DATA PROTECTION & PRIVACY

BIG DATA, MACHINE LEARNING, CONSUMER PROTECTION

Ms Patricia Adusei-Poku
Executive Director, Ghana - DPC

CONSUMER PROTECTION

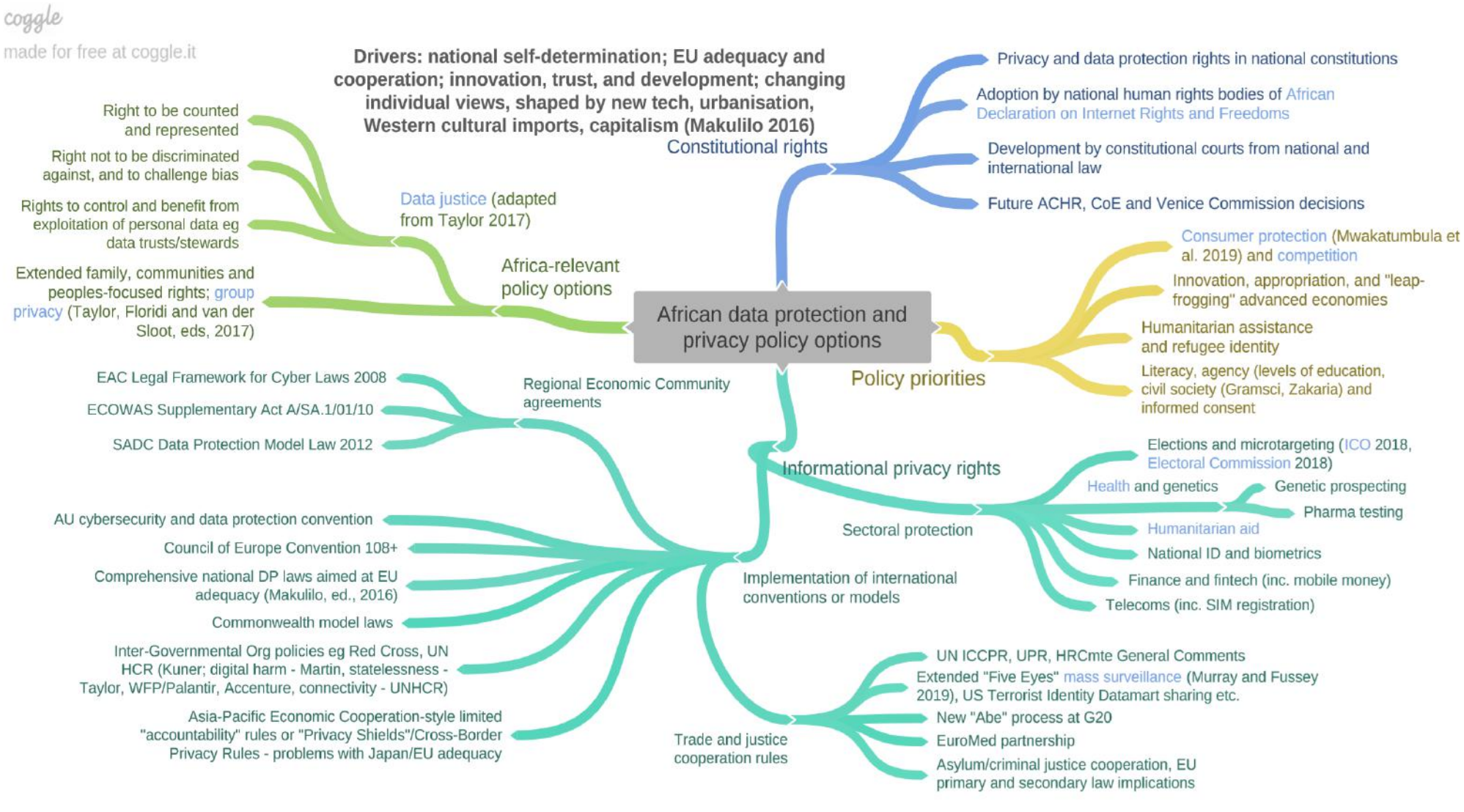
- The right to safety. ...
- The right to be informed. ...
- The right to choose. ...
- The right to be heard. ...
- The right to satisfaction of basic needs. ...
- The right to redress. ...
- The right to consumer education. ...
- The right to a healthy environment.

