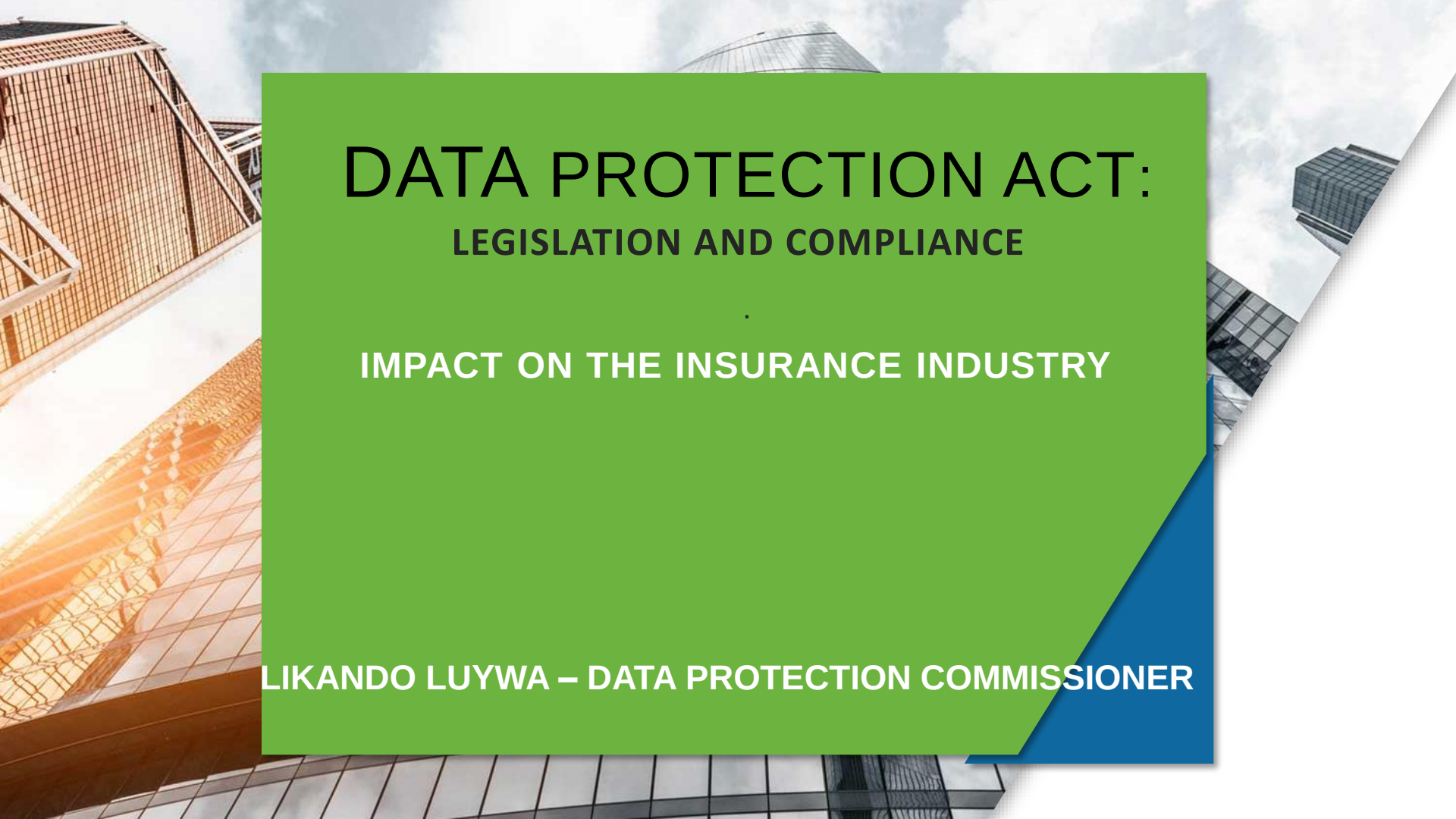


DATA PROTECTION ACT:

LEGISLATION AND COMPLIANCE

.

