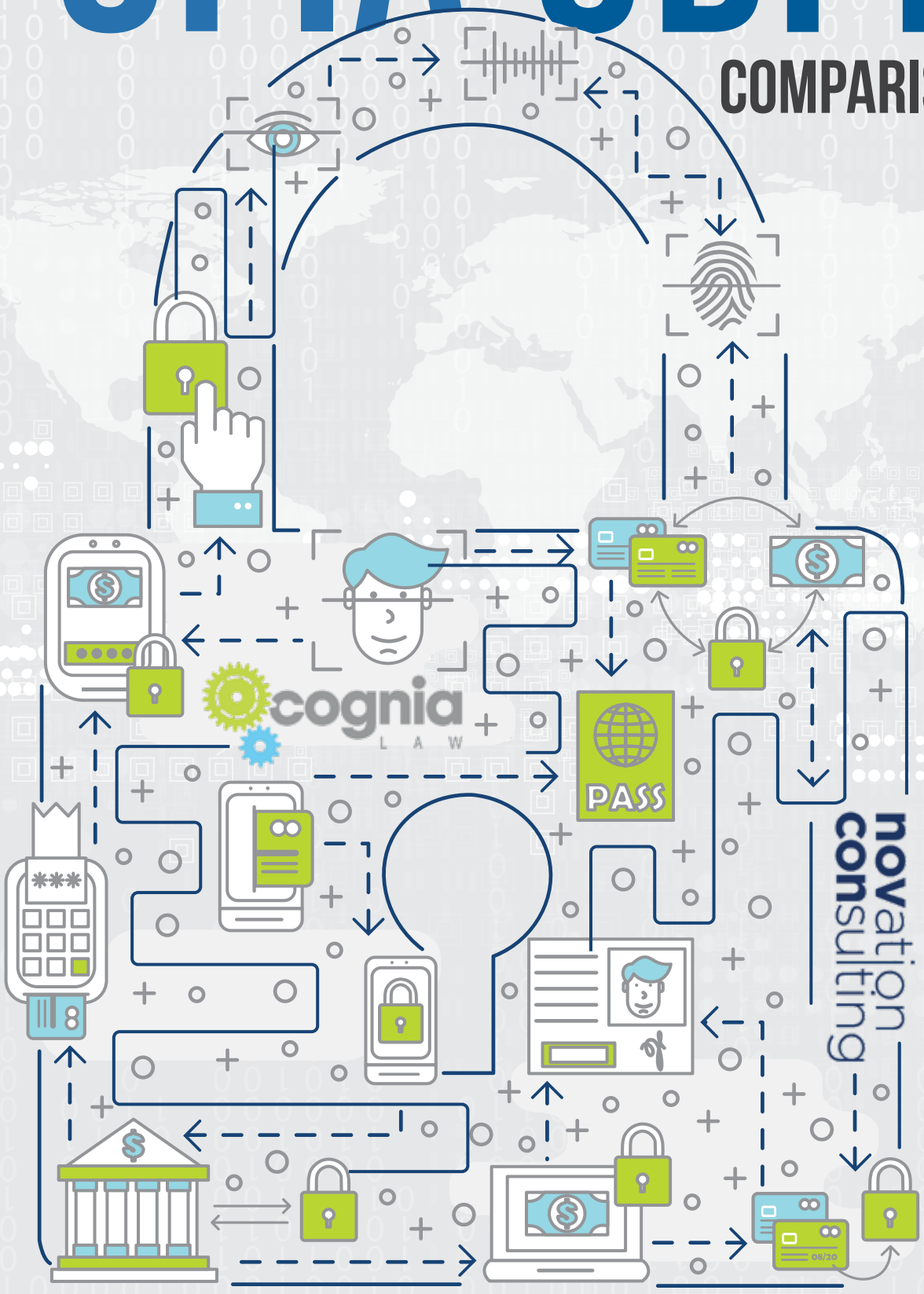
POPIA GDPR

COMPARISON



Another year, another data privacy law:
*How does the **POPIA** compare to the **GDPR**?*

For us, 2018 was the year of privacy, *and dealing with a deluge of questions from companies wondering whether they need to comply with the GDPR, and how they can combine their efforts to comply with the POPIA and the GDPR without reinventing the wheel.*

In 2019, we expect that companies will start to prepare for the effective date of the POPIA.

