Compliance is key
General Data Protection Regulation
Introduction

Compliance with the European Union General Data Protection Regulation by South African Organisations

In the realm of data protection legislation, the European Union (EU) General Data Protection Regulation (GDPR) is one of the most progressive and advanced data protection legislation globally, and will replace the current Data Protection Directive (Directive), with effect from 25 May 2018 (with the GDPR having been formally adopted in May 2016).

The current Directive only applies to organisations which are either established in the EU or European Economic Area (EEA) whereas the GDPR will now be applicable to organisations that do not have a presence in the EU/EEA or utilise equipment such as servers situated in the EU for the storage or processing of personal information. The location of the individuals whose personal data is processed, is immaterial (as further explained below).

One of the major practical considerations of the GDPR is its extra-territorial application to organisations which do not have a physical presence within the EU. Prior to the introduction of the GDPR, South African organisations engaging in commercial interactions with European data subjects such as employees, customers or business partners, were not strictly required to comply with the Directive, unless they had an establishment within the EU. Conversely, in order to fall within the purview of the GDPR, a South African organisation need not have any establishment or utilise any data processing equipment within the EU. However, it must be noted that if a South African organisation has an establishment within the EU (irrespective of the form of the establishment), the GDPR will apply irrespective of where the data processing takes place. Consequently, apart from having a physical establishment in the EU engaging in data processing activities, the GDPR will apply to South African organisations which do not have an EU presence, but:

• they process the personal data of individuals in the EU
• they have employees based in the EU
• they target individuals in the EU through either, the offering of goods or services to such individuals, or the monitoring of their behavior in the EU
• they transfer personal data to or receive personal data from the EU.

In respect of the above, it is crucial to understand that citizenship or nationality of the data subjects whose personal data is processed, is not the determining factor. Whether or not South African organisations are targeting individuals within the EU (more often than not, residents), will determine whether or not GDPR compliance should form part of such organisations’ risk and compliance agenda. The ‘targeting’ of individuals thus relates to whether or not an organisation intends to operate within the EU market, despite not having a physical presence there. The GDPR requires non-EU organisations to whom the GDPR applies, to potentially, in certain circumstances, appoint a representative in the EU, who would liaise with the relevant data protection authorities in the EU on data protection matters concerning the organisation. Therefore, where it is clear that an organisation offers goods or services to, or monitors the behaviour of individuals within the EU, a representative must be appointed and be based in the EU member state where the relevant data subjects are situated. There are exemptions to this requirement in certain limited circumstances.
One of the key differences between the GDPR and the Directive is that, unlike the Directive, the GDPR is automatically enforceable within EU member states and does not, in contrast to the Directive, have to be transposed into EU member state legislation. The GDPR therefore, harmonises the application of data protection legislation throughout the EU. South African organisations which are either based in the EU, or who target customers and business partners in the EU, need to be aware of this application for purposes of their data protection compliance initiatives.

In addition to preparing for the GDPR, South African organisations need to also deal with the imminence of the Protection of Personal Information Act 4 of 2013 (POPIA).

The Importance of Complying with Data Protection Legislation
Business has become inextricably linked with technology and the electronic transmission across various jurisdictional borders of data, including personal data, has become the norm. Numerous South African organisations of many sizes within various industries, engage in global commerce on a daily basis. Such global commerce occurs electronically and involves the exchange of personal data – in the absence of such exchanges organisations would be precluded from conducting business and tapping into global markets, including the market falling within the jurisdiction of the EU.

As such, data protection legislation such as the GDPR and POPIA have been introduced to ensure that organisations conduct their undertakings in a manner that respects and upholds individuals’ right to privacy and data protection. Consequently, compliance with the GDPR is an organisational issue, not a compliance issue, and would enhance a South African organisation’s ability to engage with EU customers, business partners and other stakeholders in order to maximise organisational objectives. Our experience shows that the competitive advantages of complying with the GDPR cannot be overstated as far as South African organisations are concerned, as EU stakeholders would likely be more comfortable to engage with South African organisations whose organisational processes and procedures are demonstrably in alignment with GDPR requirements – as they would.

3. All references to the EU include references to the EEA
Challenges faced by South African organisations from a GDPR perspective

One of the fundamental challenges which, it is envisaged, South African organisations will contend with, is the issue of what triggers the GDPR’s applicability.