IMPACT ON THE INSURANCE INDUSTRY

LIKANDO LUYWA – DATA PROTECTION COMMISSIONER

THE DATA PROTECTION ACT

An Act to provide an effective system for the

- use and protection of personal data;
- regulate the collection, use, transmission, storage and otherwise processing of personal data;
- establish the Office of the Data Protection Commissioner and provide for its functions;
- the registration of data controllers and licencing of data auditors;
- provide for the duties of data controllers and data processors;
- provide for the rights of data subjects;

THE COMMISSION'S MANDATE

- To ensure an **effective use and protection** of Personal Data through regulating the Collection, Use, Transmission, storage, security and processing of Personal Data
- To Safe guard the data subject's rights
- To ensure compliance fairly and transparently

THE COMMISSION'S PROMISE

1. To enforce this law fairly and transparently
2. To ensure this law does not increase the cost of doing business
3. To bring data normality in the nation's data environment
4. To improve business environment

BACK GROUND TO DATA PROTECTION

1995: EU DATA PROTECTION DIRECTIVE

The European Union's Data Protection Directive and was the first instrument aimed at harmonised data protection within the union.

The Data Protection Directive created a baseline of the GDPR that echoed in data protection legislation globally.

1996-1999: UNITED STATES' HIPAA, COPPA, AND GLBA

The late-1990s saw increased sector-specific privacy regulation in the US. namely:

- Health Insurance Portability and Accountability Act of 1996 ('HIPAA'),
- Children's Online Privacy Protection Act ('COPPA').
- The Financial Services Modernization Act of 1999

THE COMMISSION'S MANDATE

2014: MALABO CONVENTION

The African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention'), where member states, agreed establish legal frameworks for cybersecurity and data protection.

2016-2018: INTRODUCTION OF THE GDPR

In 2016, the EU adopted the GDPR, which entered into effect on 25 May 2018, replacing the Data Protection Directive

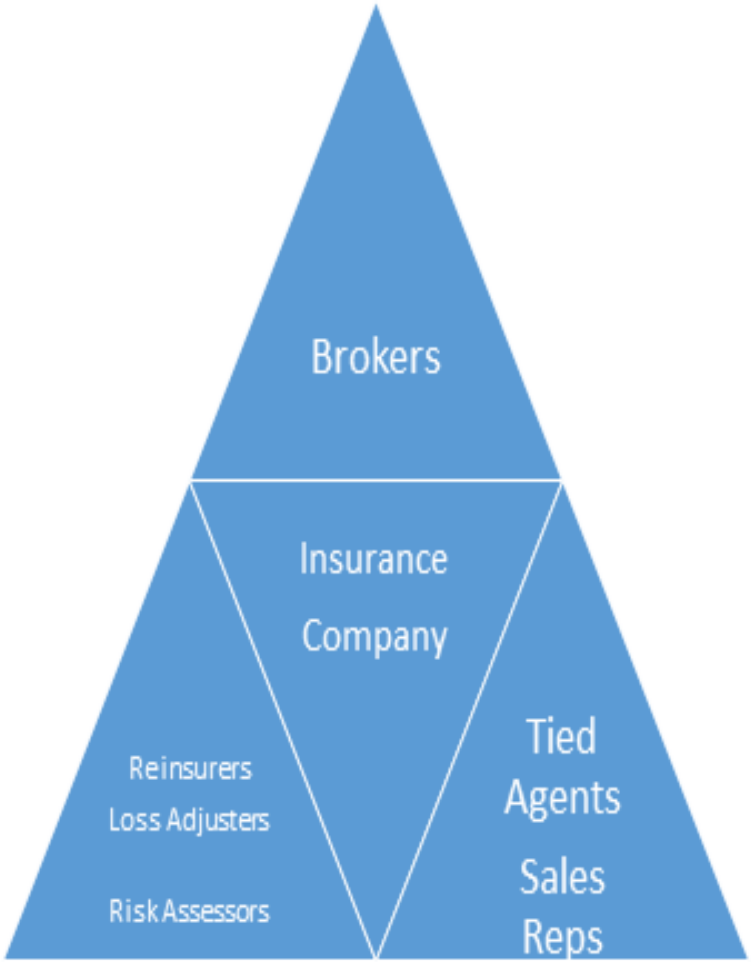
The GDPR is considered a privacy benchmark each EU member state enact Data protection Acts