COMPLYING WITH BOTH THE POPIA AND THE GDPR

As you have probably guessed, if the GDPR applies to your organisation you will have two data protection laws to worry about when the POPIA comes into effect. Most organisations resent having to do one compliance project, let alone two, so we often get asked 'if we comply with the GDPR, will we be POPIA compliant too?' Unfortunately, no. While the POPIA and the GDPR have a lot in common, there are some key differences between the two, for example, some of the duties in the POPIA are not in the GDPR, and vice versa. And that is what this white paper is about.

We are also often asked 'can we develop one set of policies and procedures that will comply with both the POPIA and the GDPR?' The answer is that it is not only possible, but also preferable because to maintain two different sets of policies depending on whether the POPIA or GDPR applies is virtually impossible. However, to get there, you have some decisions to make. Where the GDPR introduces a concept that isn't in the POPIA, you will need to decide whether you are happy to adopt it, even though it might not be a requirement for the parts of your organisation that don't have to comply with the GDPR.

But let's take a step back.

It is obviously important to figure out whether your organisation should be complying with the GDPR, but even for those organisations who don't have to comply, the knowledge and tools out there on how to comply with the GDPR can be enormously useful if you understand how to adapt these tools for POPIA compliance. And many of the tools are free.

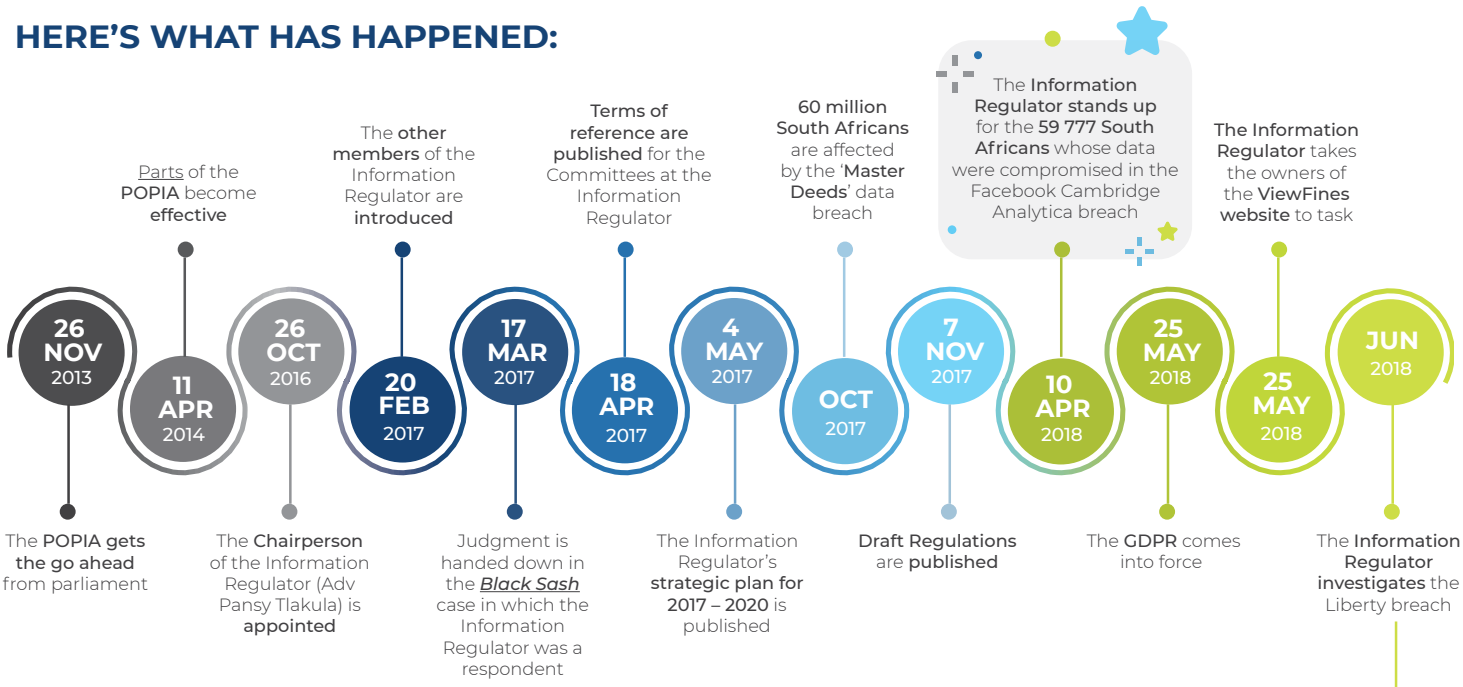
WILL THE POPIA'S EFFECTIVE DATE BE ANNOUNCED THIS YEAR?