Therefore, the main risk for South African organisations is to assume that the GDPR does not apply in instances where it does, and vice versa, which may result in unnecessary costs to the organisation – whether in the form of regulatory fines and sanctions, or compliance overheads which could have been avoided.

To understand these challenges further, we will expand on the applicability of the GDPR to South African organisations and how they may readily understand, in any particular scenario, whether they fall within the ambit of the GDPR’s extra-territorial application. The main trigger which we will focus on, is the targeting of individuals within the EU through either offering them goods or services or monitoring their behaviour in the EU.

How does a South African organisation determine whether it is offering goods or services to individuals in the EU?

Many South African organisations which engage or target individuals within the EU may erroneously assume that they are not required to comply with the GDPR if they do not have a physical EU presence. Moreover, organisations which have localised their website or made it accessible to individuals in the EU, may erroneously assume that this automatically triggers GDPR applicability. However, mere accessibility of a South African organisation’s website by individuals in the EU is not conclusive. Whether or not a South African organisation engages in the offering of goods and services to individuals within the EU is a factual enquiry. If we look at an example of a South African-based online organisation/store, the following questions should be asked to determine if such an organisation offers goods and services to or monitors the behaviour of individuals in the EU:

- Does the website make reference to customers who are EU residents? For example, in order to promote our goods and services, do we make reference to Spanish customers who use our products and services?
- Does the organisation use the local language of the EU member state in question where customers are based, and is this language relevant to South African customers? For example, does the organisation use Spanish despite the website emanating from South Africa as a South African-based organisation?
- Does the website happen to use the domain name of an EU member state? For example, does the website end in “.es” (Spanish website domain) or “.be” (Belgian website domain)?
- Does the organisation engage in targeted advertising campaigns which are directed at individuals in an EU member state?
- Is most of the organisation’s customer base situated within an EU member state?
- What currency is used or referred to on the organisation’s website? When promoting goods and services on the organisation’s website, are the prices indicated in Rands or Euros?
- Are the goods delivered to a physical address in an EU member state?

A risk-based approach should be adopted in weighing up the above considerations in order to determine whether a South African based online organisation (without an EU presence) specifically targets customers within the EU. In this manner, it could be determined whether such South African organisation is affected by the ‘long arm’ of the GDPR. Our view is that it is more prudent to comply with the GDPR where you have any association with EU-based customers or business partners. The degree of compliance efforts would differ from organisation to organisation.

As far as the monitoring of individuals’ behaviour in the EU is concerned, South African online organisations should consider whether they use advertising, targeting or web analytics cookies which could be used to profile its website users who access its website in the EU, as these could potentially trigger the GDPRs applicability.

Potential Impact of the GDPR to South African organisations and the Imminence of POPIA

Apart from having the GDPR to consider, South African organisations first and foremost, need to take POPIA into consideration. The effective date of POPIA may potentially be proclaimed in early 2018, giving organisations 12 months within which to get their processes and procedures compliant from a data protection perspective. The importance of complying with POPIA cannot be emphasised enough – especially in light of South Africa’s Information Regulator (Regulator) having been established and
in the process of laying its structural and administrative foundation. Thus, the pertinent question which arises is “why do South African organisations need to be concerned with POPIA first”? We will assess precisely why this is necessary in order to streamline an organisation’s GDPR initiatives.

South African organisations need to be aware that the data protection principles delineated in POPIA are, to a significant extent, based on the GDPR (See Fig.1 below). Thus, ensuring that regulatory, organisational and technical measures are in place for POPIA compliance would automatically tick many “boxes” for GDPR compliance – though this exercise is by no means, a ‘tick-box’ exercise. We recommend that organisations map the similarities and differences of POPIA to the GDPR and ensure that there is an integration of existing POPIA compliance programmes into any envisaged GDPR compliance initiatives.

The differences between POPIA and the GDPR should be nuanced where necessary, and a risk-based approach applied, to determine which specific risks the South African organisation faces – in light of its industry, geographic footprint and types and volume of personal data being processed to advance organisational objectives. The privacy and data protection control environment should be commensurate with these factors. It is crucial to note that the GDPR may carry a higher standard of compliance, hence, a South African organisation’s processes and procedures should be nuanced, where necessary.

