Data Protection Act

Privacy & Security in the Information Age

Presentation At the Yaoundé Conference

April 26, 2013

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Agenda

- Privacy in The Information Age
- The right to privacy
- Why We Need Legislation
- Purpose of the Act
- The Data Protection Act
  - Definitions
  - Principles
  - Rights
  - Enforcement/ Supervision
  - Exemptions / S
  - DPA Issues: The Media; The Internet

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Privacy in The Information Age

- Today, we leave "an electronic trail" from:
  - Surfing the Internet & mobile phones
  - Bank cash points & credit cards
  - Supermarket loyalty cards
- Not to mention:
  - CCTVs in city centres (with face recognition)
  - Speed cameras (number plate recognition)
  - Banks, employers, govt, and credit agencies

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

The Right to Privacy

- Do we / should we have a right to privacy?
- We all have personal details which we would **generally expect to be kept confidential –** Examples:
- Financial (bank details), professional (salary), tax status, credit status, health status, sexual preference, criminal record, political affiliation etc
- Often, employers and govt agencies need to know some of this information, BUT:
- Until recently, Ghanaians had **no legal right** to privacy

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Why we need Legislation

- Modern technology means:
  - Data can be retrieved & processed quickly
  - Data is easily copied & sent over networks
  - Errors are easily replicated but hard to fix
- The consequences of **misuse** or even simple **mistakes** can be severe:
  - You could be refused credit or employment
  - You could be misrepresented (defamation)
  - You could wrongly accused of crime/fraud, etc.

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

The Purpose of the Act

- Balances an individual's right to privacy against an organisation's need to use data relating to the individual for the purposes of their business – this includes where that purpose is research

- Defines a series of "rules" to follow when managing personal data –which include some exemptions especially for the use of data when conducting research.

- Sets out levels of "punishments" that can be handed out to organisations and individuals who fail to stay within the rules.

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

The Data Protection Act

- Definitions
- Principles
- Rights
- Enforcement
- DPA Issues: The Media; The Internet

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Definitions

- Data:
  - Information which is recorded as part of a "relevant filing system"
- Personal Data:
  - Data relating to a living, identifiable person
- Relevant Filing System:
  - Such technology that specific information on a particular individual is readily accessible

Definitions Cont.

- Data Subject:
  - Individual who is the subject of personal data
- Data Controller (individual or undertaking):
  - Determines the purposes for which and the manner in which any personal data are, or are to be, processed
- Data Processor:
  - Any person who processes the data on behalf of the data controller

Definitions Cont.

- Personal data is defined as:
- Data relating to a living individual who

  (a) can be identified from those data, or

  (b) can be identified from those data and other information held by the data controller, including any expressions of opinion about that individual

Definitions Cont.

- **Sensitive Data** is defined as data relating to:
  - Racial or ethnic origin
  - Political opinions, or religious or other similar beliefs
  - Trade union membership
  - Status of physical or mental health
  - Sexual life
  - Criminal record and court case appearances
- Processing sensitive data requires special conditions to be satisfied under the Act

Principles

The data controller has a statutory duty to ensure that personal data are:

1. Processed fairly and lawfully, plus schedules 2 & 3
2. Processed only for specified and lawful purpose(s)
3. Adequate, relevant and not excessive
4. Accurate and kept up-to-date
5. Not kept longer than necessary
6. Respectful of data subjects' rights
7. Kept secure by technical/organisational means
8. Transfers outside Ghana

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Principles I

Fair and Legal Processing

1. Obtaining Data
    - identify the Data Controller
    - state a clear purpose why it is required
    - what is involved in participation
    - data uses – primary research, storing, processing, re-use, sharing, archiving, publishing,
    - strategies to ensure confidentiality of data where this is relevant –anonymisation etc
2. Legitimate Processing
    - **data Subject must give consent**
    - processing is in legitimate interests of Data Controller
3. Processing of Sensitive Data – **Informed Consent**

Principles 2

Processed only for specified and lawful purpose(s)

- *Personal data shall be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes*

  However, researchers may be provided with an exemption.

  They may not need to further consent from the individual if:

  - it was not initially anticipated that the data would be used for research purposes, **and**
  - it is deemed as not practical to retrospectively inform the individuals, **and**

  From a Other perspective

  - that he use of the data has been approved by the ethics committee

Principles 3

Adequate, relevant and not excessive

- *Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed*
  - this means that researchers are only allowed to obtain the information required to complete the task at hand.
  - there should be no "stock piling" of information you think might be useful "later on" – this is different to finding a new use for information already held
  - if there is a valid reason for asking someone their ethnicity it is permitted, if it does not contribute to the research - **it should not be asked**.
  - If the information is collected for research it should not be used for any other purpose