The POPIA has been looming for a while now, but it is not in effect yet. Could 2019 be the year? We think it might be, and we base our belief on two factors: a slow but steady increase in activity at the Information Regulator and an increase in pressure from the public and civil society for better privacy protection in the face of a deluge of data breaches.

The plan was for the Information Regulator to be fully operational by the end of 2018. That did not happen. Media reports suggest that the delay is due to a difference of opinion between the Information Regulator and National Treasury regarding the internal structure of the Regulator, resulting in an administrative deadlock which has prevented the Regulator from filling key positions.

In the meantime, the Regulator has not been idle.

HERE'S WHAT HAS HAPPENED:



In its Media Statement on 18 June 2018 about the Liberty breach the Regulator says:
'South Africa has experienced a disturbingly high number of material data breaches in the past few months. In addition to Liberty Holdings, there have been material data breaches at Master Deeds, Facebook, and ViewFine. Without a fully functional Information Regulator, these breaches will continue to occur without sanctions provided for in the POPIA. These data breaches underscore the urgent establishment of the Regulator. It is for this reason that the Information Regulator requests the powers that be to assist it in fast-tracking its operationalisation.'

18 JUN 2018

6 AUG 2018
The Information Regulator's Annual Performance Plan and Quarterly Targets for 2018/2019 are published

14 DEC 2018
Final regulations come out

?
Effective date? Anybody's guess, but once it arrives companies will have a year to become compliant with the Act and the Regulations.

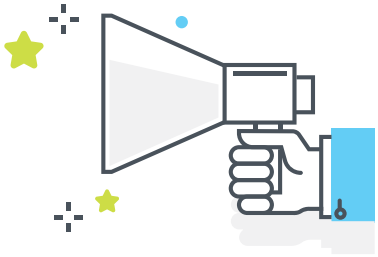
WHY IS THE GDPR SUCH A BIG DEAL?

Companies are concerned about the GDPR, partly, because of the enormous fines and risk of reputational damage, but also because the GDPR potentially applies to businesses outside the EU. Lawyers the world over had their clients in a panic by saying that the GDPR applies to all businesses who process personal information of European citizens. That is not correct, in fact, we got so worked up that we published a white paper about the GDPR and South African organisations. For a quick reference, have a look at these guidelines:

If you answer 'yes' to any of these questions, you must comply with the GDPR.

WHAT IS THIS WHITE PAPER ALL ABOUT?

In this white paper, we highlight the big differences between the POPIA and the GDPR. There are many other subtler differences in wording and we won't lie, they can trip you up. That is why we will soon make our side-by-side comparison available online



Two heads are better than one

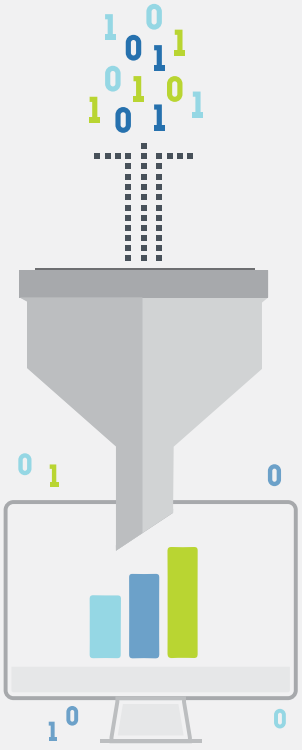
This white paper is a collaboration between Novation Consulting and Cognia Law. Novation turns POPIA compliance on its head, shakes the nonsense out of its pockets, and presents compliance advice in a fresh and exciting way. Cognia Law is a company that provides consulting and managing services to compliance departments and in-house legal functions helping them remove the busy work so they can focus on what is important. Having its headquarters in the UK, Cognia has extensive experience in helping companies prepare for the GDPR, remediate contracts, and maintain compliance. This might just be the beginning of something beautiful. ♥

WHERE PERSONAL INFORMATION (PI) IS COLLECTED FROM

WHAT IS THE REASON FOR THIS RULE?