Preventing fraud and unfair practices in the marketplace

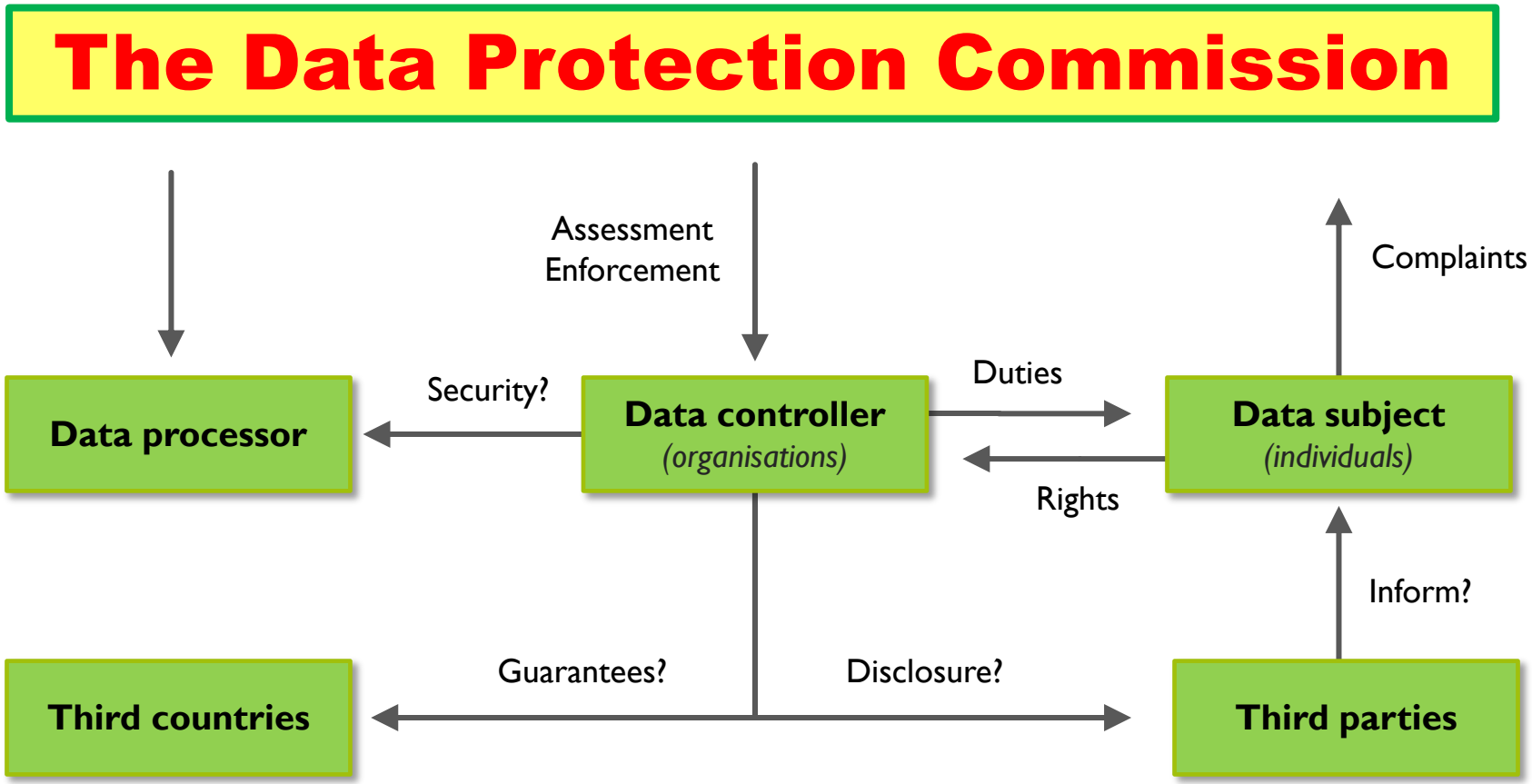
DATA PROTECTION & PRIVACY

- Measures to safeguard the processing personal data
  - accidental loss
  - unauthorized disclosure
  - unlawful use
- Regulating the processing of personal data
  - Empowering individuals

