everlytic

POPI & GDPR

Index

Visit us at www.everlytic.co.za or [click here](#) to request a demo.

The EU General Data Protection Regulation:
Should South African organisations care?

Right now, the whole world seems to be talking about data protection and privacy. That's not surprising, considering that data breaches have become part of the daily news. In South Africa, the chatter is mostly around the Protection of Personal Information Act (the POPIA). The much-anticipated Act is not in effect yet, but the Information Regulator has been established and staffed, draft regulations have come out, and the Regulator is already receiving complaints.

The rest of the world seems to be talking about the European Union's General Data Protection Regulation (the GDPR), which comes into force on 25 May 2018. The GDPR is a major overhaul of the existing data protection legislation. Its aim is to standardise the data protection law across the EU and to see to it that the new law reflects the changes in technology and the way information is used. It is also aimed at building trust in the online environment to ensure that consumers continue to buy online. However, as is the case with privacy laws in general, the GDPR's reach goes well beyond the European Union.

'The GDPR is designed to address technological and societal changes that have taken place over the last 20 years by adopting a technology-neutral approach to regulation'.

- Unlocking the EU General Data Protection Regulation (White & Case)

With its wide reach, the GDPR will have an impact on the way South African organisations do business, and it's important to determine whether your organisation is one of them. If it does, you may need to launch a compliance programme quickly, and if it doesn't, you need to know what to look out for in agreements that contain GDPR clauses. In this paper we will provide background on both pieces of legislation and provide you with the questions you need to answer to determine whether the GDPR applies to your organisation. We'll address the question of having two compliance programmes, describe the industries that will be most affected, and explain the risks of non-compliance.

POPIA versus GDPR:
Some Background

If South African organisations are focussing on data protection and privacy at all at the moment, they are probably focussing on complying with the Protection of Personal Information Act 4 of 2013 (POPIA). This Act applies to every organisation in South Africa, because all companies collect personal information from their customers, employees, and suppliers. It creates new rules for the way in which personal information is collected, what it may be used for, when it may be shared, how securely it must be stored, what the rights are of the person whose information it is, and what organisations must do in the event of a breach.

What is in a name?

POPIA refers to personal information. That is information ranging from a person's name and contact details, to medical and financial information. Here is a list. In this discussion, we also use the term 'personal data'. This is generally what it is called in the rest of the world. Why is this important? If you Google personal data or data protection, you will get more (free) information.

POPIA is not in effect yet. According to the Information Regulator, the effective date will be announced in the first or second quarter of 2018. Once this happens, South African organisations will have at least one year, but possibly as many as three years, to become compliant. So, it may still be a while before organisations begin to feel the teeth of this legislation.

We firmly believe that good data management is crucial, regardless of whether legislation compels organisations to take it seriously. We are not alone in our thinking. In fact, the information management function in organisations and its responsibility in ensuring that information assets are protected and enhanced is recognised in the King IV Report on Corporate Governance for South Africa 2016. However, this discussion is not about the importance of good data governance. If you are interested, you can read about that ***here.***

While POPIA must be a priority for 2018, many South African organisations should be focussing their attention on the latest developments in the European Union. On 25 May 2018, the EU General Data Protection Regulation (GDPR) will come into effect.

What is the EU General Data Protection Regulation?

The reforms to data protection in the EU are contained in the *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* and the *Regulation on the protection of natural personal data and on the free movement of such data.* The European Commission's website is a treasure trove of information. Here are some of our favourite research papers on GDPR compliance.

Most South African organisations have not paid any attention to the GDPR, because this is South Africa and not the EU. For many, this is a mistake for two reasons:

1

One of the major changes the GDPR makes is to extend the 'extra territorial applicability' of the law. This means that the GDPR may apply to some organisations that process personal information of individuals in Europe, regardless of where the organisation is located. This makes sense. In the hyper-connected world we live in, data flows from country to country without much regard for borders or jurisdiction. The challenge for lawmakers is that data protection laws must also cross borders effortlessly.

2

If the organisation is processing personal data with or on behalf of a European organisation, the EU organisation will often insist that the South African organisation comply with the GDPR, usually without good reason. This is because the EU organisation remains responsible for GDPR compliance even if the processing of personal data takes place in another country.