If you get PI from the data subject, you are entitled to assume that the PI is accurate. Inaccurate PI can be very prejudicial to a data subject.

The data subjects will know that you are collecting their PI if you are asking them for it. Companies that buy and sell PI often are not transparent about it.



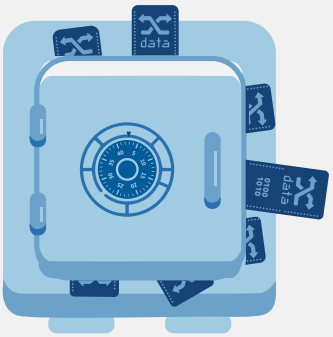
*THE **GDPR** IS SILENT ON WHERE **PI** MAY BE COLLECTED FROM. THE **POPIA** GIVES STRICT INSTRUCTIONS!*

SECTION IN THE POPIA

The POPIA is stricter when it comes to the rules regarding where PI may be collected from. The general rule in the POPIA is that a responsible party must collect PI directly from the data subject.

Any departure from this rule may be justified if

- the PI was deliberately made publicly available by the data subject
- the PI is contained in a public record
- the use of another source is not prejudicial to the legitimate interest of the data subject
- the collection is necessary for law enforcement or in the interest of national security
- the collection is necessary to maintain the legitimate interests of the responsible party or of a third party to whom the PI is supplied
- collecting the PI directly from the data subject would prejudice the lawful purpose of collection
- collecting the PI directly from the data subject is not reasonably practicable in the circumstances of the case
- the data subject consented to the use of another source.



REMEMBER, JUST BECAUSE PI IS PUBLICLY AVAILABLE, DOESN'T MEAN IT IS NOT PROTECTED.

DO

Review all your collection practices to ensure you are complying with the POPIA.

DON'T

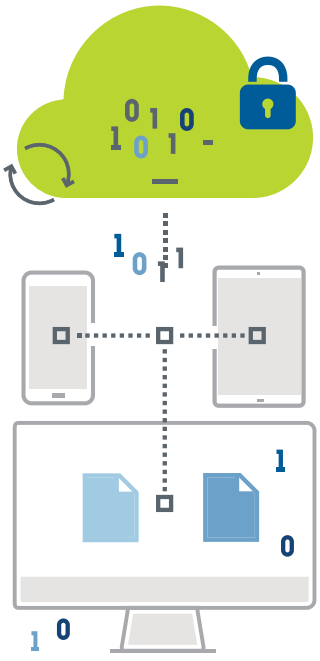
Collect PI from another source when it is possible to collect the PI directly from the data subject.

DATA PORTABILITY

WHEN DO YOU HAVE TO PORT?

The right only applies

- to PI that the data subject provided,
- when the business' basis for processing the PI is that a contract requires the processing or if the data subject has consented to the processing, and
- if the business is using automated means to process the PI.



*THE **GDPR** ESTABLISHES THE RIGHT TO **DATA PORTABILITY***

The GDPR states that data subjects have the right to receive and transfer their data from one organisation to another.

REMEMBER

this section is only applicable if the GDPR applies to you. Do you want to know whether the GDPR is applicable to you? Read our previous white paper.

Even if the GDPR doesn't apply, it might be a good idea to start thinking about data portability as it is likely that the POPIA will move in that direction. Not to mention that it is consumer-friendly.

SECTION IN THE POPIA

Thundering silence

ARTICLE IN THE GDPR

1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

b) the processing is carried out by automated means.

2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

As a business you should ask:

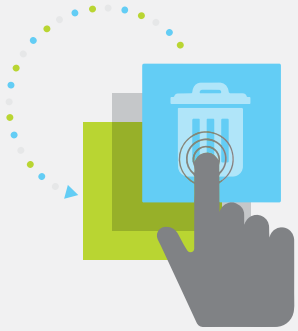
- How will we process portability requests?
- Can we validate the ID of the data subjects?
- Has all the data been found and sent?
- What format will we send the data in?