PRIVACY – A fundamental Human Right


coggle
made for free at coggle.it
Drivers: national self-determination; EU adequacy and cooperation; innovation, trust, and development; changing individual views, shaped by new tech, urbanisation, Western cultural imports, capitalism (Makulilo 2016)
African data protection and privacy policy options
Constitutional rights
Privacy and data protection rights in national constitutions
Adoption by national human rights bodies of African Declaration on Internet Rights and Freedoms
Development by constitutional courts from national and international law
Future ACHR, CoE and Venice Commission decisions
Policy priorities
Consumer protection (Mwakatumbula et al. 2019) and competition
Innovation, appropriation, and "leap-frogging" advanced economies
Humanitarian assistance and refugee identity
Literacy, agency (levels of education, civil society (Gramsci, Zakaria) and informed consent
Africa-relevant policy options
Data justice (adapted from Taylor 2017)
Right to be counted and represented
Right not to be discriminated against, and to challenge bias
Rights to control and benefit from exploitation of personal data eg data trusts/stewards
Extended family, communities and peoples-focused rights; group privacy (Taylor, Floridi and van der Sloot, eds, 2017)
Regional Economic Community agreements
EAC Legal Framework for Cyber Laws 2008
ECOWAS Supplementary Act A/SA.1/01/10
SADC Data Protection Model Law 2012
Informational privacy rights
Elections and microtargeting (ICO 2018, Electoral Commission 2018)
Sectoral protection
Health and genetics
Genetic prospecting
Pharma testing
Humanitarian aid
National ID and biometrics
Finance and fintech (inc. mobile money)
Telecoms (inc. SIM registration)
Implementation of international conventions or models
AU cybersecurity and data protection convention
Council of Europe Convention 108+
Comprehensive national DP laws aimed at EU adequacy (Makulilo, ed., 2016)
Commonwealth model laws
Inter-Governmental Org policies eg Red Cross, UN HCR (Kuner; digital harm - Martin, statelessness - Taylor, WFP/Palantir, Accenture, connectivity - UNHCR)
Asia-Pacific Economic Cooperation-style limited "accountability" rules or "Privacy Shields"/Cross-Border Privacy Rules - problems with Japan/EU adequacy
Trade and justice cooperation rules
UN ICCPR, UPR, HRCmte General Comments
Extended "Five Eyes" mass surveillance (Murray and Fussey 2019), US Terrorist Identity Datamart sharing etc.
New "Abe" process at G20
EuroMed partnership
Asylum/criminal justice cooperation, EU primary and secondary law implications

THE IDEAL STRUCTURE/MODEL



DATA SUBJECTS RIGHTS

- **Right to be informed**
- **Right to access**
- **Right to rectification**
- **Right to restrict processing**
- **Right to object**
- **Right to erasure**
- **Right to portability**
- **Right to freedom from automated decision making**
- **Right to give and withdraw consent**
- **Right to compensation**

DATA PROTECTION PRINCIPLES

1. Accountability	⟷ Demonstration of legal compliance with easily accessible documentary evidence
2. Lawfulness of Processing and Specification of Purpose	⟷ Providing evidence of legitimate grounds, fairness and transparency
3. Compatibility of Further Processing	⟷ Proactively obtaining customer consent for changed or new purposes
4. Quality of Information	⟷ Ensuring that data held is continuously accurate, available and up-to-date

DATA PROTECTION PRINCIPLES

5. Openness	**Keeping Data Subjects fully informed about their personal data via multiple channels**
6. Data Security Safeguards	**Use of appropriate of technology and organisational measures**
7. Data Subject Participation	**Empowering Data Subjects to exercise their legal Rights**
8. Purpose of Collection	**Processing personal data for clearly specified purposes only**

CONSENT

*any **freely given, specific, informed** and **unambiguous** indication of the data subject's wishes by which he or she, by **a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her.*

APPROPRIATENESS OF TECHNOLOGY AND ORGANIZATIONAL MEASURES

- ‘Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.’

