POPI AND GENERAL DATA PROTECTION REGULATION

POPI

29 August 2017

Presented by Mervyn E King SC

INFORMATION SECURITY (1)

- Critical in a world of cyber crime
- Hackers exploit an ecosystem built around a model of open collaboration and trust
- Cyber breach a much greater risk today than disaster recovery
- Estimated at 100 000 breaches per day on listed companies worldwide

INFORMATION SECURITY (2)

- Need to have a disaster recovery officer both for cyber breaches and for private information leaks
- Agenda item IT governance and security – King IV
- A clear, concise and understandable plan
- Cost benefit analysis
- Hot, cold and warm sites

BASIS OF THE POPI ACT

- Organisations should conduct themselves responsibly
- In the process of storing and sharing personal information
- Personal information seen as precious goods
- Act obliges the exercise of control over these precious goods

PERSONAL INFORMATION (1)

- Identity or passport number
- Date of birth and age
- Phone numbers
- Email address
- Online messaging identities
- Physical address

PERSONAL INFORMATION (2)

- Gender, race and ethnic origin
- Photos, voice recordings, video footage
- Marital relationship and family relations
- Criminal record
- Private correspondence

PERSONAL INFORMATON (3)

- Religious or philosophical beliefs including personal and political opinions
- Employment history and salary information
- Financial information
- Education information
- Physical and mental health information including medical history
- Membership of organisations

FACEBOOK & LINKEDIN

- Technology makes it easy to access information
- In criminal hands information can cause harm to individuals and companies
- Person has a duty, however, to protect him or herself
- The POPI Act cannot protect one if one does not care to protect oneself

ANY LEGAL ENTITY

- Act applies to other than a natural person
- Therefore includes a company or other legally recognised organisation
- All organisations are data subjects
- Afforded the same right of protection
- A company is a responsible party

UNIVERSAL APPLICATION

- Most countries have a POPI Act
- Purpose is to protect personal information of citizens
- Particularly to protect cross border transfer and the sharing of data
- Ignorance of the law no excuse
- The POPI Act is shortly to be implemented
- Time and effort needed to educate and train staff
- Updating IT processes in the company
- Early action is essential

GENERAL DATA PROTECTION REGULATION

- Designed to protect information of individuals within the EU
- Protects the export of personal data outside the EU
- The objective is to give control back to citizens and residents over their personal data
- Becomes effective from 25 May 2018

APPLICATION

- Applies to data controllers, data processors or the data subject being the individual
- Applied extra-territorially
- If information of EU residents is illegally used
- Applies to any information relating to an individual

ACCOUNTABILITY

- Has the right to question information made available purely on an algorithmic basis
- Has the right to an explanation
- Consequently measures are needed to include pseudonymising personal data by a controller
- What is adequate pseudonymising is question of fact in each case
- When information is encrypted the decrypting must be kept separate

PUBLIC AUTHORITY

- Public authority has to have a data protection officer
- Proficient at managing IT processes
- Governance and company requirements must be met in appointing the DPO

PSEUDONYMISATION

- Process that transforms personal data
- So that personal information cannot be attributed to a specific person
- The idea is to render the original data unintelligible
- Pseudonymisation is recommended in the GDPR

SANCTIONS

- Any breach of the GDPRs carries heavy fines
- Can result in the Supervisory Authority ordering regular periodic data protection audits
- Fines of up to 2% of annual global turnover of the preceding financial year
- If a breach of the GDPR's an individual can apply for the right of erasure

MANAGEMENT RESPONSIBILITY

- For all the structures, processes and mechanisms
- To execute the IT framework
- Is IT on track to achieve its objective?
- Is it resilient enough to adapt to the strategy?
- Is it adequately protected from the risks it faces?
- Can opportunities be proactively recognised and acted upon?
- CIO responsible for the management of IT
- If no CIO the service provider

THE CIO

- Understand the long-term strategy of the business
- Align with efficient and effective IT solutions
- Strategically integrate IT into the business strategy
- Exercise care and skill in developing IT solutions
- Act as a DPO

INFORMATION MANAGEMENT

- Management of risks associated with information and information systems
- Continuous monitoring of all aspects of information
- Ensuring data quality and security
- Establishing a business continuity programme

INFORMATION SECURITY

- Develop an information security management system (ISMS)
- Board should oversee the ISMS
- Management has to implement the ISMS
- ISMS should include :
- ensuring the confidentiality of information
- ensuring the integrity & security of information
- ensuring the availability of information and information systems in a timely manner

TECHNOLOGY CONVERGENCE

- Average is 3 electronic instruments
- iPhone, iPad, laptop
- Increases opportunity for attack
- Presents greater risks of the leaking of information
- Greater opportunity to obtain data

CONCLUSIONS

- Disaster and business continuity – DRO
- Cost/benefit analysis
- Secure information
- Bigger threat is cyber attack
- Response plan for cyber attack
- Audit for capacity and competency of a DRO
- DRO could also carry out function of DPO
- Destruction of evidence
- Insurance
- Board agenda item critical

THANK YOU

Prof Mervyn E King SC