UK Data Protection Act of 1998 defines personal data as:

> *data which relate to a living individual who can be identified —*
>
> *(a) from those data, or*
>
> *(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,*
>
> *and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual*

The Canadian Personal Information Protection and Electronic Documents Act defines personal information as:

> *information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.*

The Australian Privacy Act of 1988 defines personal information as:

> *information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

As can be seen from the above, the definitions of personal information or personal data in other countries are not as demanding as that of the current draft Bill.

Recommendation for organisations

Certain data elements are likely to prove difficult to protect, for example:

- Conscience or belief
- Personal opinions, views or preferences

As demonstrated above, other countries do not have data elements such as these included in their definitions, as it is difficult to protect information such as this. However, given South Africa's history, it is understandable that such data elements have been included both in the Constitution and in the Bill. Given the difficulty in protecting such personal information, it would therefore be preferable for organisations to rather avoid collecting such information as far as is possible. As we have said elsewhere, training of employees will be essential, and policies such as acceptable use of organisational email systems will have elevated importance.

In time, it is possible that the Regulator may come to realise that enforcing the protection of elements such as these is complex, and so in future more legislation may amend these definitions. However, at present that is only a remote possibility, so organisations will need to adhere to the Bill as it currently stands, regardless of the challenges posed.

Section 21 – Notification of security compromises

The current draft of the Bill makes it compulsory for entities who suffer a compromise of security leading to the disclosure of personal information to notify both the Regulator and the data subjects affected. The intention of this requirement is to allow data subjects to be aware of the potential compromise, and thus be able to take steps to protect themselves. Notifying the Regulator would ensure that the Regulator is able to investigate whether the organisation has taken the necessary precautions to apply reasonable security measures as well as other controls to minimise the risk of personal information being compromised.

Giving effect to this requirement has a very practical challenge: there may be occasions where an organisation is unaware of a compromise of its security, and therefore is unable to notify either the Regulator or the affected data subjects. Some examples may illustrate this point:

- Unauthorised persons deliberately access an organisation's systems in order to gain access to banking or credit card information, exploiting security vulnerabilities and avoiding detection by the organisation's security systems.

- In instances of internal fraud, the organisation may not be aware of the compromise of personal information for quite some time, unless the fraud is detected.

In both of the above examples, the organisation has complied with the requirements of the Bill, but there has been a compromise nevertheless as a result of the actions of individuals deliberately seeking to bypass the organisation's controls. In such instances, it would not be possible for the organisation to fulfil the requirements of s21.

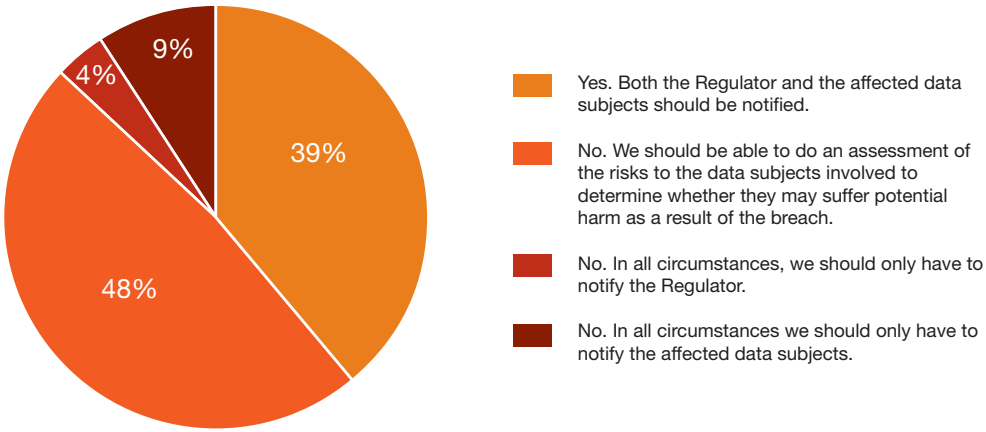
We would further argue that that there may be situations where notifying the data subjects does not have the intended effect. It is a well-known fact that consumers are bombarded with information on a daily basis, much of which goes unread, or is not acted upon. This requirement could potentially give rise to a situation where consumers are being notified on a daily basis of possible compromises of their personal information, some of which may be more serious than others. In such situations, consumers are likely to become de-sensitised to such notifications, with the result that they do not take the necessary action to protect themselves, or it becomes impractical to do so.