In the event that organisations have not commenced their POPIA compliance programmes as yet, we advocate that organisations implement data protection “quick wins” which cover the data protection principles outlined in Fig.1. These should be undertaken with a GDPR-specific focus, as it would enable automatic POPIA compliance to a certain extent as well, due to the GDPR being the more robust standard and data protection framework. Appropriate mitigating measures in accordance with the level of risk should be applied in this regard, and would potentially enable South African organisations to simultaneously become, what we refer to as “GDPR-ready” as well as “Regulator-ready”.

The failure by any organisation to be “Regulator Ready” timeously constitutes a slippery slope towards non-compliance with POPIA. The risk of non-compliance could potentially attract fines from the Regulator of up to R10 million per breach, or the imposition of imprisonment for a period not exceeding 10 years, depending on the level of non-compliance. Furthermore, such a fine and/or imprisonment may consequently be accompanied by diminished profits due to the loss of customer, investor and overall stakeholder confidence as well as any protracted law suits. Moreover, GDPR penalties could potentially carry fines of 4% of an organisation’s annual global turnover or 20 million Euros, whichever is greater. The combined fines of the Regulator and any EU data protection authorities could effectively cripple organisations financially.
### Common Data Protection Principles/Themes between the GDPR and POPIA

- Accountability and Data Protection Governance
- Data Collection, Consent and Processing Limitation
- Purpose Specification
- Retention and Destruction
- Further Processing and Data Quality
- Openness and Security Safeguards
- Third-party Processing
- Data Breach Notification
- Special Personal Data and Children's Personal Data
- Direct Marketing and Automated Decision Making
- Cross-Border Data Transfers
- Data Subject Rights and Data Subject Participation
- Appointing a Data Protection Officer
- Enforcement and Penalties

Fig. 1: Common GDPR and POPIA Data Protection Themes
Solutions for South African organisations to ensure compliance with the GDPR

There is no one-size-fits-all or silver bullet solution to data privacy compliance, whether in respect of the GDPR or POPIA.

Furthermore, with the imminence of both the GDPR and POPIA (more so the GDPR as there is a definitive commencement date), it is not possible to ensure full compliance by the respective commencement dates. In our experience, attaining full data privacy compliance is a complex and lengthy process which, depending on the size and industry of the South African organisation in question, could take between two and five years to effectively embed into the organisation’s business operations – it entails a significant overhaul of an organisation’s governance structures and people, processes and technology.

Nonetheless, to prevent last-minute panic and avoid a “wait and see” approach, South African organisations should, henceforth implement certain cost-effective “quick wins” to get the ball rolling and ensure that they are on the path to GDPR compliance. These quick wins should ideally be initiated within an organisation’s high-risk areas which process personal data, and they would help to demonstrate to any EU data protection authority (as well as the Regulator), that your organisation is able to demonstrate GDPR (and POPIA) compliance to a reasonable degree. In this regard, we suggest that South African organisations adopt the following approach, in the event that no data protection compliance measures have been put in place as yet:

- Look at jurisdiction first, as we have discussed above. Determine whether your organisation, based on its business model, falls within the ambit of the GDPR;
- If it is clear that your organisation falls within the application of the GDPR’s extra-territoriality principle, commence with a mapping exercise of the GDPR and POPIA. In the event that your organisation has not yet commenced with POPIA compliance, GDPR compliance initiatives should immediately be commenced – leveraging off the aforesaid mapping exercise. This would augment any POPIA compliance initiatives to be implemented. However, in the event that your organisation has already initiated POPIA compliance initiatives, these may be integrated into your GDPR compliance programme, leveraging off the regulatory similarities and nuancing the differences, where applicable
- Design and implement a one to three-year roadmap and implementation plan, applying a risk-based approach and focusing mainly on the GDPR, due to the imminence of its commencement (being 25 May 2018);
- Implement streamlined and cost-effective quick wins such as the following:
  - Data Privacy Risk Analysis (Risk Analysis) and Data Privacy Impact Assessment (DPIA)
    Does your organisation engage in any “high-risk” data processing which could result in the risk of a GDPR breach? If so, then a documented DPIA should be undertaken. The DPIA will assess whether your organisation’s data processing activities are indeed “high-risk” and will identify the mitigating controls to be embedded within the high-risk activities, which could entail the processing of sensitive or special categories of personal data (such as health data, race and religion), or data processing activities which involve the systematic monitoring or evaluation of data subjects (such as profiling them for business purposes or monitoring them via closed circuit television). The Risk Analysis would seek to outline your organisation’s “as is” state in relation to its business activities which involve the processing of personal data.
  - Privacy Incident Management Plan, Processes and Procedures
    Privacy Incident Management Plan, Processes and Procedures allow your organisation to be more proactive, and less reactive, in effectively dealing with any incidents involving the loss, damage or unauthorised access to the organisation’s data, including personal data. In this regard, you should determine whether your organisation has a process in place for the logging and management of incidents. Is there a breach register in place? Organisations should be aware that the GDPR requires incident to be reported to a relevant data protection authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the incident. Moreover, a risk-based approach should be applied in this regard as the GDPR obviates the need for reporting incidents where they are unlikely to result in any risks to individuals.
Personal Data Lifecycle Inventory (Data Lifecycle Inventory)
This is a consolidated document which indicates what types of personal data are collected, used and stored within an organisation. Consider whether your organisation is aware of the various categories of personal data it collects, processes and shares, and whether it has a holistic view of data flows and where all personal data may reside (both hardcopy and electronic records comprising personal data). In addition, consider third parties with which your organisation shares personal data and why. Having a Data Lifecycle Inventory in place will assist your organisation in understanding where its high-risk areas are, and which systems are used for the various personal data processing activities. For example, it may reveal that the high-risk processing activities occur predominantly in your human resources department, and give you an idea of the mitigating controls to be embedded within the relevant business processes. You would then need to decide whether the existing controls are sufficient or which require enhancement.

Data Privacy Governance and Target Operating Model (Operating Model)
An Operating Model provides an overview of the proposed impact of data protection on the internal structure, roles, responsibilities and management of an organisation and its business areas. There is no standard Operating Model for data privacy compliance purposes. It is crucial to determine whether your organisation is required to formally appoint a data protection officer for purposes of the GDPR. An additional consideration is determining who your organisation’s information/privacy officer will be for POPIA purposes.

Privacy Policy and Privacy Notice
A Privacy Policy prescribes and defines the handling practices and obligations that staff must abide by when processing personal information. A Privacy Notice sets the tone and defines your data privacy mission statement for your organisation’s external stakeholders.
Implementing, operationalising and maintaining a GDPR compliance program should be of paramount importance for most South African organisations operating in, or seeking to expand their operations into, the EU market.

Given the imminence of the May 25, 2018, enforcement deadline, now is the time to get started with all compliance initiatives, and no less can be said for the commencement of POPIA.

Our Technology and Data Privacy team, having assisted numerous large multinational clients in a myriad of industries, are well-placed to partner with your organisation on its GDPR (and POPIA) compliance journey.

Conclusion
Contacts

Southern Africa

Navin Sing
Managing Director: Risk Advisory Africa
Tel: +27 83 304 4225
Email: navising@deloitte.co.za

Daniella Kafouris
Associate Director: Risk Advisory Africa
Tel: +27 72 559 0360
Email: dkafouris@deloitte.co.za

Dean Chivers
Risk Advisory Africa Leader: Governance, Regulatory & Risk
Tel: +27 82 415 8253
Email: dechivers@deloitte.co.za

East Africa

Julie Akinyi Nyangaya
Risk Advisory Regional Leader: East Africa
Mobile: +254 72 011 1888
Email: jnyangaya@deloitte.co.ke

William Oelofse
Director: Risk Advisory East Africa
Mobile: +254 20 423 0000
Email: woelofse@deloitte.com

West Africa

Anthony Olukoju
Risk Advisory Regional Leader: West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory West Africa
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

Central Africa

Tricha Simon
Risk Advisory Regional Leader: Central Africa
Mobile: +263 867 700 0261
Email: tsimon@deloitte.co.zm

Rodney Dean
Director: Risk Advisory Central Africa
Mobile: +263 867 700 0261
Email: rdean@deloitte.co.zm
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500\textsuperscript{®} companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018. For information, contact Deloitte Touche Tohmatsu Limited (814485/rina)