GDPR/POPIA – Where Technology and Ethics have reached crossroads

By Megan Grindell

Hansal International

GDPR (Genera Data Protection Regulation) came into effect on 25 May 2018. Its enforcement, preceded by a 24 months grace period, has seen an unprecedented data privacy shake-up in the last year.

Application
Whilst the data protection and privacy provisions under GDPR are principally extended to European Union (EU) citizens, the impact on the average South African business that holds and/or processes data of EU citizens has been significantly underestimated. This coupled with the fact that GDPR presents as a precursor to South Africa's (soon to be enforced) data privacy legislation POPIA (Protection of Personal Information Act), is now slowly dawning on the SA market.

Accountabilities
As a responsible corporate citizen you are now faced with an emerging challenge in that you will be held to account, in more ways than a mere fine, for what and how you process an individuals personal data. The misconception that this is purely an IT security issue must also be quickly dispelled.

Data
privacy is far more than merely securing data: it goes to the heart of decisions taken by an organisation as to what data is held by an entity and the legality, fairness and transparency thereof in legitimising its purpose.

Impact
A number of organisations have historically permitted many of our fundamental rights of privacy to be carried away on a 'wave of technological processes'. Data breaches in recent periods involving a number of high profile entities, including Equifax, Uber and, more recently, Facebook, have highlighted these exposures. We as data subjects (that is you and I) are reeling in the realisation that, unbeknown to us, not only is our personal information being passed from one processor to another across the world, but that we may also be the subject of manipulation as a consequence thereof. …think Cambridge Analytica here. Whilst we may understand and possibly even respect the developments in artificial intelligence (AI), which are largely enabled online through the use of cookies (which, simplistically, filters and processes information through your online choices and feeds you back information in alignment with such preferences), where do we draw the line?

Who owns PII (Personally identifiable information)
The most important factor with GDPR is that you draw the line effectively as the data subject. Through GDPR's enforcement, you are now the master of your own data, dictating to the controller (the entity who has 'loaned' your PII for a specific purpose and period) what, how, when and for what purpose your data may be used. This is a fundamental step in the realm of data privacy and social justice and gives justifiable effect to the privacy rights of individuals across the world.

Enforcement

A large number of organisations with multi-jurisdictional reach have chosen to adapt the principles of GDPR in their operations across the world. No doubt we have all seen the notices in the last few weeks where those organisations that, mostly as a consequence of holding data on EU citizens, have had to 're-boot' their data privacy policies and, importantly, re-introduce themselves to the data subject. In addition, many have also had to advise the data subject on the use of cookies as a condition of use. There have been a number of different approaches to driving GDPR compliance with some
organisations merely re-introducing themselves to the data subject and providing a directed link to a revised data policy, coupled with a reminder of the data subjects right to unsubscribe (be forgotten). Others are seeking a more directed opt-in (providing clearer and, in certain cases, explicit consent) in line with GDPR. These options may be directed by the nature of the information held on the data subject, its purpose and, importantly, to what extent this information is processed. Under GDPR there is no effective grace period as is anticipated under POPIA. Enforcement will be immediate with fines of up to €20 million or 4% of annual global turnover representing the big stick of enforcement for GDPR. POPIA has far less punitive values but does extend its measures to include criminal offences.

The real consequences …
There are far more significant consequences of a breach of data privacy than the punitive fines. Firstly, in the event of a data breach under GDPR, the Supervisory Authority within each EU member state could enforce a shutdown of all processing activity until the exposure has been sufficiently addressed. The true effect of this can be illustrated in any online purchasing entity (and there are a number of significantly big ones around the world). Could you imagine the losses incurred if these operations were to grind to a halt as a consequence of a data privacy exposure? More importantly, and as is seen in the growing social conscience of the data subject, the indisputable reputational burden that it carries could present a consequence far greater than any punitive fine may impose. GDPR or not, it's just good practiceThis write up is not intended to go into the regulation in detail, save to say that GDPR, as with South Africa's POPIA, are excellent pieces of regulation giving effect to important social justice issues enhanced further through various E-Privacy Directives (locally and abroad). There is a growing recognition that the most significant risk to individuals' personalinformation is in fact driven by new technologies. It is incumbent on organisations now to ensure that innovation works hand in hand with privacy and that it is used in ways that are both ethical and moral.

MEGAN GRINDELL (ASSOCIATE)
www.hansal-international.com

Research sources:
• Ethics and Compliance Matters: NAVEX Global.co/blog
• EUGDPR.ORG
• ICO.ORG.UK
• FCPA Blog Alerts
• Michalsons.com/blog
Hansal International