30 JUNE 2020

POPI BUMPER SPECIAL **ALERT**

COMPILED BY CDH'S POPI SPECIALISTS

The President of the Republic of South Africa has indicated that the Protection of Personal Information Act 4 of 2013 will come into force on 1 July 2020. Due to the wide definition of personal information, the commencement of POPI will have far reaching implications for responsible parties. This Alert serves to provide you with some insight into the implications which POPI may have on you and your organisation.

FOR MORE INSIGHT INTO OUR EXPERTISE AND SERVICES

CLICK HERE

CDH
CLIFFE DEKKER HOFMEYR

INDEX

CDH
CLIFFE DEKKER HOFMEYR

Personal Information: Four key areas to be aware of

POPI – when it becomes fully operative – will regulate the collection, storage and dissemination of personal information.

Personal information is everywhere. It is almost impossible to do business these days without collecting personal information of customers, suppliers and employees. Personal information is collected in so many ways, although to an ever increasing extent, online through contact forms, email and the creation of online profiles. The Protection of Personal Information Act of 2013 (POPI) – when it becomes fully operative – will regulate the collection, storage and dissemination of personal information. Businesses must ensure that the necessary consents for the collection, storage and dissemination of personal information are obtained. But first, businesses will need to be clear that what they are collecting is in fact personal information.

So, what is personal information? Personal information includes, among other things, the following:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- the e-mail address, physical address and telephone number of the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

There are four key areas of collection of personal information that businesses need to be aware of:

(1) Market research via direct marketing

Collecting personal information is big business. Understandably, businesses can profitably make use of this information to market their products or services. Many businesses undertake research as regards prospective customers by, among other things, accessing information already available in the public domain (for example, through publicly accessible social media platforms and websites) as well as obtaining contact information in respect of potential customers (for example, from a company switchboard). The personal information is then captured and stored to be used for purposes of direct marketing. The business then reaches out to these persons via personalised or mass-generated emails and/or via telephone calls. This is all personal information. Even the personal information of persons who have indicated that they do not wish to be contacted again via direct marketing is required to be stored for a certain period of time.

(2) Online

As noted, most businesses these days also collect information from their clients and customers via their websites. For example, most e-commerce stores require users to complete a profile of themselves,

Personal Information: Four key areas to be aware of...*continued*

Service level agreements are a common source of personal information that businesses collect, store and disseminate.

containing personal information. If you collect personal information from your clients or customers, make sure that they are made aware of this in clear and express terms, and make sure that you provide that they expressly consent to the collection, sharing and storage of such personal information. This can be achieved by introducing such consents into the business's online terms and conditions.

(3) Employment Agreements

A third significant source of personal information that businesses collect, store and disseminate is that of its employees and prospective employees. Employment agreements (including both permanent and fixed term employment agreements), as well as independent contractor and consultancy agreements need to have the requisite provisions in place as regards the collection, storage and dissemination of the personal information. Similarly, any application forms that are used for application purposes will need to contain similar provisions (even if the person never becomes an employee of the business).

(4) Service Level Agreements

Service level agreements (or 'SLAs') are a common source of personal information that businesses collect, store and disseminate. This will contain information about customers or third party service providers. Customer-facing service level agreements and third-party supply agreements need to have the requisite provisions in place to ensure that consent is provided to collect, store and disseminate this information.

It is critical that businesses are alive to the personal information being collected, stored and disseminated via market research, online browsing, employment agreements, customer-facing service level agreements and third party supply agreements, and ensure that the requisite approvals are in place from data subjects. The collection, storage and dissemination of all of this personal information will need to comply with the requirements of POPI.

Justine Krige

When is the further processing of personal information applicable?

Section 15 of POPI provides that in order to determine whether further processing is compatible with the purpose for which the personal information was originally collected.

The Protection of Personal Information Act 4 of 2013 (POPI) provides that personal information must be collected for a specific, explicitly defined and lawful purpose related to the function or activity of the responsible party. From this it appears that any consent obtained from a data subject should not be generic in nature but should set out details as to the purpose for which the personal information is sought and how the personal information of the data subject will be processed.

POPI defines "*processing*" as '*any operation or activity or any set of operations, whether or not by automatic means, concerning person information*'. This includes, amongst other things, the collection, recording, organisation, storage, modification or transmission of personal information. Despite this definition of "*processing*" no indication has been provided in POPI as to what the section 15 phrase "*further processing*" means. Since POPI is a new piece of legislation (only coming into force on 1 July 2020) there is no case law, at this stage, which can assist us in interpreting the phrase. However, POPI does provide that the further processing of personal information must be in accordance or compatible with the purpose for which the personal information was originally collected.

From this, it may be deduced that where a data subject provides consent to the processing of personal information for a specific expressly-defined purpose, and during the processing of such personal information it transpires that further processing (not originally envisaged and for which consent was not originally received) is required in order to fulfil the purpose that such further processing will fall within the ambit of section 15 of POPI. However, this viewpoint is yet to be tested and will, mostly likely, be expanded upon by our courts in the future.