Principles 4

Accurate and kept up-to-date

- *Personal data shall be accurate, and where necessary, kept up to date*

  - researchers have a duty to ensure that the information they collect is accurate
  - they are not required to keep the information up to date unless it is absolutely necessary for ongoing research
    - For example, where you will go back to the subjects again
  - where the research is based around a “snap shot” in time, there is no need to go back and update it

Principles 5

Retention and Disposal /Not kept longer than necessary

- *Personal data shall not be kept for longer than is necessary, for the purposes for which it is being processed*
  - Records should be retained as evidence of the project
    - How it was managed - controlled
    - The procedures followed
    - The data collected
  - Standard University Retention periods are available
  - External funded research may be subject to their own retention periods – check them
  - Make sure you specify the correct retention period when you seek consent- holding it for longer than permitted would be a breach!

Principles 6

Respectful of data subjects' rights

- *Personal data shall be processed in accordance with the rights of data subjects under this Act*

  - This means that you cannot do things that violate the rights given to data subjects, especially denying access
  - They have the right to object to processing which may cause unwarranted damage or distress
  - They have the right to withdraw consent
  - Right to ask the Information Commissioner to assess an organisation's processing for compliance – **Possible Compensation or fines**

Principles 7

Kept secure by technical/organisational means

- *Appropriate security measures shall be taken against the unauthorised or unlawful processing, accidental loss , destruction , or damage of personal data*
  - Store personal data on a secure server – not hard drives
  - Make use of central filing
  - Avoid duplication as much as possible
  - Restrict access on the basis of authority levels
  - Use strong password protected documents and screensavers
  - Change passwords at regular intervals
  - Do not use global passwords
  - Keep paper records under lock and key

Security

- Determine what is appropriate having regard to -
  - the nature of the personal data to be protected
  - the resulting harm which might arise from a breach
  - state of the art & implementation cost
  - the effectiveness of existing measures
  - reliability of staff (e.g. appropriate training for *all* staff)

Risk

- Is there proof that all reasonable steps have been taken to comply with DPA's security duties?
- Are security standards for industry or sector being met?
- Is there a security policy?
- Is there a business continuity plan to cover inability to process data in an emergency?
- Does management take security seriously?
- Are the service provider's staff adequately trained in respect of data protection requirements? Have they been security vetted?

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Risk

- What contractual security obligations have you imposed upon the service provider?
- Is there a duty upon the service provider to report data security breaches?
- What powers do you have to audit the service provider to ensure that they are complying with their data protection obligations?
- What are the known risks for the kind of processing undertaken?
- Are data transferred securely?
- Is encryption used when data are processed on mobile devices?

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Principles 8

Data transfers outside of Ghana

"Personal data shall not be transferred to a country or territory outside Ghana unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data"

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

Rights

- Individuals have the following rights under the DPA:
  1. Subject access
  2. Object to processing in certain circumstances
  3. Object to direct marketing (promotion of aims & ideals is marketing)
  4. Automated decisions
  5. Ask court to order compensation for damage caused by controller's breach of principles
  6. Ask court to order correction of inaccurate data

- Controller liable under 6th Principle for 1-4 above

Enforcement

- If the Information Commissioner finds that the DPA has been breached by a DC, he/she serves an **enforcement notice** on the DC
- The notice identifies the breach or omission, and specifies how to correct it
  - Failure to comply is **an offence**
  - However, a DC may appeal to the **DP tribunal**
  - With the approval of the **Director of Public Prosecutions**, legal proceedings may follow, which could **result in a fine**

Exemptions

- Certain agencies or types of data are exempt from the DPA
  - National Security
  - Tax/revenue gathering agencies
  - Judicial appointments & honours
  - Corporate finance / negotiations
  - Legal/professional privilege (doctor/patient)
  - Human embryos/ IVF/adoption

Supervision

- Data Controllers must apply for registration on the **Data Protection Register**
- DPR is overseen by the **Information Commissioner**
- On registration (notification), DCs must provide details of the data to be stored and its use, and the measures to be taken to comply with the Act (including data security and data transfer)
- Note: "notification" does not mean "licensing"
- DCs do not need to wait for approval from DPR
- Establishment of Data Protection Commission

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

DPA Issues: The Media

- The DPA has special provisions for journalism, and artistic or literary purposes
  - Basically, journalists/authors may hold/use personal data for journalistic/artistic/literary purposes only if the data are necessary to reconcile the rights to privacy with the rules governing freedom of expression
- So, investigative journalists & political strategists or commentators are not treated as Data Controllers!!

Patricia Dovi Sampson, Director Research, Statistics & Information Management
Ministry of Communications, Ghana

The End

Thank You!

CONTACT

Email: Patricia.dovi-sampson@moc.gov.gh

: sampsonpatricia@hotmail.com

Patricia Dovi Sampson, Director Research, Statistics & Information Management

Ministry of Communications (MoC), Ghana