A review of legislation in Australia, Canada and the United Kingdom has shown that notification is currently not a mandatory requirement, although in the UK providers of public electronic communications services are required to notify the Information Commissioner's Office ("ICO") of any compromises, and sometimes individuals in certain circumstances. The ICO in the "Guidance on data security breach management" (http://www.ico.gov.uk/for_organisations/data_protection/the_guide/ principle_7.aspx) recommends making an assessment of the risks, considering, amongst other risks:

- The nature of the information disclosed;
- The number of people involved; and
- Whether notification would help the individual.

The guide specifically makes reference to "over-notification", which in this case refers to advising people who may not have been affected by the compromise.

In our survey of business in South Africa, we received mixed responses to our question regarding the notification requirement, although the majority favour assessing the risks prior to notification, as shown below.



Do you believe that if there is a breach of security at your organisation which results in the disclosure of personal information, that notification of the breach to both the Regulator and the affected data subjects should be mandatory regardless of the circumstances and the data concerned?

Recommendation for the Regulator

Based on the above, we suggest that an approach similar to that of the UK be followed, in that organisations should be required to assess the risks to individual data subjects, with the Regulator being advised of all breaches. The Regulator should then review the risk assessment, and the organisation's proposed actions to respond to the breach.

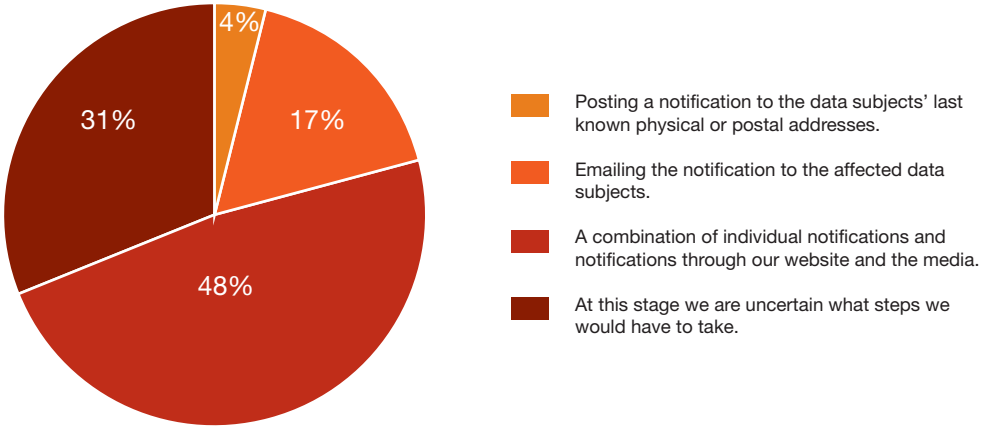
However, time is of the essence when it comes to compromise of personal information, as delays in notifying the data subjects could lead to the theft of their identities, with associated financial consequences. We therefore suggest that in the Regulations it be a requirement that once organisations have completed the risk assessment, they then immediately take the actions necessary based on the results of the risk assessment, in parallel with the notification to the Regulator. We further suggest that the Regulations should stipulate a timeframe within which the risk assessment should be complete. Given how a matter of days can make a significant impact when it comes to scenarios of identity theft, we recommend that the Regulations stipulate that the risk assessment should be completed within five working days from the time that the breach was first detected. Should the organisation's response be inadequate, the Regulator can issue a notice to force the organisation to take more appropriate actions, with administrative fines being levied in the event that the organisation does not comply.

Section 21(4) – How to notify data subjects that their data has been compromised

Canada's Office of the Privacy Commissioner of Canada ("OPC") in their guidance document "Leading by Example" (http://www.priv.gc.ca/leg_c/leading_e.cfm) recommends that notification through the media or the organisation's website only be done in the following circumstances:

- Where direct notifications could result in further harm.
- Where direct notification is prohibitive in cost.
- Where the contact information for data subjects is not known.

In our research amongst South African businesses, we found that the majority of organisations favour a combination of individual notifications and notifications through the media and/ or the organisation's website.



Should there be a breach of security at your organisation which results in the disclosure of personal information held by your organisation, what steps would your organisation consider to be reasonable to advise the affected data subjects of the breach?

Consideration for the Technical Committee

We propose that consideration be given to amending the clause to include similar requirements to those recommended by the OPC. The risk otherwise is that organisations may post notices on their websites or in the media that may not be seen by the affected data subjects, who would then not be able to take the necessary steps to protect themselves. Notification, where required according to the risk assessment discussed above, should ideally be directly to the data subjects concerned.