GLOBAL PERSPECTIVE

- The DPA was as a results of the AU's Malabo Convention on Cyber Security and Data Protection of June 2014
- The AU's Malabo Convention was a result of the Data Protection Trends in the EU and First world
- In as much as only 20 countries have established Commissions 39/55 African States have enacted DP laws

Whilst the DPAct could be new to Zambia, It's not new to the region or Africa or the world as it is an off shoot from EU

WHO DOES THE ACT AFFECT



THE DATA PROCESSING PRINCIPLES

1. Lawfulness, Fairness, and Transparency

•- Process data lawfully and fairly. E.G. BANKING

•- Inform individuals about data collection and processing.

2. Purpose Limitation

•- Collect and process data for specific, explicit, and legitimate purposes.

•- Avoid processing data for secondary purposes without consent.

3. Data Minimization

•- Collect and process only necessary data.

•- Avoid excessive data collection.

THE DATA PROCESSING PRINCIPLES

4. Accuracy

•- Ensure data accuracy and quality.

•- Update and correct data regularly.

5. Storage Limitation

•- Store data for limited, specified periods.

•- Delete or anonymize data when no longer needed.

6. Security

•- Protect data against unauthorized access, theft, or damage.

•- Implement robust security measures (e.g., encryption, access controls).

THE DATA PROCESSING PRINCIPLES

7. Accountability

•- Demonstrate responsibility for data processing.

•- Appoint a Data Protection Officer (DPO) if necessary.

8. Data Subject Rights

•- Respect individuals' rights to:

- - Access
- - Erasure
- - Restriction of processing
- - Data portability
- - Objection

•9. Data Integrity and Confidentiality

•- Protect data integrity and confidentiality.

•- Ensure data is not modified or disclosed unauthorized.

THE
90s
Against
21st Centuary
Risks

Portable Devices

Floppy Disk 1.44Mb => SD card 1Tb

- Needed 70 floppies for 1 XRay |
  1 SD Card (875,000 Floppies) -19,000XRay imagines
- Needed 1 CDRoms for 2 XRay -
  To copy 19,000XRay imagines 9,500 CDRoms

Data Transfer Rate:

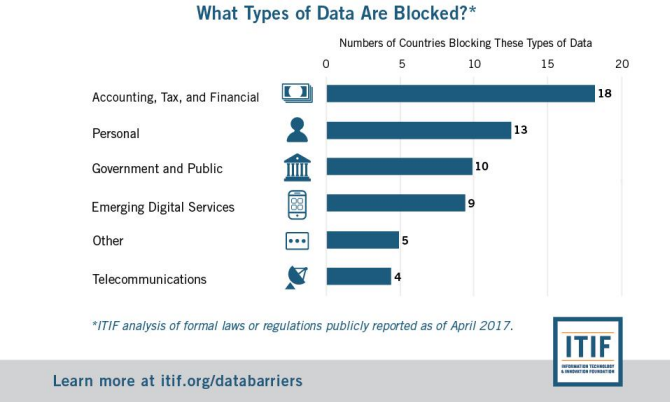
14.4kbs => 20-250Mbps Bursting to 500Mbps+