This discussion is about when a South African company will be directly subject to the GDPR (so reason #1). If your organisation is being forced into GDPR compliance by EU customers or partners, think carefully before you sign.

Which South African organisations should be worried about the GDPR?

If you answer 'yes' to any of these 4 questions, you must comply with the GDPR.

1 **Does the organisation have a legal entity (e.g. a company) which is registered in Europe?**

2 **Is the organisation established in the EU in some other way?**

What does 'established' mean?

The test that European courts have used in the past is very flexible, making it difficult to distil into a checklist. The test is whether the organisation exercises 'any real and effective activity – even a minimal one' through 'stable arrangements' in the EU (Weltimmo v NAIH (C-230/14)). Here are some examples from court cases on this topic:

- The organisation has a representative in the EU. That representative can be a single individual, an agent, sales office, branch, or subsidiary.
- The organisation has a website in the language of a European country (other than English).
- The organisation has equipment which is located in Europe.
- The organisation has a European postal address.

3 **Does the organisation offer goods or services to individuals in Europe?**

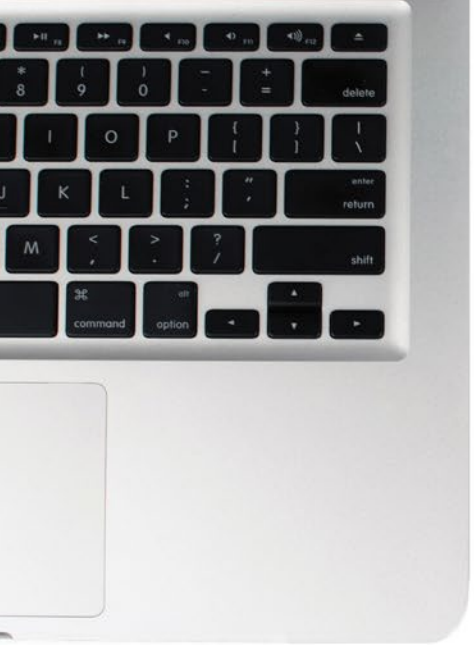
Another flexible requirement

Many organisations, particularly those engaged in e-commerce, offer goods or services worldwide. So, does that mean the GDPR will apply? Not necessarily. Once again, whether or not the legislation applies will be determined on a case-by-case basis, but mercifully the mere fact that a website can be accessed in the EU is not enough. The question is whether that organisation foresees that its activities will reach individuals in the EU. Factors typically considered are whether these services are offered in an EU language (other than English), whether payment can be made in an EU currency, or whether the organisation mentions European customers in its publications.

4 **Does the organisation monitor the behaviour of individuals in the EU while they are in the EU?**

What does 'monitoring behaviour' mean?

It includes tracking individuals in the EU on the internet or elsewhere in order to create a profile of them or to analyse their preferences, behaviour and attitudes. In data protection circles this kind of activity is referred to as 'profiling'. Profiling takes place when an organisation uses automated processes (technology in other words) to analyse personal information to learn about and predict an individual's performance at work, financial status, health, personal preferences, interests, reliability, behaviour, location, and movement. Read more about it here.



What about the United Kingdom?

The confusion around Brexit most definitely extends to data protection. The European Commission issued a notice to stakeholders. Essentially it points out that UK organisations will be treated in the same way as organisations from any other non-EU countries. In other words, EU organisations will no longer be able to freely transfer personal data to the UK.

The UK organisation will have to provide additional safeguards. PwC argues that this should not concern UK organisations too much. From the perspective of South African organisations, the fact that the UK will no longer be part of the EU, does have relevance when determining whether the GDPR applies.

POPIA *and* GDPR?

Do South African organisations need two compliance programmes?

Most organisations do not want to run one compliance programme, let alone two. So, the name of the game is to marry your GDPR compliance with your POPIA compliance. In other words, if you can help it, your GDPR compliance programme must always advance your POPIA compliance. The good news is that in most cases it will.

The United Kingdom Information Commissioner's Office has developed ***12 steps*** that all organisations who are subject to the GDPR should take now. We have gone one step further by indicating whether similar steps are required in terms of POPIA.

Step 1.