Section 21(5) – What information to give data subjects if their information has been compromised

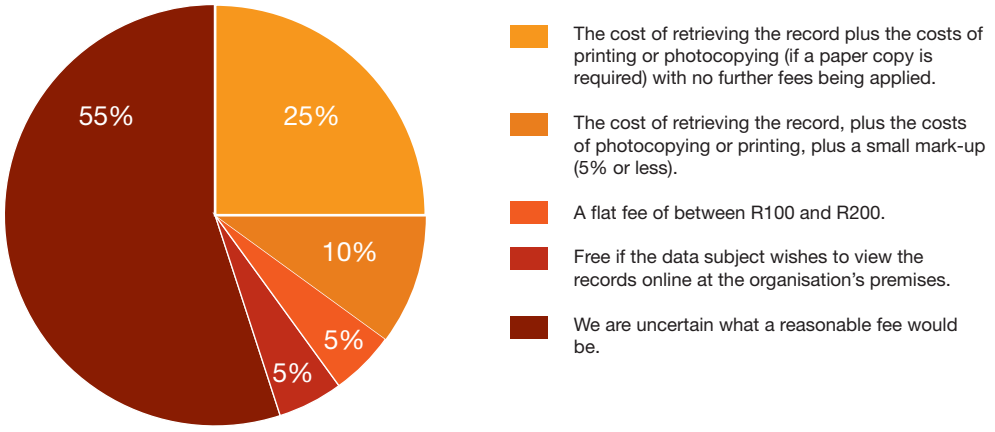
Canada, Australia and the UK have all provided detailed guidance on the information that organisations should provide to affected data subjects whose personal information may have been compromised.

Consideration for the Regulator

As is the case in other countries, we advocate that there be more specific requirements regarding the information that should be supplied to data subjects in the event that their personal information is compromised. This could be legislated through the Regulations that will accompany the Bill, but we believe that it may be more appropriate in the early days of this legislation to follow a softer approach by providing guidance to organisations on what they should disclose to affected data subjects.

Section 22 – Access to personal information

Section 22 refers to the requirement that information be provided to a data subject on request "at a prescribed fee, if any". In our view, this creates an opportunity for organisations to impose fees that are so exorbitant that the effect would be that the organisation does not comply with this provision.



What fee would your organisation consider to be a reasonable fee to give a copy of a data subject's records to him/her?

Discussions in the Technical Committee have already revealed that it can be challenging for an ordinary consumer to request information in terms of the "Promotion of Access to Information Act". This section may be used as an additional obstacle by organisations to avoid providing information to data subjects.

Consideration for the Regulator

Given the uncertainty of organisations regarding what would constitute a "reasonable fee", we recommend that there be more clarity on this section, either through the published Regulations, or through the Regulator providing guidance once the Regulator is formed. In the US HIPAA legislation reference is made to a "cost based fee". The Canadian Commissioner found in one of the complaints it investigated that the organisation concerned was charging a fee that was prohibitive, and would thus be not in the spirit of the legislation (Leading By Example, pg 48). We thus suggest that the Regulations make specific reference to a cost based fee, but bearing in mind that this may still be prohibitive for a data subject that earns a basic salary. It may therefore be wise to include a maximum fee that may be charged.

Other issues noted in the draft Bill

- Section 22 allows a data subject to request access to his/ her information held by a responsible party. However, no time limit is specified, which means that organisations may use delaying tactics in order to avoid providing this information to a data subject. We suggest that either a time period be specified in the Bill for a responsible party to deliver the requested information, or alternatively that a time period be specified in the Regulations. The time period may vary according to the industry, as in certain industries (such as banking) it may be more difficult to extract all information relating to the data subject, especially when information is archived.

- The Data Protection Act from the United Kingdom states under the seventh principle that the "data controller must take reasonable steps to ensure the reliability of any employees" so as to give effect to the principle of "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". No mention is made in the current draft of the PoPI Bill of ensuring that a responsible party ensures that their employees are reliable, in other words that they can be trusted and that they have no prior record of either fraud or non-compliance with legislative requirements. We believe that this could be a gap which may lead to a lack of compliance, and recommend that the Regulations include requirements that background checks of potential employees be conducted prior to their being employed in positions where they will be responsible for handling personal information.

- Section 34 allows for the Regulator to authorise the processing of personal information even in situations where the processing does not comply with the requirements of the PoPI Bill. In our discussions with our PwC colleagues locally and in other jurisdictions, they have all expressed concern that this section may be open to abuse, as the circumstances outlined where the Regulator may authorise such processing are quite broad in nature.

- Section 13(2) states that personal information may be retained for "historical, statistical or research purposes". We submit that this wording may be open to interpretation, and that organisations may retain personal information for 'research', which may be their own marketing research. In the United States, research refers to academic research, and we suggest that the same or similar wording be used for the PoPI Bill.