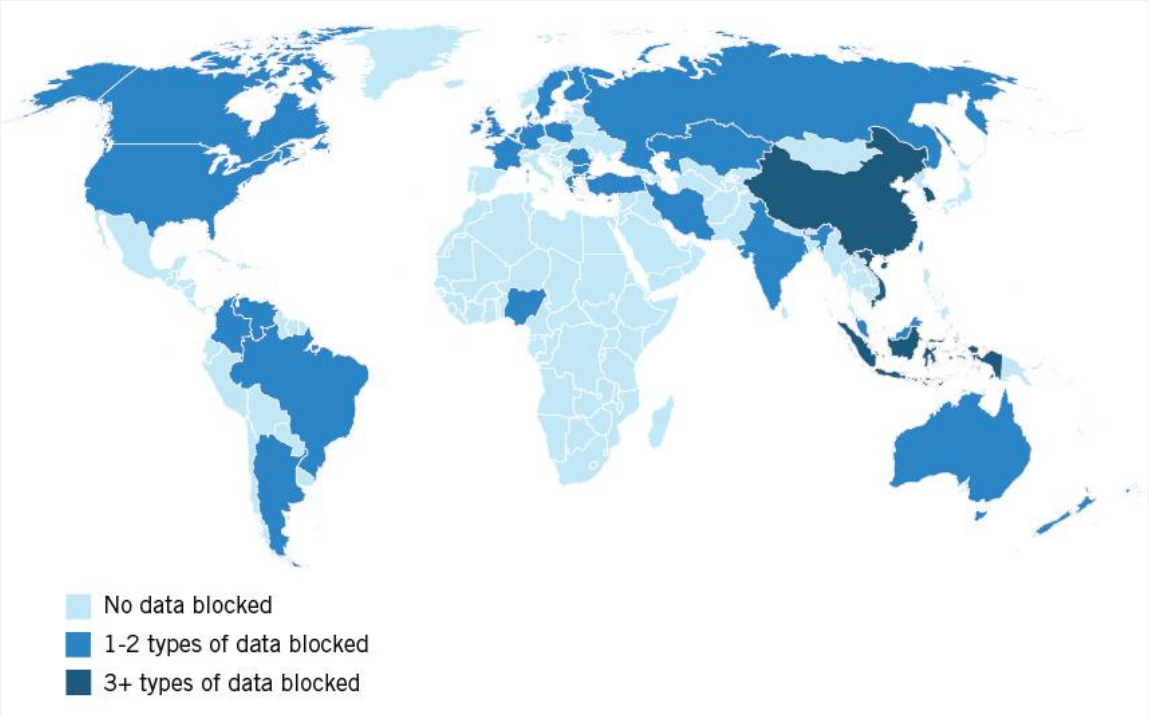
- almost 1 x-Ray/Sec on internet
- 93,000 high resolution x-Ray/min on FIBRE 5Gbps