Section 15 of POPI provides that in order to determine whether further processing is compatible with the purpose for which the personal information was originally collected. The following factors must be taken into consideration, namely:

- the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
- the nature of the information concerned;
- the consequences of the intended further processing for the data subject;
- the manner in which the information has been collected; and
- any contractual rights and obligations between the parties.

POPI further provides that where the purpose of the further processing is not compatible with the purpose for which such personal information was originally collected, further processing of such personal information may still occur where:

- the data subject consents to such further processing;
- the personal information is available in or derived from a public record or has deliberately been made public by the data subject;

CDH
CLIFFE DEKKER HOFMEYR

When is the further processing of personal information applicable?

...continued

From this it appears that where the further processing of personal information is not in accordance or compatible with the purpose for which such personal information was originally collected, the consent of the data subject to such further processing will need to be obtained.

- further processing is necessary to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences; to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue; for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or if in the interests of national security;
- the further processing of the personal information is necessary to prevent or mitigate a serious and imminent threat to public health or public safety; or the life or health of the data subject or another individual;
- the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in identifiable form; or
- the further processing of the information is in accordance with an exemption granted by the Regulator in accordance with the provisions of POPI.

It may be difficult to determine the extent of processing which needs to be undertaken by a responsible party in order to fulfil the purpose for which the personal information of the data subject was originally sought and for which such data subject originally provided consent. The provisions of POPI pertaining to the further processing of personal information appear to create an instance where the responsible party does not need to constantly revert to the data subject to obtain the relevant consent to further process the personal information, provided that the further processing is in accordance or compatible with the provisions of POPI as detailed in this article. Where it is not, the responsible party may be required to once again approach the data subject to obtain consent for further processing.

It is important to ensure from the outset that the consent you, as the responsible party, obtain from a data subject provides such data subject with enough information regarding how and what manner the provided personal information will be processed. It is also important to understand and keep in mind the instances where further processing will occur and to ensure that it is compatible with the original purpose for which the personal information was provided.

This is a difficult concept to navigate and we are happy to provide assistance with regards to the content which should be set out in your consents as well as provide you with advice as to when further processing may occur during your processing method.

Kendall Keanly

CDH
CLIFFE DEKKER HOFMEYR

Five legal tips for direct marketing

South African companies better ensure that they get their ducks in a row - whether it's direct marketing by post, telephone, email or SMS, make sure that your business doesn't cut any corners.

Direct marketing is often favoured as a popular means of product marketing, especially for start-ups looking to grow their customer base. It is, however, often also a source of irritation for many consumers as suppliers are increasingly testing the boundaries of what is allowed. Internationally, personal information data breaches are attracting heavy fines by regulators, British Airways, Facebook and Yahoo already having attracted fines in the region of US$500,000, and when the Protection of Personal Information Act (POPI) (which will regulate direct marketing via electronic communication) comes into force, regulation of direct marketing in South Africa is going to become even stricter. South African companies better ensure that they get their ducks in a row - whether it's direct marketing by post, telephone, email or SMS, make sure that your business doesn't cut any corners.

These five tips should assist.

1. Obtain consent

Ensure you have consent. Direct marketing via any form of electronic communication including automated calling machines, faxes, SMSes and email will no longer be permitted once POPI comes into force, unless the person has either given his/her consent to receive such electronic communication, or is an existing customer. Otherwise, the person's consent will be required. For this purpose, the responsible party may approach a person whose consent is required, and who has not previously withheld such consent, only once in order to request the consent of such person. If the person is an existing customer, the responsible party may only send direct marketing electronically to such person if (1) the customer's contact details were obtained in the context of a sale of a product or service; (2) for the purpose of direct marketing of similar products or services; and (3) the customer has been given a reasonable opportunity to object to the direct marketing (i) at the time the personal information was collected; and (ii) on every communication. In respect of direct marketing via telephone, post and in person, every person similarly has the right to refuse to accept the unwanted direct marketing and require the supplier to discontinue such activity.

2. Don't forget the "*unsubscribe*" option

The Consumer Protection Act (which regulates direct marketing by post and telephone) and POPI (which regulates direct marketing by electronic communication) empower consumers to block marketing communications. All electronic direct marketing communications must contain an "*unsubscribe*" option. Similarly, physical post boxes containing a direction that "*no junk mail*" will be accepted cannot be used for direct marketing. Companies are going to need to manage their customer databases a lot more effectively – where, how and when was the personal information initially obtained; whether the person is an existing customer and, if so, in respect of what products or services;

CDH
CLIFFE DEKKER HOFMEYR

Five legal tips for direct marketing

...continued

Specific days and times of days have been prescribed for direct marketing, and a supplier must not engage in any direct marketing directed to a consumer at home for any promotional purpose during a prohibited period.

whether the person has consented to receiving direct marketing; and whether the person has unsubscribed from receiving direct marketing. In particular, companies are going to need to adopt a vigilant approach in enforcing requests from consumers to discontinue any marketing activities.

