CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

Johannesburg
10 September 2018

GDPR SUBSTANTIALLY CHANGES THE MANNER IN WHICH PERSONAL DATA IS TREATED

By Terrance M. Booysen (Director: CGF) and peer reviewed by Dr. Peter Tobin (GDPR & POPIA Specialist)

In recent months, there has been much discussion and focus on GDPR -- the new European Union ('EU') General Data Protection Regulation 2016/679 -- which came into force on 25 May 2018. This EU legislation aims to strengthen the application and enforcement of data privacy laws, not only through its principles and the obligations it places on organisations, but also through its global reach.

Why should South African organisations understand the GDPR?

While the GDPR has a direct impact on individuals and organisations based in Europe, its provisions give rise to responsibilities for organisations based anywhere in the world; if they offer goods or services to residents of the EU, or if they monitor the behaviour of those residents, they are affected.

At some stage in the course of their operations, a large number of South African organisations -- especially those in the e-commerce sector -- will no doubt fall within the scope of the GDPR. This means that they will have to comply with the provisions of the GDPR. Indeed, this is no mean feat and becoming GDPR-compliant, let alone remaining compliant with its stringent provisions, is an onerous task for many organisations to contemplate.

"In an age of Big Data, 24/7 connectedness and ever-present surveillance, customers' demands for data privacy are greater than ever before. The most enlightened businesses will recognise this and grasp the GDPR compliance nettle with vigilance."

Consent and the GDPR - An Essential Guide (April 2018)

The task of GDPR compliance is made even more onerous in light of the fact that many South African organisations are still in the process of aligning their business systems, operations and procedures with the South African Protection of Personal Information Act 4 of 2013 ('POPIA'), which is still not fully in force at this point in time. POPIA, which is considered by many governance authorities to be less draconian than its GDPR counterpart, as it is based on legislation over 20 years old, seeks to protect personal information which is processed by public and private bodies and sets out various conditions which must be met before such processing is permitted.

The GDPR's key principles

The principles required by the GDPR include lawfulness, transparency and fairness in data processing, as well as accountability for compliance by organisations. Organisations processing data must have a specified, explicit and legitimate purpose for doing so and this must be indicated to individuals when their personal data is collected. Organisations may only collect and process the specific personal data necessary to fulfil the intended purpose, and they should hold no more data than that which they strictly require.

The personal data which is collected and processed should be adequate, relevant, and limited to what is necessary. Moreover, organisations must ensure that the personal data which they collect and process is accurate and up-to-date, furthermore ensuring that the data is not stored for any longer period than is necessary.

Importantly, organisations must also ensure that appropriate technical and organisational safeguards are in place so that personal data is properly secured, and personal data must, among other things, be protected against unauthorised or unlawful processing, including accidental loss, destruction or damage.

What happens if South African organisations fall foul of the GDPR?

GDPR cannot be ignored simply because it has origins in the EU. In the ordinary course of their business operations, organisations should hold the principles espoused by the GDPR in high regard, not least for the reason that protecting people's private information is ethically correct as well as aligned with good governance practices.

For organisations that advocate the values of being a 'good corporate citizen', it is expected that they proactively engage -- amongst other activities -- the necessary means of protecting the privacy rights of all individuals associated with their business; albeit employees, suppliers and their customers. Whilst these organisations will still be required to 'ramp up' their data protection procedures to meet the provisions of the GDPR, those who choose to ignore this legislation may be severely punished. Organisations that fail to comply with the GDPR will be subjected to fines of up to 20 million Euros or four percent (4%) of their annual worldwide turnover, whichever is the greater.

Notably, non-compliance with the GDPR could also lead to lost customers and reputational damage, as well as damages payable to EU residents ('data subjects') in the case of a data privacy breach where organisational security systems were lacking. The worst case scenario is that organisations may be required to cease their processing of personal data entirely.

"There is not only one thing for companies to do to become GDPR-compliant - it is very much a multi-disciplinary project involving functions across the business, from HR to legal to finance to IT, security and so on. GDPR fundamentally tries to change the way that organisations think about personal data, and how it is treated. GDPR is as much about the people and processes as it is about the technology."