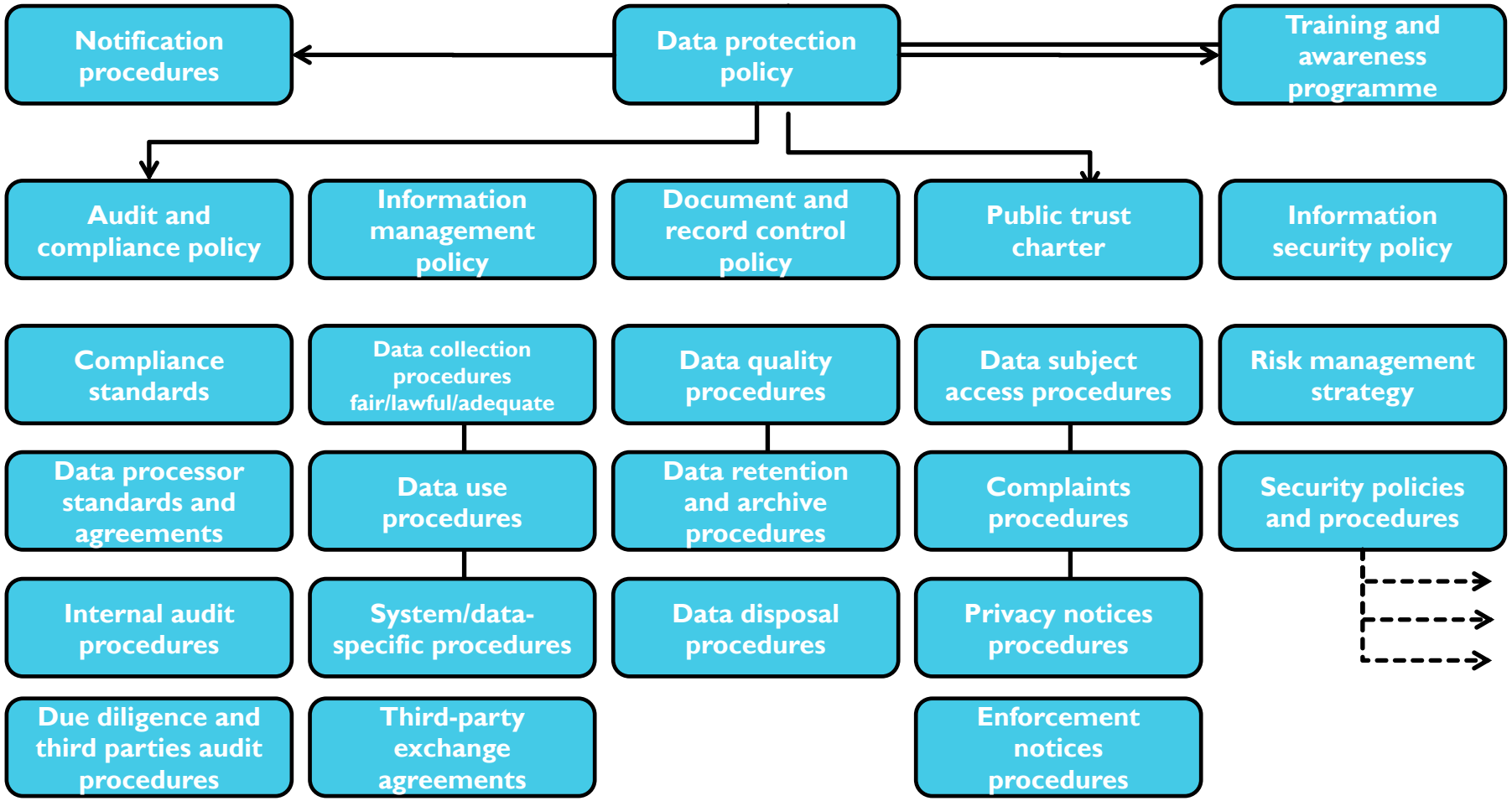
Threat scenario

- **Digital transformation** (e.g. Smart offices, National ID, Payment Platforms)
- **Power and portable computing devices** increasingly facilitating information collection, aggregation, and dissemination (e.g. Tablets, IOT)
- Increasing number of **third-party relationships** (e.g., connection and application providers)
- **Other laws and regulations**
- **Professionalisation of attackers** (e.g individuals crackers and funded teams)
- **The Cloud** (e.g., data centers, communication backbones)