3. Include the sender's details

All direct marketing communications must contain the sender's details. Any communication for the purpose of direct marketing must contain the details of the identity of the sender or the person on whose behalf the communication has been sent; and an address or other contact details to which the recipient may send a request that such communications cease.

4. Stick to permitted contact times

Stick to the permitted contact times. Specific days and times of days have been prescribed for direct marketing, and a supplier must not engage in any direct marketing directed to a consumer at home for any promotional purpose during a prohibited period. The prohibited times for contacting consumers at home (this includes via telephone, SMS or email) are as follows: Sundays or public holidays; Saturdays before 09h00 and after 13h00; and all other days between the hours of 20h00 and 08h00 the following day, except to the extent that the consumer has agreed otherwise. A direct marketer is not in breach if it has sent out the direct marketing within the period provided for even if the consumer received the direct marketing outside of the aforementioned period, but the onus to prove that the direct marketing was dispatched during the allowed period rests fully on the direct marketer.

5. Beware the "*cooling-off*" period

It is important to bear in mind that a consumer has an entitlement under the CPA to cancel a transaction resulting from any direct marketing without reason or penalty, by written notice to the supplier, within 5 days after the later of (1) the transaction was concluded; or (2) the goods were delivered to the consumer.

Justine Krige

CLIFFE DEKKER HOFMEYR

Has the role of the Information Officer changed?

With the coming into force of POPI, the role of the Information Officer has expanded.

Prior to the commencement of the Protection of Personal Information Act 4 of 2013 (POPI), the role of the Information Officer was governed by the provisions of the Promotion of Access to Information Act 2 of 2000 (PAIA). Under PAIA, the Information Officer was the individual tasked with ensuring compliance with its provisions. No process is required to be followed by a company for the appointment of an individual as an Information Officer, as the position is automatically assigned to the head of an organisation (be it the chief executive officer or otherwise).

With the coming into force of POPI, the role of the Information Officer has expanded. Their role within an organisation is now not only governed by the provisions of PAIA, but also POPI.

POPI provides that the Information Officer is responsible for, amongst other things:

- ensuring that the organisation complies with the conditions of lawful processing of personal information; and
- working with the Regulator in relation to any investigations conducted in accordance with the relevant provisions of POPI.

These responsibilities are amplified in the regulations published in terms of POPI (Regulations), which provide that an Information Officer is required to, amongst other things, ensure a compliance framework is developed, implemented, monitored and maintained; attend to a personal information impact assessment to ensure that adequate measures and standards exist within the responsible party in order to comply with the various conditions for lawful processing of personal information as contemplated in POPI; and ensure that a manual as contemplated in PAIA is developed, monitored, maintained and made available. The Information Officer is also required to ensure that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations and any codes of conduct or information obtained from the Regulator.

Although the position of the Information Officer is still an automatic appointment, the Information Officer is now required to register with the Regulator prior to taking up their duties as an Information Officer under POPI. From this it appears that although an Information Officer may continue to act in accordance with the provisions of PAIA, they will need to first register with the Regulator before attending to their duties and responsibilities under POPI. It is not clear, at this stage, what this registration process will look like or whether any proof of registration will be provided to the Information Officer as confirmation of their position as such within an organisation.

In addition to an organisation having an Information Officer, it is entitled to appoint as many deputy information officers as may be necessary to perform the duties placed on the Information Officer by the relevant legislation. From these powers

Has the role of the Information Officer changed?...*continued*

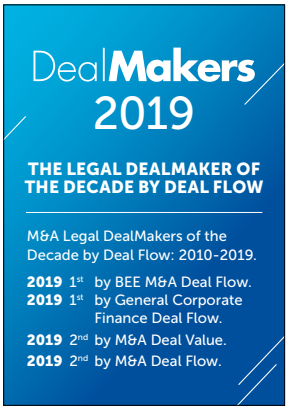
As both Acts impose strict requirements on responsible parties to ensure compliance with the provisions thereof, an organisation must carefully consider who will take the position of deputy information officer.

of delegation, there appears to be an understanding that the Information Officer may need assistance attending to all the duties required of them under the legislation.

However, as both Acts impose strict requirements on responsible parties to ensure compliance with the provisions thereof, an organisation must carefully consider who will take the position of deputy information officer. Will it be the organisation's chief information officer, the head of information technology or another individual? Selecting the right individual for this role is important because if a deputy information officer fails to perform the duties delegated to them, it could have adverse implications for not only the responsible party (as defined in POPI) but also the Information Officer.

We are happy to provide assistance with regards to any queries you may have relating to aspects of POPI, the role of the Information Officer and/or deputy information officer, the drafting of a compliance framework, attending to any personal information impact assessment; and providing you and your employees with internal POPI awareness sessions.