Data Storage Costs

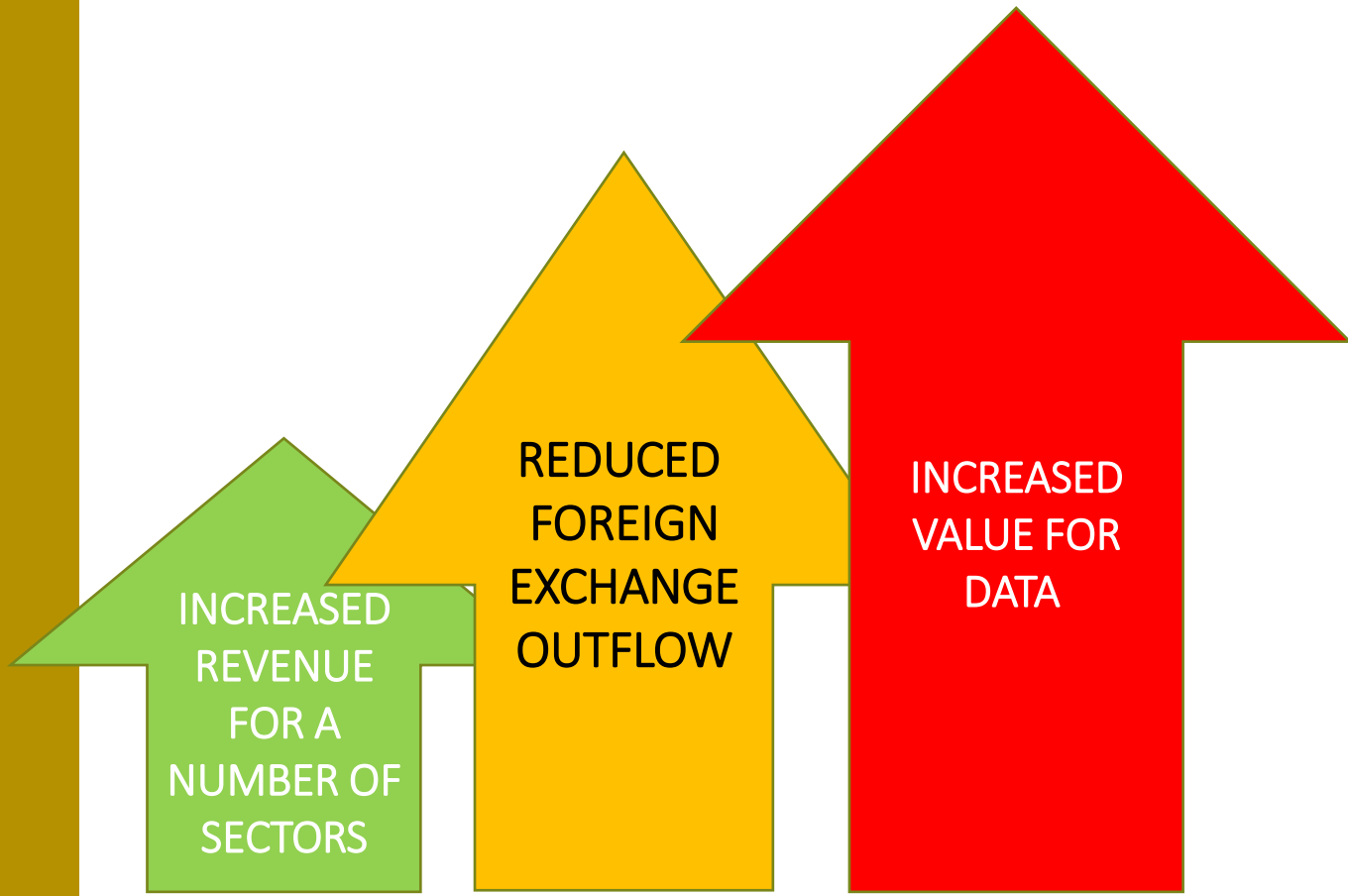
- 1990 1Gb/Month $10,000
- 2024 100Gb/Month => $2.00

Top countries that block data flow





FINANCIAL PERSPECTIVE (REVENUE INCREASE)



FAIRNESS OF THE ACT

Section 70(1)

Data Controller to process and **store personal data** on server or data centre located **in the Republic**.

Section 70(2)

Despite subsection (1), the **Minister may prescribe categories of data** that may be **stored outside the Republic upon Data Commissioner's recommendation**.

FAIRNESS OF THE ACT

Section 71

Where as the Data Controller can not transfer data outside **the Republic**.

The law gives many instances where data may be transferred outside Zambia and these include

- Nature of business
- Emergencies
- Commissioner's approvals
- Data subject's consent

OTHER MANDATORY PROVISIONS

19. (1) A person shall not control or process personal data without registering as a data controller or a data processor under this Act.

48. (1) Subject to subsection (2), a data controller and data processor **shall appoint a data protection officer.**

81. (1) The Data Protection Commissioner or an independent data auditor licensed by the Data Protection Commissioner under this Act shall, audit the policies of a data controller and the conduct of processing of personal data **annually**.

49. (1) A data controller shall notify the Data Protection Commissioner **within twenty-four hours of any security breach affecting personal data processed.**

SANCTION FOR BREACH

Section 55

Sanction for Breach by Body Corporate

Body corporate liable to **2% of Annual Turnover** of preceding financial year or 2 Million penalty units, whichever is higher.

Sanction for Breach by natural person

Natural person liable to fine not exceeding **1 Million Penalty Units** or **imprisonment** for no more than 10 years or both.

BENEFITS OF THE ACT

- Improved Data security
- Reduces Financial loss due to breaches
- Data Compliance will improve institutional reputation
- Adds Value to this commodity - Data
- Will Help Grow our local ICT capacity
- Will Create new business opportunities

Thank You

Data Protection Commissioner
LIKANDO LUYWA | 0966 762407
Likando.Luywa@dataprotection.gov.zm