IT'S A GOOD IDEA TO HAVE A DATA PORTABILITY POLICY!

WANT TO KNOW MORE?

ICO: The right to data portability
Article 29 Data Protection Working Party: Guidelines on the right to data portability

THE RIGHT TO BE FORGOTTEN



*GONE, BUT ALSO DEFINITELY **FORGOTTEN***

SECTION IN THE POPIA

Close, but no cigar

The right to be forgotten isn't in the POPIA, however the principle of minimality comes close.

WHAT IS THE PRINCIPLE OF MINIMALITY?

PI may only be processed if it is

- adequate,
- relevant, and
- not excessive.

The right to be forgotten applies if PI is no longer necessary for the purpose for which it was collected making the PI not relevant. The Google Spain case established that the responsible party must take reasonable steps to ensure that PI not meeting this requirement must be erased or rectified.

ARTICLE IN THE GDPR

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

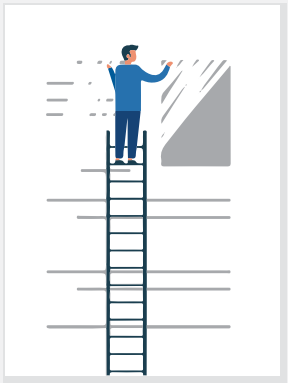
f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

ICO: right to erasure

ALWAYS TAKE REASONABLE STEPS TO INFORM YOUR OPERATORS THAT YOU ARE ERASING PI

The right will not apply if processing is necessary for

- freedom of expression and information
- compliance with a legal obligation
- reasons of public interest in the area of public health
- archiving purposes in the public interest, scientific or historical purposes, or statistical purposes
- the establishment, exercise, or defence of legal claims



DATA SUBJECTS

THE POPIA PROTECTS ***INDIVIDUALS AND COMPANIES***

THE GDPR ONLY PROTECTS ***INDIVIDUALS***

DID YOU KNOW

that the Promotion of Access to Information Act(PAIA) also sees dead people? While the POPIA only protects the PI of living individuals, the PAIA omitted the word from its definition of personal information.

The GDPR doesn't apply to deceased persons.

THE POPIA IS APPLICABLE TO THE PROCESSING OF DATA OF NATURAL AND JURISTIC PERSONS.

A juristic person includes a

- body corporate
- partnership
- association
- trust

SECTION IN THE POPIA

A 'person' means a natural person or a juristic person.

ARTICLE IN THE GDPR

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

What is PI of a natural and juristic person?

- Identifiers
- Demographic information
- Contact details
- Financial information
- Correspondence
- Usernames and social handles
- Biometric information
- Health information
- Preferences and opinions
- Behavioural information

DATA PRIVACY IMPACT ASSESSMENT

THE POPIA DOESN'T PROVIDE FOR THE USE OF A PRIVACY IMPACT ASSESSMENT (PIA) ... ***OR DOES IT?***

A PIA is an assessment that must be conducted before the intended processing of personal information starts.

What your PIA must be able to do?

- Describe the nature, scope, context and purposes of processing.
- Access necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

The GDPR says a PIA must be carried out if you plan to

- use systematic and extensive profiling or automated decision making to make significant decisions
- process special categories of PI on a large scale
- systematically monitor a publicly accessible area on a large scale

SECTION IN THE POPIA

The Act itself doesn't refer to PIAs, however, PIAs snuck into the brand-new Regulations that state that an information officer must ensure that a personal information impact assessment is done to make sure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of PI.

ARTICLE IN THE GDPR

Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Office of the Privacy Commissioner of Canada:

DO'S and DON'TS for PIAs

GDPR: Privacy Impact Assessment

ICO: Data Protection Impact Assessment

ICO: sample DPIA template

Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment

WE CAN HELP YOU PROVIDE TRAINING TO YOUR EMPLOYEES ON HOW TO CARRY OUT A PIA.

OPERATOR AGREEMENTS

What is a processor in terms of the GDPR?