Kendall Keanly



CDH
CLIFFE DEKKER HOFMEYR

POPI: Questions & Answers

It is a good idea to always consult your legal adviser or the actual provisions of POPI to ensure that you are complying with your privacy obligations under POPI.

My business operates in other jurisdictions such as the European Union. If the business complies with legislation such as the European Union's General Data Protection Regulation (GDPR), does this automatically mean that it will be POPI compliant?

Despite using different terminology (e.g. POPI refers to personal information, while the GDPR refers to personal data), many of the substantial obligations set out in the GDPR are also required by POPI.

For instance, just like the GDPR, POPI requires the processing of personal information to be adequate, relevant and not excessive (i.e. minimal) in relation to the purpose for which it is processed. This means that businesses complying with the GDPR have already made some headway in POPI compliance.

However there are some discrepancies between the legislation and in some instances, POPI has more stringent provisions than the GDPR. One such instance is that personal information under POPI applies to the personal information of both living natural persons and existing juristic persons where as the GDPR is confined to only personal data about natural persons.

It is therefore a good idea to always consult your legal adviser or the actual provisions of POPI to ensure that you are complying with your privacy obligations under POPI.

What is a 'POPI Policy'?

A 'POPI Policy' is, broadly, a privacy policy which describes how an organisation collects, uses, stores, processes, and shares personal information of its data subjects.

It is important that an organisation takes its privacy obligations seriously and carefully considers the contents of its POPI Policy. Critically, no one size fits all when it comes to a privacy policy – organisations should avoid 'off the shelf' bought policies and rather tailor its POPI Policy to be applicable to its business. An organisation may require more than one POPI Policy – for internal purposes (i.e. its employees and prospective employees) and external (i.e. suppliers and services providers, on the one hand, and customers on the other).

An organisation's POPI Policy should be effectively communicated to the data subjects concerned and POPI gives data subjects the right to be notified that personal information about him, her or it is being collected. In this regard we recommend that organisations host training sessions and educate its employees on the importance of data protection and its POPI Policy. An organisations POPI Policy may be embedded on its website (where applicable) and/or included in contractual arrangements with suppliers and customers.

Key take away:

- Ensure your organisation has a privacy policy, or policies (as applicable); and
- Review your employment, customer and supplier agreement to ensure that the contracts contain data protection clauses which align to your organisations privacy policies and/or incorporate, by reference, its privacy policy.

CLIFFE DEKKER HOFMEYR

POPI: Questions & Answers*...continued*

In order to ensure that an organisation meets all its obligations – under both POPI and contract – we recommend clients have a comprehensive incident response plan.

Data breach – now what?

A 'data breach' is not defined in POPI, but it generally refers to the access or acquisition of personal information by an unauthorised person. Where a data breach occurs, there exists an obligation on the responsible party to report the breach to (i) the Information Regulator; and (ii) the affected data subject (subject to certain limitations).

The notification must be made in writing as soon as reasonably possible after the discovery of the data breach. The notification must provide the data subject with sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach.

Apart from any data breach notification obligations set out in POPI, there may be additional contractual obligations regarding what an organisation must do in the event of a data breach as set out in agreements with its suppliers, customers, or set out in its privacy policy.

Non-compliance with the obligation to notify is a breach of POPI and may, upon conviction of certain offences, lead to imprisonment, a fine, or both. To the extent that there are notification or other obligation in contract, an organisation must ensure adherence thereto to avoid a contractual breach.

In order to ensure that an organisation meets all its obligations – under both POPI and contract – we recommend clients have a comprehensive incident response plan (Incident Response Plan) or IRP). This Incident Response Plan should set out what needs to be done by the organisation in the event of a data breach, including (but not limited to) who is assigned to respond to the breach; what the internal response times are; how the organisation will communicate the breach to the Information Regulator and data subjects and any other reporting requirements (both internally and externally).

An organisation could incur costs and losses as a result of the data breach. In this regard organisations should consider purchasing tailored cyber liability insurance which covers the losses associated with data breaches or cyber-attacks. An organisations Incident Response Plan should refer to this cyber liability insurance policy as notification to its insurers, and potentially external parties, will need to occur in accordance with the IRP.

Key take away:

- Ensure that your organisation has a comprehensive Incident Response Plan;
- Ensure that, where a data breach occurs, your organisation (i) notifies the Information Regulator; and (ii) each data subject impacted by the breach (to the extent applicable). We recommend that each organisation have a template data breach notification letter;
- In the event of a breach, ensure that the cause of the breach is investigated and repaired to avoid any further loss.

POPI: Questions & Answers*...continued*

Section 19(1) of POPI states that parties who process personal information must take *"appropriate reasonable technical and organisational measures"* to secure the integrity and confidentiality of personal information in its possession or under its control.