Awareness

Organisations must ensure that decision makers and key people know that the law is changing.

POPIA requirement

Yes. It is a requirement in terms of the draft POPIA Regulations that the organisation must ensure that employees receive POPIA training.

Step 2.

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.

POPIA requirement

Yes. 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.

Do South African organisations need two compliance programmes? (cont.)

Step 3.

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.

POPIA requirement

Yes. 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.

Step 4.

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.

POPIA requirement

Yes. POPIA also requires that people have the right to access, change or correct, and delete their personal information unless an exception applies.

Do South African organisations need two compliance programmes? (cont.)

Step 5.

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.

POPIA requirement

Yes. 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 POPIA.

POPIA and PAIA do not prescribe a specific timeframe within which access has to be granted. The timeframe just has to be reasonable.

Step 6.

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.

POPIA requirement

Yes. POPIA contains a virtually identical requirement.

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

Do South African organisations need two compliance programmes? (cont.)

Step 7.

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 can't be asked on a 'take it or leave it' basis. If the person can't refuse or withdraw the consent without a negative effect, it isn't 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.

POPIA requirement

Consent also features strongly in POPIA. In many instances, organisations will be able to get around complying with the principles of 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 POPIA is qualified in this fashion.

The important question will be when consent will be considered valid. In 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 can't have the product. We question whether such a 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.

Do South African organisations need two compliance programmes? (cont.)

Step 8.

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.

POPIA requirement

Yes. 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, POPIA requires parental or guardian consent.

Step 9.

Data Breaches

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

POPIA requirement

Yes. POPIA requires breach monitoring and response policies and procedures. Not having this in place has sunk many businesses.

Step 10.

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.*

POPIA requirement

Yes, but not in so many words. POPIA requires that all processing activities should be assessed, but privacy by design or privacy impact assessments are not mentioned specifically. 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.

Do South African organisations need two compliance programmes? (cont.)

Step 11.

Data protection officers

Organisations should designate someone to take responsibility.

POPIA requirement

Yes. 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 POPIA also allows for the designation of Deputy Information Officers.

Best practice is for organisations to have Deputy Information Officers and privacy officials (sometimes called privacy stewards or champions) in each business area. If POPIA compliance is not written into a number of people's job descriptions, POPIA compliance won't work.

Step 12.

International

Organisations should designate someone to take responsibility.

POPIA requirement

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.

Which organisations should be really worried?

Any compliance effort should be risk-based. In order to make sure that organisations spend what limited funds they have available for compliance wisely, any compliance initiative should focus on the high-risk areas. If any of the activities mentioned in this section are important parts of an organisation's operations (or will be in the future), urgent action is probably required to make sure that business will not be interrupted by a regulator.

High-risk areas for GDPR compliance

Risky Business	Is it a high risk in terms of POPIA too?
Routine processing of sensitive personal data. ***What is sensitive personal data?*** It is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, or biometric data.	Yes. The definition is very similar. POPIA adds information about criminal behaviour that relates to alleged offenses or the prosecution of those defences.
Automated decision making based on profiling. The European Commission has issued ***draft guidelines*** on this topic. We also found ***this blog*** useful.	Yes, but not to the same degree.
Buying and selling personal information.	Yes.
Sending data around the world.	Yes.
Products and services where children are the target market.	Yes.

What will happen to organisations who don't comply?

One of the biggest (and certainly most frightening) changes made by the GDPR is the increase in the size of the fines that may be issued for non-compliance. For serious infringements, the fines can be as much as 4% of the organisation's global turnover or €20 million (whichever will hurt the most), making the R10 million for a POPIA transgression look like chump change.

As is the case with POPIA, the GDPR will also allow data subjects to pursue claims for privacy infringements against organisations. In the case of POPIA the claims can be brought by the Information Regulator itself. Provision is also made for class actions.

Very often, the true damage caused by data breaches is not the cost of litigation or fines. The biggest risk lies in the massive reputational harm suffered by organisations who suffered a breach. The recent *Equifax breach* serves as a grim reminder of the extent to which a breach and an ineffective response by an organisation can wreak havoc on the trust of consumers and the bottom line.

This whitepaper is used with the permission of *Novation Consulting.*