STEPS TO BECOMING GDPR COMPLIANT AS A SOUTH AFRICAN COMPANY

Category: Media and OTT,Privacy Law, Infosec, and POPIA,Technology Law
written by Nonhlanhla Ngwenya | May 23, 2018



There is a plethora of information relating to the necessity of compliance of the General Data Protection Regulation ("**GDPR**") , a European Union directive that will come into force on 25 May 2018. This legislation will fast forward European law into new ways of protecting personal data around the world especially given the advancing of modern technology and its ability to harvest how personal information is stored and shared.

Companies must attempt to keep up with the pace of this new law which in its framework strongly advises companies on what they must do to abide by the rules in order to protect personal information, including explicit consent, communicating with data subjects, implementing data protection through composite data policy and advising companies on whether they need a data protection officer. Failure to comply may lead to the company being fined up to 4% of their global turnover or otherwise they can be sanctioned including an injunction to cease all commercial activities dealing with personal data, depending on the gravity of the violation.

Within an ever-globalized world with free data processing, companies generally don't have their geographic foot print limited. It's important for companies that suspect that they will be affected by the GDPR to understand the streamline of personal and sensitive data arising from the EU that is being transferred to South Africa. I list below 5 key elements that South African companies who suspect they will be affected by the GDPR be aware of for GDPR compliance purposes.

1 Identify what is the GDPR and when it will come into force.

The General Data Protection Regulation (GDPR) is a European Union ("**EU**") directive. GDPR applies to any organization that is doing business in the EU and is collecting, processing and storing the data of EU citizens, no matter where the company is based or located. This applies the principle of 'long arm of jurisdiction.' The GDPR will effectively come into force 25 May 2018.

2 Generate a composite data policy

GDPR requires a company to understand the networks in production and trade that affect personal data and requires companies to organize data for GDPR compliance. This gives rise to the need of

companies doing business in the EU and collecting, processing and storing the data of EU citizens to run a data inventory. This will help companies to:

- map how personal data is stored;
- to review compliance practices and design on processing activities, that the company may require for each type of data it collects.;
- to further analyse the risks it may cause to the data subject. This is due to the fact that GDPR requires that companies must prove that they can protect the data of EU citizens from sign-up to delivery.

3 Seek explicit consent to gather data

Under the new GDPR, consent for gathering data must be given freely, and must be specific, informed and unambiguous. Consent cannot come from silence, pre-ticked boxes or inactivity.

4 Appoint a Data Protection Officer (DPO) to take responsibility for the regulatory compliance.

The DPO will take full responsibility in making sure that the company will take the needed measures to have its processes and information flow, according to the GDPR.

5 Data breaches and notifications

A company affected by the GDPR must adopt internal procedures for and require the same of third-party partners, in order to deal with data breaches.

These procedures should include identification of the actual data breach, investigation of the circumstances of the breach, assessment of the implications it may cause both to the company and to the data subject regarding his or her privacy.

This includes notification within 72 hours when data subjects are exposed to some risk, as well as the need for notification to the Supervisory Authority within no more than 72 hours when the data subjects are exposed to risk.

Therefore, if you suspect yourself to be at risk of GDPR non-compliance, ask yourself does my company get exposed to EU citizens personal information? If yes than GDPR compliance applies to you.