REASONABLE TECHNICAL AND ORGANISATIONAL MEASURES

What security safeguards would be regarded as appropriate?

Section 19(1) of POPI states that parties who process personal information must take *"appropriate reasonable technical and organisational measures"* to secure the integrity and confidentiality of personal information in its possession or under its control.

The measures provided for in section 19 are aimed at preventing the loss of, damage to or unauthorised destruction of personal information as well as unlawful access to or processing of personal information. Organisations should thus consider whether their current measures leave personal information vulnerable to being lost, damaged or destroyed and/or whether an unauthorised third party could easily access or process such personal information.

Organisations should ensure that the steps they take are appropriate within the context, and thus that the level of security is proportionately suitable and proper considering the personal information being processed. Accordingly, it would be appropriate for an organisation such as a hospital, which processes special personal information such as information regarding patients' medical records, to have stricter and more robust data protection measures in place than a small business which only processes its clients' email addresses and cellphone numbers.

These steps taken should also be reasonable, and organisations should thus measure their data protection safeguards against what would be logical, equitable and fair for an organisation in their position and not simply against a general standard or an organisation which is not comparable.

Which practical steps can a business take to comply?

The technical and organisational measures required by POPI are the pragmatic steps an organisation should implement to protect personal information. Organisations should consider the extent to which they process personal information as well as the nature of the personal information to assess which measures are appropriate. Section 19(2) of POPI sets the following requirements for organisations:

- Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control: An organisation should conduct an audit or similar exercise to evaluate any flaws in its data protection systems in place, in order to establish which of its systems and/or processes leave personal information at risk.
- Establish and maintain appropriate safeguards against the risks identified: Once an organisation knows where its data protection vulnerabilities lie, it should implement practical steps. These steps range from sophisticated information technology solutions such as firewalls, anti-virus programmes

POPI: Questions & Answers...*continued*

It is important to take note of the stipulation in section 19(1) that an organisation's duty of care does not only apply to personal information in its possession, but also to personal information which is under its control.

and encryption (a process whereby information is converted to a code, so that only authorised users can read it) to simpler steps such as only giving persons and devices access to personal information on a need-to-know basis, ensuring that all devices and servers are password protected, and ensuring employees are educated about basic information security protocols as well as the organisation's information security policy.

- Regularly verify that the safeguards are effectively implemented: Once the practical steps have been implemented, an organisation should be sure that these steps work and work effectively.Appropriate testing, scanning and analyses is required to determine whether the data protection measures are efficient and are being adhered to.
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards: Organisations should be mindful of the fact that compliance with POPI and the effective protection of personal information is not a once-off activity, but an ongoing process. The practical steps an organisation has taken should thus be scrutinised and evaluated regularly to ensure that these are aligned to and updated for potential changes to the organisation's business, the personal information it processes and/or the type of processing it engages in.

Section 19(3) adds that organisations must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations. Certain industries may have additional responsibilities, such as those engaged in direct marketing or those processing personal information of minors, and organisations should ensure that they are well-informed about any particular additional obligations they may have.

What if processing of personal information is outsourced?

It is important to take note of the stipulation in section 19(1) that an organisation's duty of care does not only apply to personal information in its possession, but also to personal information which is under its control.

If an organisation, in its capacity as a *"responsible party"* under POPI, outsources certain services which involve the processing of personal information, to a third-party (which POPI defines as an *"operator"*), that organisation remains liable for the protection of that personal information even though it is not processing the personal information itself. Organisations should therefore note that they cannot evade their data protection responsibilities simply by relying on a third-party service provider.

However, a third-party service provider may in some instances provide improved data security if it is a specialised service provider with stringent protection of personal information measures in place. To the extent that organisations rely on third-party service providers, these third parties should be reputable service providers with a proven track record.

Fatima Ameer-Mia, Nikita Kekana, Lee Shacksnovis and Mieke Vlok

CDH
CLIFFE DEKKER HOFMEYR

The POPI Act – increased liabilty for employers

In terms of section 99(1) an employer may be held liable for the conduct of its employees, regardless of whether there is any willful or negligent conduct on the part of the employer.

With effect from 1 July 2021, employers will bear increased liability for the conduct of their employees. Significant sections of the POPI Act will come into effect on 1 July 2020 including section 99 relating to civil remedies. Employers have one year to prepare for and take steps to mitigate the risk which this section creates.

Under the common law an employer may be held vicariously liable for a wrong committed by an employee during the course and scope of his or her employment. The fact that an employer has taken steps to train its employees, issued instructions and developed policies to ensure that its employees conduct themselves in a certain manner when performing their work and do not engage in certain forms of conduct, often serves as a competent defence in a claim of statutorily created vicarious liability. These steps limit the risk to the employer. However, the nature of the civil liability created in terms of section 99(1) of the POPI Act and the restricted nature of the defences in terms of section 99(2) create significant risk for employers which may not be adequately addressed by the steps typically taken by employers to limit such risk.