If you are processing personal data on your client's behalf the GDPR would call you a processor. Processing includes any collection, recording, organisation, storage, use, transmission, and destruction of data.

What is an operator in terms of the POPIA?

An operator is a person who processes PI for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

*THE **GDPR** HAS MORE ONEROUS REQUIREMENTS FOR **OPERATOR AGREEMENTS***

The GDPR refers to operator agreements as processor agreements.

SECTION IN THE POPIA

In a nutshell, the POPIA requires that the operator does the following:

- Only process PI with the authorisation of the responsible party.
- Treat PI that comes to its knowledge as confidential.
- Establish and maintain the security measures discussed in section 19 of the POPIA.
- Notify the responsible party immediately where there has been a breach.

ARTICLE IN THE GDPR

Article 28(3) of the GDPR sets out what must be in your operator agreement. As a minimum the contract must set out:

- The subject matter and duration of the processing, for example, you will send out promotional vouchers to the client's customer database for the next three months.
- The nature and purpose of the processing, for example, you will send promotional vouchers to the client's customer database via SMS and email.
- The type of personal information and categories of data subjects, for example, you will have the names, cell phone numbers and email addresses of your client's customers.
- The obligations and rights of your client.

This is not all. Read this blog, if you want to know what else to expect in a processor contract.

Should you include the additional GDPR requirements in your POPIA operator agreement?

It depends on who is writing the agreement. (We know, it's a lawyer answer, sorry.)

If it is the responsible party who is drafting the agreement, it is in their best interest to include the more comprehensive provisions of the GDPR.

If you are the operator. Well, less is more.

REMEMBER: THE GDPR REFERS TO OPERATORS AS DATA PROCESSORS

SOME FREE STUFF

ICO: Contracts

ICO: How to distinguish between a processor (operator) and data controller (responsible party)

DATA PROTECTION BY DESIGN

Privacy by Design was first implemented by the Information and Privacy Commissioner of Ontario and it emphasised the notion of embedding privacy measures and enhancing privacy technologies into the design of IT systems.

Data Protection by Design and by Default is about implementing security measures into all systems and processes within an organisation so that the PI does not need protection at a later stage but that protection is embedded from the very beginning when the PI is collected.

*THE **GDPR** REQUIRES THE **IMPLEMENTATION OF DATA PROTECTION** BY DESIGN AND BY DEFAULT*

SECTION IN THE POPIA

Quite similar to the principles of accountability and minimality.

ARTICLE IN THE GDPR

Data protection by design: Responsible parties must put technical and organisational measures in place before and during processing to ensure GDPR compliance and to protect the rights of data subjects. Here is the full article.

Data protection by default: Responsible parties must only process data that is necessary and must only store it as long as necessary. Here is the full article.

SOME FREE STUFF

ICO: data protection by design

Norwegian Data Protection Authority: Software development with Data Protection by Design and by Default

Novcon: Our top five privacy notices

READ WHAT WE SAID ABOUT THE SEVEN PRINCIPLES OF PRIVACY BY DESIGN

Some practical tips for implementing Privacy by Design:

- Introduce clear privacy and data sharing notices.
- Display short messages when users are entering their PI that can link to the more detailed information on what you do with their PI
- Always use an opt-in as this aligns with the direct marketing principles in both the POPIA and GDPR
- Minimise the amount of PI you collect from the data subject.

Data protection by default is close to the POPIA principle of minimality that we discussed in the context of the right to be forgotten.

INFORMATION OFFICER

THERE IS NO NEED TO CREATE THE POSITION OF AN INFORMATION OFFICER (IO) UNDER THE POPIA, IT HAPPENS AUTOMATICALLY. SO, WHO WILL IT BE?

- Private companies: The CEO
- Other organisations: The Head of the organisation

The GDPR doesn't require all organisations to appoint a DPO.

*THE POPIA REFERS TO AN **INFORMATION OFFICER (IO)** AND THE GDPR REFERS TO A **DATA PROTECTION OFFICER (DPO).***

THE POPIA

An 'information officer' of, or in relation to, a

- public body, means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
- private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.

THE GDPR

You must appoint a data protection officer if

- you are a public authority or body;
- your core activities require regular and systematic monitoring of individuals; or
- your core activities consist of large-scale processing of special categories of PI or PI relating to criminal convictions and offences.

