Privacy implementation in South Africa – Quo vadis?

By Johanette Rheeder

The Protection of Personal Information Act, 2013 (POPIA) is yet to be implemented, and every now and again, South Africa is faced with the effect of privacy violations and cybercrime.

The City of Johannesburg (COJ), on 24 October 2019, announced a breach of its network by hackers and shut down its website and all e-services as a precautionary measure. In a tweet, the City said it had detected a network breach "which resulted in an unauthorised access to our information systems". A deadline to pay bitcoin as ransomware, set by a group calling themselves "Shadow Kill Hackers" has passed without COJ complying. The group sent a ransom note to the City of Johannesburg, demanding payment of 4.0 bitcoins by October 28 at 17:00, or it would upload all data it had hacked from the City's servers.[1]

This again, brings to the forefront, the question as to when POPIA is going to be implemented to provide the users of these systems such as COJ's network, with privacy protection?

According to recent studies in the South African privacy environment, 77% of South African decision-makers admit their organisation will suffer reputational damage, if fined for non-compliance with POPIA(Protection of Personal Information Act, 2013). The reputational damage can be more damaging than the financial penalties, as it involves loss of goodwill, unplanned costs and loss in client or customer trust. Penalties can include fines up to 10 million rand or imprisonment for Privacy officers (Heads of the organisations).

The burning questions with regard to Privacy protection in South African is not why we must comply anymore, but when are we going to start the process? Privacy protection are Constitutionally recognised in South Africa and places privacy protection in our Country on par with international protection such as found in Europe and England.

POPIA and its regulations require each organisation to do a protection of personal information impact assessment or commonly known as a Gap assessment, a compliance framework and a continued implementation plan. The regulations also require organisations to do awareness training amongst all its employees. After implementation, organisations will have one year to comply. High priority in terms of POPIA compliance should translate to determine the readiness of the organisation; and without a concrete PIIA and action plan to protect personal information, organisations will lag behind and may be caught off guard.

Unfortunately, in terms of data breaches, nobody knows when or where it is going to strike next, which is why being prepared is so important. Data breaches, such as experienced by COJ, is not the only risk organisations face, as technical and organisational security measures are but one of the eight conditions of POPIA that an organisation must comply with.

One year to comply is very short, especially taking into consideration that GDPR in Europe allowed two years to become compliant and only 30 to 40% of these international organisations are complaint yet, after GDPR came into operation on 25 May 2018.

[1]Source: https://www.news24.com/SouthAfrica/News/hackers-deadline-passes-city-of-johannesburg-says-it-is-not-paying-20191028