Vulnerability

- More valuable data being electronically stored and processed on a massive and centralized scale (e.g., data warehouses)
- Increasing number of sources to collect data (e.g., IP cameras, biometric, GPS, RFID, etc.)
- Lack of privacy protection concerns in applications / systems development
- Information shared, combined, and linked together with greater frequency
- Use of common credentials to access multiple systems
- Increasing number of people performing activities in the cyberspace

PERSONAL INFORMATION MANAGEMENT SYSTEM (PIMS)

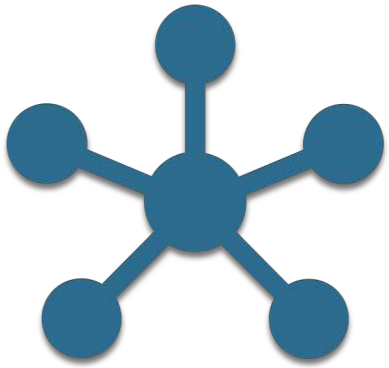


SECURITY CONTROLS

114 CONTROLS

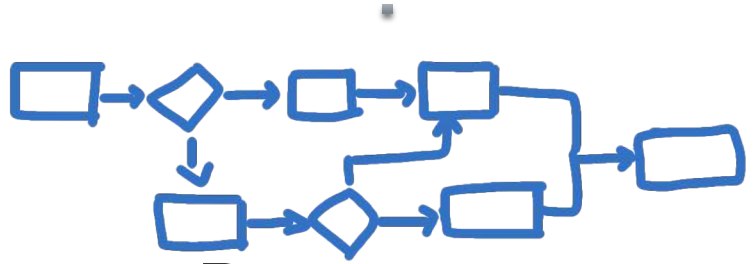
ISO 27001 Annex A:
14 Control Categories

- **5 Information security policies**
- **6 Organisation of info. security**
- **7 Human resources security**
- **8 Asset Management**
- **9 Access Control**
- 10 Cryptography
- **11 Physical & environmental sec**
- **12 Operations security**
- **13 Comms security**
- **14 System acq, dev & mnt.**
- 15 Supplier relationships
- **16 Info. security incident management**
- **17 Info. sec aspects of BC Mngt**
- **18 Compliance**



Technology

People



Processes

SCOPE OF ENFORCEMENT

PLANNING FOR PRIVACY BY DESIGN

- High level policies
  - Incorporate privacy impact assessments (PIA) throughout the systems lifecycle.
  - Managing privacy related risks to predefined levels.
  - Consider submitting PIAs to ICO for verification.
  - Publishing PIAs to promote transparency.
  - Work towards automating Subject Access Requests (SARs).

PROMOTING PRIVACY ENHANCING TECHNOLOGIES

- support existing and future PETs research into:
  - mechanisms to simplify consent, revocation and data minimisation;
  - ‘privacy-friendly’ identification and authentication systems
  - methodologies to test and prove the effectiveness of privacy controls

WHAT IS PERSONAL DATA?