Section 99(1) provides that a data subject, or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court against a responsible party for breach of the POPI Act, whether or not there is intent or negligence on the part of the responsible party. Responsible party includes an employer. In terms of section 99(1) an employer may be held liable for the conduct of its employees, regardless of whether there is any willful or negligent conduct on the part of the employer.

Most employees process personal information as contemplated in the POPI Act. For example, employees employed in human resources are continuously engaged in the processing of personal and special personal information. The following HR related processes involve the processing of personal information:

- The recruitment and selection process starting with application forms, the sorting and storing of CVs, the shortlisting process, conducting interviews, vetting and verifying of references,
- Processing payment of remuneration and recording bank account details,
- Receiving and storing of leave applications and records, sick leave and medical records,
- Monitoring performance, conducting written performance assessments, and
- Investigating possible misconduct and conducting disciplinary processes.

Many employees engage in the process of significant volumes of varied personal information, both internal and external to a business, on a daily basis.

The POPI Act – increased liabilty for employers*...continued*

While steps taken by an employer to limit the risk of a breach by one of its employees may not serve as a defence to a breach of the POPI Act by one of its employees, such steps on the part of an employer may serve to limit the quantum of the award.

Measures which employers can implement to limit the risk of employees processing information in breach of the POPI Act include the implementation of internal policies relating to the processing of personal information and compliance with the conditions for lawful processing in terms of the POPI Act and compulsory training sessions, workshops and awareness campaigns. Application forms for employment and employment contracts should also include consents to the processing of information.

But, as already stated, these measures may not always be sufficient to limit the risk. Section 99(2) of the POPI Act sets out the limited defences which an employer may raise in response to a claim in terms of section 99(1). The defences include vis major, consent of the plaintiff, fault on the part of the plaintiff, compliance was not reasonably practicable in the circumstances of the particular case or the Regulator has granted an exemption in terms of section 37.

Of concern to employers will be the fact that the defences do not include circumstances in which the employer is able to show that it did all that was reasonably practicable to ensure that the employee did not breach the POPI Act.

While steps taken by an employer to limit the risk of a breach by one of its employees may not serve as a defence to a breach of the POPI Act by one of its employees, such steps on the part of an employer may serve to limit the quantum of the award. In terms of section 99(3) a court is empowered to award an amount that is just and equitable.

Having regard to the provisions of section 99, employers will be well advised to take steps over the next year to limit the risks created by the section in particular ensuring that their employees do not process information unlawfully and that they are aware of the conditions for lawful processing and act in accordance with these conditions at all times.

Gillian Lumb and Chanté du Plessis

CDH
CLIFFE DEKKER HOFMEYR

POPI and the defense of legitimate interest

POPI defines both *"processing"* and *"personal information"* in section 1, as well as providing eight conditions in section 4 that needs to be met in order for the processing of such information to be lawful.

The long-awaited commencement of key provisions of the Protection of Personal Information Act 4 of 2013 (POPI) has finally been announced and whilst some companies have spent the past few years preparing for it, others will now be scrambling to make sure they are POPI compliant within the grace period of one year.

However, given the wording of some of the sections of POPI, it seems unlikely that anyone can be fully prepared, since guidance and interpretation from the Information Regulator (Regulator) will be required to understand the extent of some of the sections. The term *"legitimate interests"* is referred to regularly in POPI and mainly relates to potential defenses available to persons and companies not complying with certain requirements set out in POPI, such as consent to process personal information.

POPI defines both *"processing"* and *"personal information"* in section 1, as well as providing eight conditions in section 4 that needs to be met in order for the processing of such information to be lawful. Read together, the processing of personal information relates to the obtaining, dissemination or merging of information relating to either a natural or a juristic person, where such information can be used to identify the person.

Sections relating to legitimate interest

POPI uses the term *"legitimate interests"* throughout the Act, but the most relevant provisions are those contained in sections 11, 12, 18 and 71.

Section 11 does not require consent to process personal information, provided that such processing either protects a legitimate interest of the data subject, or is *"necessary for pursuing the legitimate interest of the responsible party or of a third party to whom it is supplied"*. However, this defense against a lack of consent is obviated by the caveat in section 11(3), which allows a data subject to explicitly object to such processing.

Section 12 excuses the collection of personal information directly from the data subject under the same circumstances, but does not give the data subject the option to object, as in section 11(3).

Section 18 requires notification to a party whose information is being processed, but section 18(4)(b) specifies that compliance with this notification requirement is not necessary if *"non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act"*.

Section 71 relates to automated decision making regarding the use of personal information and restricts such automated decision making, unless provision is made for the legitimate interest of the data subject.

CDH
CLIFFE DEKKER HOFMEYR

POPI and the defense of legitimate interest...*continued*

Section 233 of the Constitution of the Republic of South Africa, 1996 provides for the consideration of relevant international law in interpreting areas of uncertainty in South African law.