IO RESPONSIBILITIES UNDER THE POPIA

An IO's responsibilities under the POPIA are to

- encourage compliance within the organisation
- develop, implement, monitor, and maintain a compliance framework
- deal with requests from data subjects and the Regulator
- work with the Regulator during investigations
- conduct a personal information impact assessment
- conduct awareness sessions

DPO RESPONSIBILITIES UNDER THE GDPR

A DPO's responsibilities under the GDPR are to

- inform and advise organisations and employees about their obligations to comply with the GDPR
- monitor and audit compliance with the organisations' policies, the GDPR, and other data protection laws
- assign responsibilities
- raise awareness and conduct training
- advise on, and to monitor, data protection impact assessments
- cooperate with and act as the contact point with the supervisory authority
- be the first point of contact for supervisory authorities and for individuals whose data is processed, such as employees

ICO: Data protection officers

Wondering what you should do now?

All companies have a decision to make about whether they want to comply with the POPIA and the GDPR. We believe that it's not only possible to become compliant with both in one shot, but that it is a good idea. All of the things that the GDPR introduces are good privacy practices. However before developing a PIA and making sure that your personal information is portable, you need to get the basics in place. The ICO has developed a fantastic 12-step programme towards complying with the GDPR and, you guessed it, all of those steps are required in terms of the POPIA too.

THE POPIA & GDPR?

DO SOUTH AFRICAN ORGANISATIONS NEED **TWO COMPLIANCE PROGRAMMES?**

ICO's recommended step	Does the POPIA require it too?
Awareness Organisations must ensure that decision-makers and key people know that the law is changing.	**Yes.** It is a requirement in terms of the draft POPIA Regulations that the organisation must ensure that employees receive POPIA training.
Know your information Document what personal data the organisation holds, where it came from and who you share it with. In other words, organisations should do a personal data audit.	**Yes.** The POPIA requires that all processing of personal information must be documented. More importantly, it is impossible to do a POPIA compliance programme without knowing what personal information the organisation has and what it does with it.
Privacy notices Organisations should review their current privacy notices and ensure that they make the necessary changes in time for the GDPR implementation. The European Commission has published draft guidelines on transparency. At a minimum, the information must be easily accessible and easy to understand. Crucially, the Commission has affirmed an established principle of plain language drafting that organisations must identify the intended audience, assess the average member of that audience's level of understanding and continuously check that the information is tailored to the needs of the actual audience.	**Yes.** The POPIA places extensive notification obligations on organisations. The key principle is that people should not be surprised by what their personal information is used for. A privacy notice, also known as a privacy policy, is usually hidden behind a URL in the footer of a website. This notice or policy needs to come out of hiding. Here are some of our favourite privacy notices. When it comes to making information accessible and easy to understand we are crusaders for plain language. Using plain language when you talk about privacy and personal information is key if you want to win your customers' trust. Here are the steps we take to ensure that our clients get it right.
Individuals' rights Organisations must ensure that their procedures cover all the rights individuals have, including when and how to: · give people access to personal data · change or correct personal data · delete personal data	**Yes.** The POPIA also requires that people have the right to access, change or correct, and delete their personal information unless an exception applies.
Access requests Organisations should update their procedures and plans for when people request access to their personal data. This is necessary, because the GDPR will change the timeframes within which access has to be granted.	**Yes.** The POPIA interacts with an existing piece of legislation, the Promotion of Access to Information Act (PAIA). It has not changed PAIA much, but the Information Regulator will now be tasked with enforcing it. Organisations also need to dust off their PAIA manuals and review them to determine whether they comply with the POPIA. The POPIA and PAIA do not prescribe a specific timeframe within which access has to be granted. The timeframe just has to be reasonable.

Legal processing
Organisations must identify the purposes for which data is used and whether this usage is justified (there are justifications listed in the GDPR). These purposes must be documented and explained in the organisation's privacy notice.

Yes. The POPIA contains a virtually identical requirement.

The most common justifications are that the personal information must be processed in order to fulfil a contractual obligation or if there is other legislation that requires organisations to process personal information to comply.

Consent
Organisations should review how they seek, record, and manage consent and whether any changes need to be made.