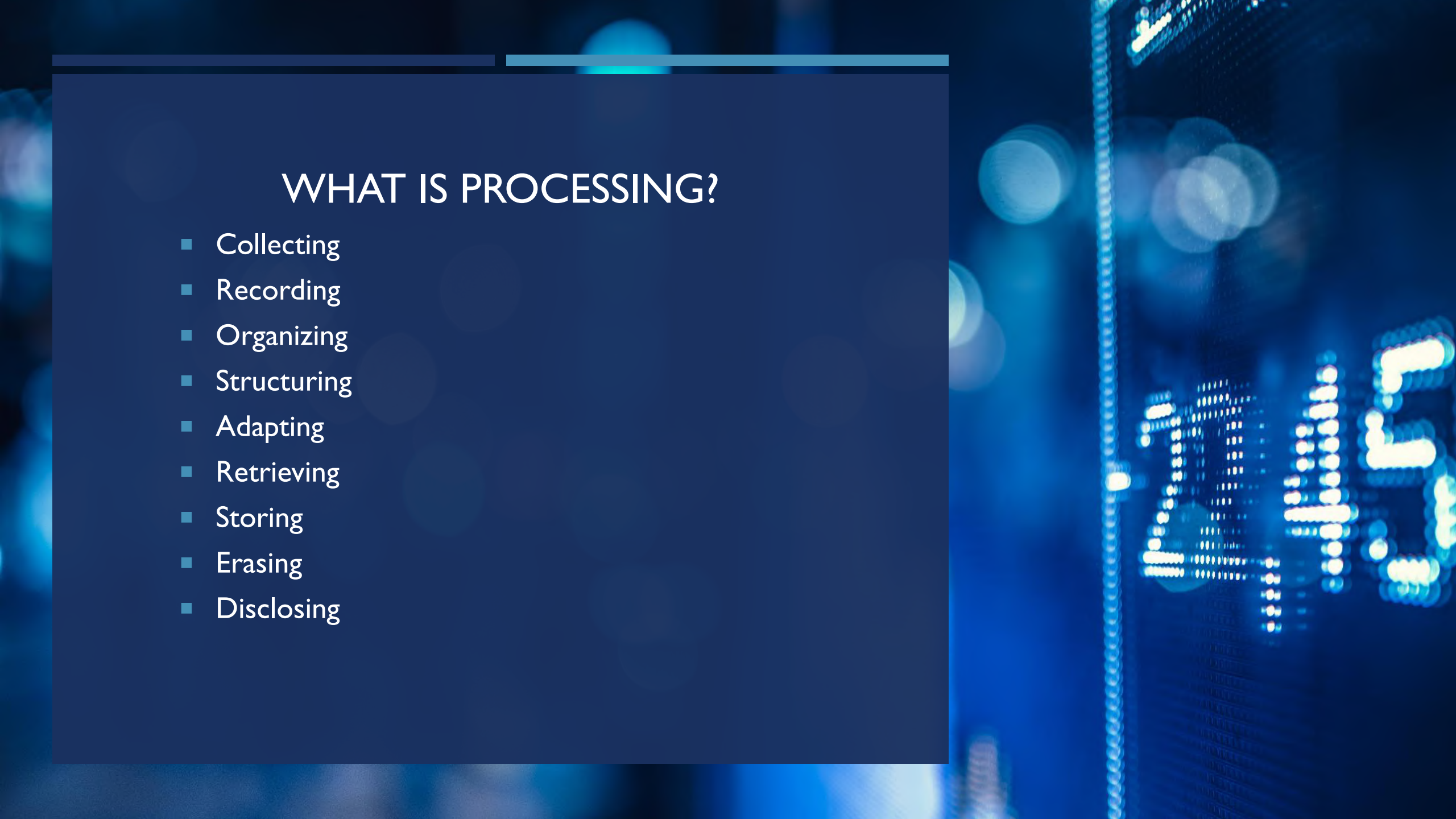
- Personal data is any information that **uniquely** identifies a **living** individual from information in the possession of, or likely to come into the possession of a Data Controller.

WHO IS A DATA CONTROLLER?

- Any person who either alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed
-

WHAT IS PROCESSING?

- Collecting
- Recording
- Organizing
- Structuring
- Adapting
- Retrieving
- Storing
- Erasing
- Disclosing



DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

- Purpose
  - Assess and identify potential DP risks and ensure they are minimised
- When to conduct PIA
  - New, change, review process , project or systems
- Format
  - List of question, screening vs full assessment
- Outputs
  - Report which highlights risks and remediation actions
  - Action Plan

THE WAY FORWARD - A CONVENTION OF EXPERTS

KEY QUESTIONS

'How do we convince African Nations to pass the DP law and establish independent authorities?'

'Considering the diverse cultures and specific challenges such as literacy levels and internet penetration levels, what best practice exist in Data Subject awareness in this region?'

KEY QUESTIONS

'how practical, realistic and applicable are the international conventions to the African Region?'

'What is the regional status, the global impact and actions required to protect individuals privacy in the cyber space?'

KEY QUESTIONS

'How do we ensure the continuous protection of personal data and privacy with the increased use of inclusive and mobile Financial Technology in the region?'

'Research, tools, frame works and other resources available'

KEY QUESTIONS

Ethical Approaches, Digital Economy and processing for the global good **– *'a focus on the African Region'***

2016 Octopus Conference
Workshop 5
Legislation on Cybercrime and Electronic Evidence in Africa

Comparative analysis: Malabo Convention of African Union and Budapest Convention on Cybercrime

THANK YOU

PATRICIA.POKU@DATAPROTECTION.ORG.GH

PATPOKU@GMAIL.COM