EUROPEAN COMMUNITY (*'EC'*) GENERAL DATA PROTECTION REGULATION (*'GDPR'*) [945 WORDS]

There has been much hullabaloo about the GDPR of late - is the noise justified and where does the South African Protection of Personal Information Act (*'POPIA'*) fit into the picture?

Before you carry on reading and reach out for a cup of coffee (or something stronger!) to clarify the confusion and complexity, let's **make one or two things quite clear**:

- The GDPR is the first comprehensive review of privacy legislation in the EC for **20 years**
- It has in fact been **around for 2 years** i.e. it came into effect May 24 2016 - May 25th 2018 in simply the expiration of the 2 year **grace period** provided for (Similar to our Consumer Protection Act ('*CPA*') and POPIA)
- It applies to all entities wherever they are **in the world** that provide goods and services to any consumer who resides in any of the 28 EC member states
- Given the more pervasive nature of the GDPR, it is recommended that it be used as a standard rather than POPIA (see *'aims'* below)
- You will see references to *'Privacy Shield'* (formerly *'Safe Harbor'*) - this only applies to data exchanges between the EC and the USA

So as an opener and to ease your mind let's look at some of the key **similarities** and then some of the key **differences** between the GDPR and POPIA:

SIMILARITIES

- 'Data Subject' is described more broadly e.g. a person who can be identified by an 'identifier' such as user name or web cookie - this appears in POPIA where it refers to 'personal information' as including such an 'online identifier' (Read with definition of 'unique identifier')
- 'Personal Information' is called 'Personal Data'

- The POPIA 'Responsible Person' (one who 'determines the purpose of processing') is called a 'Controller'
- The aforesaid role is extended to a so called 'Processor' i.e. an entity/person that processes personal data on behalf of the controller e.g. a developer or analyst, referred to in POPIA as an 'Operator'
- The POPIA 'Information Officer' is called a 'Data Protection Officer' BUT the definition stipulates that such a person must have 'an extensive knowledge of data privacy laws and standards'
- As with POPIA 'consent' is not required in the case of a 'lawful basis' (Section 11 (1) (c) & (e)) or 'legitimate interest' (Section 11 (1) (d) & (f))
- It is not stated in POPIA but as you may know from my previous articles, I am of the view that the POPIA Information Officer (GDPR 'Data Protection Officer'*) can be an external or internal appointment - the following aspects of the GDPR may be a useful guideline for an internal appointment: ensure there is no conflict of interest e.g. a financial director as opposed to the IT director or manager. Additional guidelines appear in the definition* i.e. legal, security or accounting background and knowledge of privacy.

DIFFERENCES

- 'Data Subject' does NOT include legal entities (juristic persons) e.g. companies - only natural persons can rely on the protection of GDPR
- The fines are materially higher i.e. the greater of 4% of the entity's global annual revenue or €20 million - compare with the POPIA R10 million. However during the period 2016/'17 of the 17300 cases investigated in the EU, only 16 fines were imposed and the highest was £500 000, 00 and this was because the breach impacted 3 million people!
- The Data Protection Officer is only required for public authorities
- So called 'smaller firms' i.e. less than 250 employees do not have to comply with certain GDPR requirements (See list in GDPR) but they must keep a record of processing if there is 'a risk to the rights and freedoms of the Data Subject'

- Data breaches must be conveyed to the authorities and affected consumer within 72 hours - POPIA states '.. as soon as reasonably possible... ' (Section 22 (2))

Now let's briefly discuss the **aims of the GDPR** which, whilst aligned with POPIA, is worth considering in more detail:

- Assess security and privacy risks by means of a data protection impact assessment i.e. identify when processing may result in risks to data - what is required is a 'systematic and extensive evaluation of the organisation's processes and what safeguards it has'
- The assessment should address the origin, nature, likelihood and severity of such risks
- Business must show that it has implemented strategies not only to identify and pre-empt risk but also to manage and mitigate same.
- Preventative measures can include encryption and controlling privileges of users - ideally it should be impossible to tamper with and/or destroy data (See POPIA section 19)
- Regular audits of data must be carried out and monitoring must of be of such a nature as to detect breaches as early as possible
- It is imperative that security applies to the entire life cycle of data
- Incident response must be swift as it will impact on customers, brand & share value : engage lawyers, PR, insurance and the authorities

The **IBM** report suggest that you look at the half full rather than the half empty glass and ***'Go Beyond Compliance'***:

- Cost benefit approach: in depth analysis of data processed and stored - if possible discard data that does not add value
- Make privacy part of corporate culture - it may well be a good idea to incorporate it in your corporate social responsibility policy, both from an ethical and moral perspective

- 'Leverage privacy to drive superior customer experience' - doing so may give you a competitive advantage, promote transparency, trust and brand resilience.

*I hereby wish to **acknowledge the copyright** of the following websites from where I obtained the bulk of the above information and quoted content:*

- www.go.oracle.com;
- www.government.diginomica.com;
- www.ibm.com;
- Forrester Research

LOUIS-THE-LAWYER

MAY 14 2018

DISCLAIMER

This newsletter/article is intended to provide a brief overview and is not intended as legal advice. As every situation depends on its own facts and circumstances, only professional advice should be relied on. Please contact Adv. Louis Nel at louis@louisthelawyer.co.za **or on +27 83 679 4556'**