DATA PRIVACY AND CYBERSECURITY

BY DATA PROTECTION COMMISSIONER

MOBIUS COMPUTING & BAKERTILLY

12 APRIL 2019

AGENDA

- THE DATA PROTECTION ACT 2017
- AIMS OF THE DPA
- THE DATA PROTECTION OFFICE
- FUNCTIONS OF DPO
- DPA & GDPR
- BIG DATA
- BIG DATA AND DATA PROTECTION CONCERNS
- ARTIFICIAL INTELLIGENCE
- AI AND DATA PROTECTION CONCERNS
- AI RECOMMENDATIONS
- BLOCKCHAIN
- BLOCKCHAIN AND DATA PROTECTION CONCERNS
- CYBERSECURITY
- OVERLOOKED AREAS
- STEPS TO A GOOD DATA PROTECTION OR CYBERSECURITY PROGRAM
- CONCLUSION

THE DATA PROTECTION ACT 2017 (DPA)

Replaces the Data Protection Act 2004.

Passed on 8th December 2017 at the National Assembly and presidentially assented on 23rd December 2017

Came into force on 15 January 2018

AIMS OF THE DPA

To strengthen the control and personal autonomy of data subjects (individuals) over their personal data

In line with the European Union's General Data Protection Regulation (GDPR)

To simplify the regulatory environment for business in our digital economy.

To promote the safe transfer of personal data to and from foreign jurisdictions

THE DATA PROTECTION OFFICE (DPO)

Public office which acts with complete independence and impartiality

Not subject to the control or direction of any other person or authority in the discharge of its functions

Head of the Office is the Data Protection Commissioner

FUNCTIONS OF DPO

I	• Ensure compliance with DPA 2017 and regulations
II	• Registration of controllers and processors
III	• Investigation of complaints
IV	• Sensitisation/ Training
V	• Exercise control on all data protection issues
VI	• Conduct data protection compliance audits
VII	• Cooperate with supervisory authorities of other countries
VIII	• Research on data protection

DPA & GPDR

DPA has been adapted from the GDPR for the Mauritian context

Similarities between the articles of GDPR and sections of the DPA

BIG DATA

Big data feeds AI.

AI algorithms need big data to fulfil their purpose.

Big Data and AI are very much interrelated.

Increasing internet, mobile and social media fuel an explosion in digital data volumes.

Availability of data at this scale provides the raw material for AI.

"In summary, big data can be thought of as an asset that is difficult to exploit. AI can be seen as a key to unlocking the value of big data; and machine learning is one of the technical mechanisms that underpins and facilitates AI. The combination of all three concepts can be called 'big data analytics". (Paragraph 11 of ICO: Big data and data protection 2017.)

BIG DATA ANALYTICS AND DATA PROTECTION CONCERNS

Use of complex algorithms and involves a "discovery" phase to find relevant correlations, which can be a form of machine learning.

Limited transparency on how algorithms work. "Black box" effect makes it very difficult to understand the reasons for decisions made by the algorithms.

Tendency to collect "all the data" as it is more easily available rather than limiting the analytics to random samples or statistically representative samples.

Often data is re-used for a different purpose for which it was originally collected, because it is obtained from third parties.

Involves data from Internet of Things (IoT) and "observed" data that has been generated automatically and new "derived" or "inferred" data produced by the algorithms is used further in the analytics.

ARTIFICIAL INTELLIGENCE (AI)

AI is the ability of a computer to perform tasks commonly associated with human beings

AI can cope with, and to a large extent is predicated on, the analysis of big data in its varying shapes, sizes and forms

AI AND DATA PROTECTION CONCERNS

Processing of personal used for different purposes than those originally set.

Hard to obtain express consent and withdrawal of consent often create operational issues that may not be unmanageable.

Legitimate interest may also be critical, as it requires a difficult balance between the rights of the data subjects and the legitimate interests of the controller.

Issue of inferred becomes even more relevant as anonymous information may be transformed into personal data, including special categories of personal data.

AI providers "reluctantly" allow audit and controls on their AI systems due to the complexity.

RECOMMENDATIONS FOR AI

- Privacy by Design
- Right not to be subject to decisions merely based on automated decisions making
- Data Protection Impact Assessment
- Privacy Enhancing Technologies

BLOCKCHAIN

Technical structure for the bitcoin

Shared, immutable ledger for recording the history of transactions

Applications in different fields

BLOCKCHAIN AND DATA PROTECTION CONCERNS

- **"The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner".**
- **Adequate protection from business perspective.**
- **Addressing a compliance process with the law after design phase**

CYBERSECURITY

Data Privacy or Cybersecurity: Which is More Important?

Both

OVERLOOKED AREAS

- **Bring Your Own Device**
- **The Cloud**
- **Voice and video**
- **People**

STEPS TO A GOOD DATA PROTECTION OR CYBERSECURITY PROGRAM

- Map out what data you have or intend to collect
- Determine what laws apply to that data
- Identify what security you have in place to protect it
- Prepare a gap analysis of what needs to be addressed
- Take steps to bridge those gaps
- Test to ensure compliance

CONCLUSION

Data privacy and cybersecurity are just two different sides of the same coin

Poor data privacy leads to poor cybersecurity

and vice versa

THANK YOU

Contact us:

Website: **http://dataprotection.govmu.org**

Email: **dpo@govmu.org**

Tel: **460 0251**