General good practices noted in other countries

Guidance documents

In most countries where there are privacy laws active, the regulator in the country has published documents to assist organisations with being compliant with the relevant laws, most of which are aimed at small to medium businesses who do not have access to the resources that larger organisations have. For example:

- Australia has published a number of information sheets on specific aspects of privacy laws to guide organisations.

- The UK has published "The Regulator's Guide to UK Data Protection".

- The Canadian OPC has published the "Privacy Guide for Small Business: The Basics". The Canadian OPC also has links to video content on their site that gives guidance to small businesses and individuals regarding their obligations and rights with respect to privacy.

All the documents are in terms that are easy to understand, and assist lay persons in understanding what their personal rights are, as well as what the requirements are of organisations.

We suggest that the South African Regulator should publish similar documents, either as the Bill is enacted or as soon as possible after the enactment. We believe that making use of social media as the Canadian OPC has done to publish videos for guidance is likely to be effective.

Given the complexity of this legislation, small businesses in particular are likely to find it difficult to understand what is required of them.

Training

In the United States and the United Kingdom, the regulators in both countries have placed heavy emphasis on the training of staff regarding the requirements of privacy legislation and what each employee's responsibility is to ensure that personal information is protected. Other countries have similar requirements.

In many instances, simply having a policy and procedures in place is insufficient. In order to ensure compliance in full, organisations need to have a training programme and on-going awareness to educate their staff on what their responsibilities are when it comes to protecting personal information. We therefore suggest that training become a requirement of the legislation, either as part of the Bill itself or as part of the Regulations, with the training in privacy being related to the employee's job function.

Given that many smaller organisations do not have access to training resources in-house, we urge the Regulator to consider running training courses on a regular basis that are aimed at small to medium size businesses. Education of employees has been demonstrated to be far more likely to result in compliance than simply instituting privacy policies and procedures. However, as the Regulator's resources are likely to be limited, one possibility is to create a panel of accredited organisations who will be permitted to deliver such training. The training should be reviewed by the Regulator to ensure that it properly addresses the requirements of the Bill.

9. Conclusion

The enactment of the PoPI Bill is going to bring a significant level of protection to individuals and organisations in South Africa with regard to how their personal information is handled. When the effects of this legislation are considered in conjunction with other legislation that has been passed in recent years, individuals will have the ability to hold organisations to account for the actions that are taken regarding personal information. Therefore, from the perspective of an individual, this legislation is welcome.

From the perspective of the organisations that will have to amend systems, processes and policies in order to comply with the legislation, however, this Bill may have a significant impact on the way that they do business. The Regulator therefore needs to take cognisance of this, especially given the heavy compliance burden that organisations already carry. As has been seen in other countries, it may initially be wise for the Regulator to focus on awareness and training of organisations, educating rather than enforcing in the beginning. However, as compliance with privacy legislation becomes a mature process, the Regulator should then move to playing more of an enforcement role, penalising those organisations that do not take the necessary steps to protect the personal information they are responsible for.

As we hope has become evident in the forgoing discussions, becoming compliant with the Bill is likely to be a long and arduous journey for many organisations. We therefore urge organisations to establish their privacy programmes soon, and make a start on their journeys. Our experience with our clients has shown that organisations soon find that there are complexities with regard to privacy internally that they had not anticipated, and thus it may take longer than anticipated to become compliant.

We would like to thank the organisations and individuals who participated in our research. They played an important role in the development of this white paper. For reasons of privacy, they are not named, but they know who they are.

10. About the PwC Privacy Team

Maintaining data privacy while keeping it protected has never been more of a challenge nor more of an imperative, particularly in view of the impending PoPI Bill.

PwC's multidisciplinary Privacy Team brings together leading global expertise and project implementation capabilities to support and guide your organisation to implement a comprehensive privacy programme scalable according to your size, needs and budget. We bring to our clients a combination of:

- Experience in delivering and implementing privacy programmes
- Expertise in legislation affecting privacy and aspects of information technology
- Expertise in IT security and how it affects privacy
- Experience in programme management and delivery of complex, multi-faceted programmes

11. Contacts

For more information, please contact:

Pierre Dalton
Director
pierre.dalton@za.pwc.com
(27) 11 797 4635

Hester Scholz
Privacy Competency Leader
hester.scholz@za.pwc.com
(27) 11 797 5899

Dr. Adele da Veiga
Senior Manager
adele.da.veiga@za.pwc.com
(27) 11 797 5343