Interpretation of term "*legitimate interest*"

Relying on the "*legitimate interests*" defence of the data subject, the responsible party or a third party may thus find a way to get around some of the more restrictive provisions of POPI, when coming under scrutiny for seemingly not adhering to certain sections. It will be up to the Regulator to determine the interpretation and scope of the term "*legitimate interests*" and it seems likely that it will seek guidance from the European Unions' General Data Protection Regulation 2016/679 (GDPR), The GDPR is a regulation in EU law on data protection and privacy, but unlike POPI, it is limited to the protection of natural persons and does not extend to juristic persons.

Section 233 of the Constitution of the Republic of South Africa, 1996 provides for the consideration of relevant international law in interpreting areas of uncertainty in South African law. Such guidance will be essential, especially since the term "*legitimate interest*" is not defined in POPI and, as the relevant provision will only commence on 1 July 2020, no case law on this POPI related issue exists.

Although there has been much speculation regarding the issue of "*legitimate interests*", the South African Law Society has noted that much of this is based on an interpretation in favour of the data processor, rather than the data subject and have put forward the view that this approach is contrary to the provisions of the GDPR and is unlikely to find favour with the Regulator.

In its guidelines issued during 2018, the Law Society submitted that when considering the legitimate interests of a responsible- or third party, the data subject's constitutional right to privacy must be balanced with the rights of the processor. The fact that the right to privacy is expressly protected in the South African Bill of Rights is an important consideration when undertaking this balancing of rights.

The GDPR has established a three-pronged test in interpreting "*legitimate interests*", which is derived from Article 6(1)(f) of the GDPR and it is likely that the Regulator will, at least in the beginning, follow a similar approach. This test, which makes provision for three key elements of legitimate interests has been developed and confirmed by the Court of Justice in the European Union in the *Rigas* case C-13/16, 4 May 2017. The test looks at purpose, necessity and balance. It first asks, *"Is there a legitimate reason or purpose for the processions?"*, secondly "*Is processing the information necessary for that purpose*" and thirdly "*Is the legitimate interest overridden by the interests of the data subject?*" Only once all three these questions have been answered, will a determination be made on "*legitimate interest*".

In addition to seeking guidance from the GDPR, the Regulator might also start looking to industry specific code, such as those developed by companies in line with the Consumer Protection Act 68 of 2008. If such industry code is subsequently accepted by the Regulator, it may become part of POPI.

CDH
CLIFFE DEKKER HOFMEYR

POPI and the defense of legitimate interest...*continued*

A less clear cut example is a situation where a company uses a customer's data to personalise their websites content by giving them more suitable recommendations.

Practical consequences

The approach to interpreting "*legitimate interest*" laid out above is admittedly quite a technical one and each case will likely have to be dealt with on its own merits. There are however, certain examples where it seems likely that the Regulator will find the defense of legitimate interests to prevail.

One such example would be where parties enter into a credit agreement and the one party defaults on its payments. Using the defaulting party's personal information, without their consent, to track them and collect the debt owed would likely be justified by a "*legitimate interest*" defense. Another example would be where a user has requested deletion of their data, or to unsubscribe from a website or mailing list. In order to ensure that such a user remains unsubscribed, or that their email address is not used by another person, a data processor may retain only the details necessary for furthering those legitimate interests of the person.

A less clear cut example is a situation where a company uses a customer's data to personalise their websites content by giving them more suitable recommendations. They could potentially argue that this will improve the customer experience and is thus in the legitimate interest of the customer.

Conclusion

Given the uncertainty regarding the way in which the Regulator will approach the interpretation of "*legitimate interests*", we recommend that companies rather err on the side of caution. Instead of relying on the possible defense, it would be prudent to first attempt to comply with the provisions of POPI, especially those relating to consent and notification of the data subject. As companies have been given a period of one year to ensure that they comply with the provisions of POPI, there might be some guidance published by the Regulator during the course of this one year period. However, when in doubt it is always advisable to consult a legal practitioner to ensure compliance with the new act.

Lucinde Rhoodie and Kara Meiring

CDH
CLIFFE DEKKER HOFMEYR

A look at some practical implications of POPI on the Real Estate industry

The real estate sector consists of various responsible parties and operators for the purposes of POPI.

Each person has a constitutional right to privacy. This includes the right to have personal information safeguarded by a person entrusted with such information. On 1 July 2020 substantive provisions of the Protection of Personal Information Act 4 of 2013 (POPI) will come into operation and this article discusses some practical implications that POPI requires of service providers in the real estate industry.

The real estate sector consists of various responsible parties and operators for the purposes of POPI. All these role players collect personal information from data subjects in the performance of their duties. The data gleaned from data subjects are used to complete various commercial instruments such as lease agreements, sales of property, FICA compliance affidavits, bond approvals, mortgage bonds, notarial bonds, antenuptial contracts and deeds of transfer.