Valid consent in terms of the GDPR must be:

- freely given
- specific
- informed
- unambiguous, and
- given by a statement or a clear affirmative action

The European Commission has published draft guidelines on consent. Here are some of the highlights:

- People must be given a real choice and control. Consent cannot be asked on a 'take it or leave it' basis. If the person cannot refuse or withdraw the consent without a negative effect, it is not freely given.
- In many cases public authorities will probably not be able to rely on consent, because there will often be a clear imbalance of power. This imbalance also occurs in the employment context. Employers must find other ways to justify their activities (in most instances it will be authorised by labour legislation).
- It is problematic to exchange free services for consent to use personal data for a non-essential purpose such as behavioural advertising. In other words, consent should not be used as a trade-off for additional services.
- If consent is being asked for more than one purpose, people should be free to agree to some, but not others. The consents must not be bundled into one, it must be granular.

Consent also features strongly in the POPIA. In many instances, organisations will be able to get around complying with the principles of the POPIA by obtaining consent from data subjects. For instance, in principle, personal data must be collected directly from the individual unless that individual has given the organisation permission to collect it from somewhere else. Virtually every principle in the POPIA is qualified in this fashion.

The important question will be when consent will be considered valid. In the POPIA consent is defined as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information'. It is similar to the GDPR which means that we can be guided by how the requirements for valid consent has been interpreted in the EU.

The myth of consent

Organisations are often advised that they need consent to process personal information. That is 100% untrue and a very bad practice because those consents are obtained on a take-it-or-leave-it basis. If the customer says no, they cannot have the product. We question whether such consent is legal. The European Commission has stated that 'if consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given.'

In any event, our research has shown that this kind of 'consent' infuriates people and erodes their trust in the organisation. Most processing activities are justified because they are required to fulfil a contract (e.g. delivering online shopping to a person's physical address) or legislation (e.g. collecting information about a person's race in terms of the Employment Equity Act). There are other justifications too. Consent should only be obtained as a last resort.

Children
Organisations must consider whether they need to put a system in place to verify individuals' ages and to obtain parental or guardian consent for processing activities involving child data. A child is anybody under the age of 14.

Yes. The POPIA also contains very specific requirements for the processing of the personal information of children, but the relevant age in South Africa will be 18. Around 90% of the time, the POPIA requires parental or guardian consent. This can be challenging, but here are some of our thoughts on the matter and things we have learnt along the way.

Data breaches
Organisations must make sure that they have the right procedures in place to detect, report, and investigate personal data breaches.

Yes. The POPIA requires breach monitoring and response policies and procedures. Not having this in place has sunk many a business. Here are some thoughts on how to deal with personal data breaches.

Data protection by design and privacy impact assessments
Organisations should think about how to ensure that all current processing activities and future (new) processing activities go through privacy impact assessments. The ICO has a terrific code of practice on privacy impact assessments and the latest guidance from EU authorities.

Yes, but not in so many words. The POPIA requires that all processing activities should be assessed, but privacy by design or privacy impact assessments are not mentioned in so many words. In our experience, it is impossible to ensure lasting POPIA compliance without privacy impact assessments, but they can be complex and experience is required to accurately gauge the level of risk a particular activity poses to the organisation. In fact, it is so important that we are currently developing a digital privacy impact assessment which should enable organisations to identify privacy risks with a high level of certainty.

Data protection officers
Organisations should designate someone to take responsibility.

Yes. The POPIA provides that the head of a private organisation is automatically the Information Officer of the organisation. Of course, the CEO cannot actually do the work, so the POPIA also allows for the designation of Deputy Information Officers.

In our experience organisations need Deputy Information Officers and privacy officials (sometimes called privacy stewards or champions) in each business area. We have found that if POPIA compliance is not written into a number of people's job descriptions, POPIA compliance won't work.

International
If organisations operate in more than one EU member state, they should determine the lead data protection supervisory authorities.

The POPIA does not contain an equivalent provision, because the Act only applies to South Africa. It does contain provisions on the cross-border transfer of personal information. The bottom line is that the level of protection has to remain at the POPIA levels even when organisations send the information somewhere else. This will be the case if the country has adequate data protection legislation or if agreements or binding rules to ensure compliance have been put in place.