David Warburton, Senior Systems Engineer, F5 Networks (2018)

What should South African organisations be doing to comply?

There are many steps which organisations will need to consider in order to comply with the GDPR, ranging from briefing their governing bodies on this new piece of legislation to implementing and updating their Customer Relationship Management (CRM) systems across their entire supply chain.

Some important examples of specific actions to take include: ensuring that the correct people within the organisation understand the provisions and implications of the GDPR; having appropriate, automated systems and filters in place to identify when the GDPR is applicable to the organisation at any point in time, or deciding to comply with its provisions as a 'gold standard' of data protection legislation.

On the basis that a South African organisation is required to comply with the GDPR, noting that proactive measures should be taken to safeguard the personal information of EU residents, it would be wise for the organisation to adopt a "privacy by design" approach to all of their systems (e.g. information technology, security, legal and finance, etc.), rather than being passive, or reactive in the case of complaints or a data privacy breach. In fact under the GDPR *privacy by design* and *data protection*, impact assessments are mandatory in certain circumstances.

Privacy by design considerations should make provision for communicating appropriately with those EU residents whose data is collected and processed, this includes updating all the organisation's customer-facing documents and internet platforms in order to comply with the GDPR's requirements.

A data protection officer will need to be appointed in the organisation and a relevant supervisory authority will need to be appointed in the EU. Organisations will need to determine the circumstances in which personal data will be allowed to be processed and when it can be transferred between organisations and countries. In the event of any data privacy breaches, proper breach management steps and incident response processes will be required.

Considering the EU stakeholder

Those individuals affected by the GDPR now have more rights and protection against the abuse of their personal information than ever before. As priority stakeholders of an organisation, they are likely to cause organisations to drive the proper implementation of data privacy and protection measures. Considering the massive consequences linked to non-compliance with the GDPR, organisations clearly have a vested interest to implement effective safeguards that protect the intended beneficiaries.

The rights of data subjects are numerous under the GDPR and include, for example, the right to *receive clear and understandable information about the organisation processing their data*; *what data is being processed and the reasons why the organisation is processing that data*; the right to *object to the processing of their personal data*, or to *have their details corrected*; as well as the right to *request that their personal data is deleted* by an organisation. Data subjects have the right to *consent to the use of their information*, as well as the right to be *timeously informed if their data is lost or stolen*.

It is clear that the provisions of the GDPR are more onerous than local privacy-protection legislation -- such as POPIA in the South African

"The more the world's population carries out activities online, the more important it becomes for individuals to have their data privacy. The key to GDPR is giving control of that privacy to the data subject - to the individual. The EU is trying to change the way that we think about protection of data - it shouldn't be an after-thought, and we welcome the way that the EU is championing the importance of data privacy."

A Jacobsz, Managing Director at Networks Unlimited (2018)

context -- and the GDPR may become a catalyst that causes all organisations dealing with data subjects in the EU to set even higher compliance standards as compared to those contained in POPIA. These collective standards will serve to protect the use of EU residents' personal data -- including other citizens' personal data -- especially in light of increasing incidences of identity theft and its associated crimes.

The 'benchmark' standards set by the GDPR will also become increasingly indispensable in the context of the Fourth Industrial Revolution and the burgeoning use of Artificial Intelligence (AI) in everyday life, where systems, products and smart devices will require personal data in order to operate effectively and to capitalise on predictive behaviours.

ENDS

Words: 1,412

For further information contact:

CGF Research Institute (Pty) Ltd
Terrance M. Booysen (Chief Executive Officer)
Tel: +27 (11) 476 8264 / Cell: 082 373 2249
E-mail: tbooysen@cgf.co.za
Web: www.cgf.co.za

Peter Tobin Consultancy
Dr Peter Tobin (Independent Consultant: GDPR & POPIA Specialist)
Tel: +27 (0) 83 922 3444
E-mail: peter@p-t-c.co.za
Web: www.p-t-c.co.za