The processing of personal information by various persons is integral to the operation of the real estate industry. Conveyancers, for example, receive personal information from purchasers, sellers, developers, estate agents, insurers, auditors, homeowners' associations and financial institutions. Some of the information is, in turn, passed onto government institutions such as SARS, deeds registries and municipalities for further processing either directly or via various vendor software packages.

Responsible Parties

A responsible party like an estate agent, broker, mortgage originator or conveyancer is defined in section 1 of POPI as a "*public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.*"

A responsible party has the duty to ensure that it meets the conditions of lawful processing of personal information and adheres to the security measures on integrity and confidentiality in respect thereof under section 19 of POPI.

In terms of the security safeguards, a responsible party must take appropriate, reasonable technical and organisational measures to prevent the loss of, damage to, or unauthorised destruction and unlawful access to or processing of personal information. This includes the duty to take reasonable measures to identify all reasonably foreseeable internal and external risks to personal information; establish and maintain appropriate safeguards against the risks identified; regularly verify that the safeguards are effectively implemented; and to ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Data Subjects

A data subject is the person to whom personal information relates and POPI provides a non-exhaustive list of what constitutes personal information in terms of section 1. In addition, POPI awards rights to data subjects, which include the right to have their personal information processed in accordance with prescribed conditions for its lawful application.

Processing of personal information and what is required from a real estate perspective

Section 11 of POPI provides for the consent, justification and objection of processing of personal information. Processing of information includes the collection, recording or use thereof, the

CDH
CLIFFE DEKKER HOFMEYR

A look at some practical implications of POPI on the Real Estate industry

...continued

All real estate role players are required to notify all data subjects (section 18 of POPI) of *inter alia* the collection of and the manner in which their personal information will be processed.

dissemination thereof and the merging or destruction of such personal information. Personal information may only be processed if the "*processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; for the proper performance of a public law duty by a public body; for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied*". Processing personal information, in addition must, "*comply with an obligation imposed by law on the responsible party*" and protect the interests of the data subject.

The conditions for lawful processing of personal information notably also require the data subject to consent to the processing of the personal information. Examples of data subjects include landlords, tenants, sellers, purchasers and their authorised representatives. It is required that a consent be obtained from a data subject prior to receiving any personal information and we would recommend that such consent be in writing.

Furthermore, the collection of the personal information must be taken directly from the data subject unless the information contained is derived from a public record or has deliberately been made public by the data subject (section 12 of POPI) and obtained for a specific purpose related to a function of the responsible party (section 13 of POPI), which the data subject must be informed of.

All real estate role players are required to notify all data subjects (section 18 of POPI) of *inter alia* the collection of and the manner in which their personal information will be processed. We recommend that such notification be advanced in writing and is to specifically be brought to the attention of the data subject who is to confirm that they understand the contents thereof. It should be noted that the notification must be provided prior to the personal information of a data subject being disclosed to the responsible person.

It is also important to note that responsible parties who authorise operators like a vendor software operator to collect personal information on their behalf, must ensure that POPI compliance is included as one of the obligations of their contract. Operators must ensure that they maintain security safeguards and must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

Sanctions

Contravention of POPI could result in far-reaching sanctions, these include the imposition of fines, imprisonment for a period of 12 months to 10 years and/or a damages claim by the data subject. Each role player has one year within which to ensure that their business practices comply with POPI, failing which, they will fall foul of the statutory provisions.

Simone Franks, Robyn Geswindt and Sikelelwa Stemele

CDH
CLIFFE DEKKER HOFMEYR

OUR TEAM

For more information about our practices and services, please contact:

Fatima Ameer-Mia
Director
Technology, Media & Telecommunications
T +27 (0)11 562 1837
E fatima.ameermia@cdhlegal.com

Justine Krige
Director
Corporate & Commercial
T +27 (0)21 481 6379
E justine.krige@cdhlegal.com

Robyn Geswindt
Senior Associate
Real Estate
T +27 (0)21 481 6382
E robyn.geswindt@cdhlegal.com

Simóne Franks
Director
Real Estate
T +27 (0)21 481 6464
E simone.franks@cdhlegal.com

Lucinde Rhoodie
Director
Dispute Resolution
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com

Nikita Kekana
Associate
Technology, Media & Telecommunications
T +27 (0)21 481 6334
E nikita.kekana@cdhlegal.com

Kendall Keanly
Director
Corporate & Commercial
T +27 (0)21 481 6411
E kendall.keanly@cdhlegal.com

Gillian Lumb
Director
Employment
T +27 (0)21 481 6315
E gillian.lumb@cdhlegal.com

Lee Shacksnovis
Associate
Technology, Media & Telecommunications
T +27 (0)21 481 6453
E lee.shacksnovis@cdhlegal.com

BBBEE STATUS: LEVEL TWO CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

PLEASE NOTE
This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa. Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

CLIFFE DEKKER HOFMEYR