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
THE IDEAL STRUCTURE/MODEL

The Data Protection Commission

Data processor

Data controller (organisations)

Data subject (individuals)

Third countries

Third parties

Assessment Enforcement

Duties

Rights

Inform?

Complaints

Security?

Guarantees?

Disclosure?
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
5. Openness

Keeping Data Subjects fully informed about their personal data via multiple channels

6. Data Security Safeguards

Use of appropriate 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
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.
‘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.’
<table>
<thead>
<tr>
<th>Threat scenario</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Digital transformation</strong> (e.g. Smart offices, National ID, Payment Platforms)</td>
<td>• More valuable data being electronically stored and processed on a massive and centralized scale (e.g., data warehouses)</td>
</tr>
<tr>
<td>• <strong>Power and portable computing devices</strong></td>
<td>• Increasing number of sources to collect data (e.g., IP cameras, biometric, GPS, RFID, etc.)</td>
</tr>
<tr>
<td>increasingly facilitating information collection, aggregation, and dissemination (e.g. Tablets, IOT)</td>
<td>• Lack of privacy protection concerns in applications / systems development</td>
</tr>
<tr>
<td>• Increasing number of third-party relationships (e.g., connection and application providers)</td>
<td>• Information shared, combined, and linked together with greater frequency</td>
</tr>
<tr>
<td>• <strong>Other laws and regulations</strong></td>
<td>• Use of common credentials to access multiple systems</td>
</tr>
<tr>
<td>• <strong>Professionalisation of attackers</strong> (e.g. individuals crackers and funded teams)</td>
<td>• Increasing number of people performing activities in the cyberspace</td>
</tr>
<tr>
<td>• <strong>The Cloud</strong> (e.g., data centers, communication backbones)</td>
<td></td>
</tr>
</tbody>
</table>
PERSONAL INFORMATION MANAGEMENT SYSTEM (PIMS)

- Notification procedures
- Data protection policy
- Training and awareness programme
- Audit and compliance policy
- Information management policy
- Document and record control policy
- Public trust charter
- Information security policy
- Compliance standards
- Data collection procedures fair/lawful/adequate
- Data quality procedures
- Data subject access procedures
- Risk management strategy
- Data processor standards and agreements
- Data use procedures
- Data retention and archive procedures
- Complaints procedures
- Security policies and procedures
- Internal audit procedures
- System/data-specific procedures
- Privacy notices procedures
- Due diligence and third parties audit procedures
- Third-party exchange agreements
- Data disposal procedures
- Enforcement notices procedures
SECURITY CONTROLS

114 CONTROLS

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

ISO 27001 Annex A:
14 Control Categories
SCOPE OF ENFORCEMENT

Technology

People

Processes
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).
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