

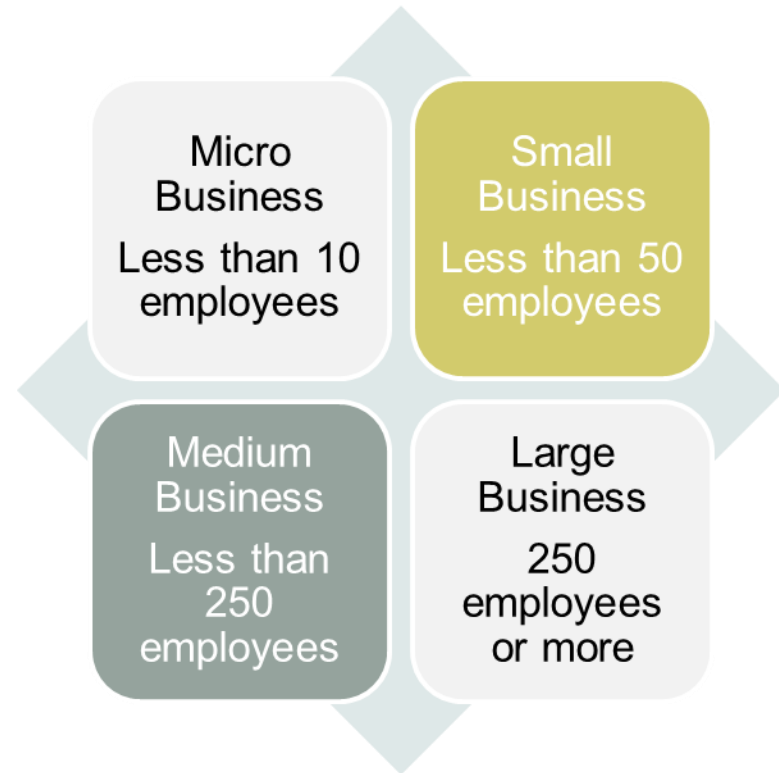
DATA PROTECTION CONFERENCE 2016
ACCRA, GHANA
28 – 29 JANUARY 2016

Breakaway Session 2:
Data Protection and The Role of the Data
Protection Supervisor

Michael Mingle
Director, NTSS Solutions (UK)

The SME sector

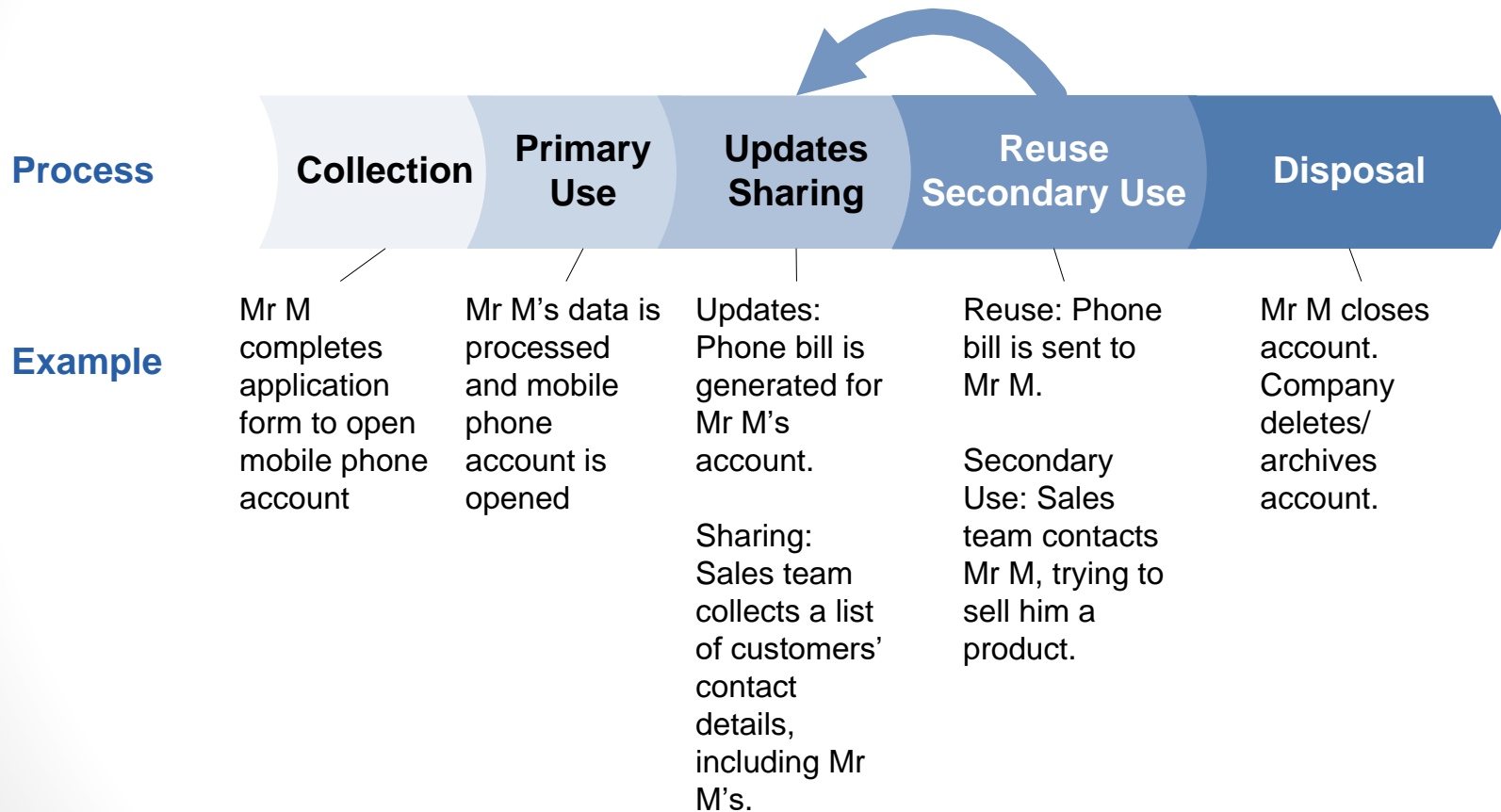
- Owner-Managed businesses (SME)
- None has a dedicated Data Protection Officer



Insider threat

- Many data breaches occur due to employee error
- A disgruntled employee with a USB stick or camera smartphone can cause a lot of damage
- Data Protection Supervisor – vital tool in minimising the risk of data breaches by
 - raising awareness of privacy and data protection
 - ensuring technical and organisational controls in place

Lifecycle of data



What is data protection?



- The means of protecting personal data, and the systems that hold that data, from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
- To protect the privacy of individuals
- In order not to put them at risk of harm

Risk of Harm to Individual

When personal data is

- inadequate, insufficient or out of date
- excessive or irrelevant
- kept for too long
- improperly disclosed to others
- used in ways that are unacceptable or unexpected by the person it is about
- used or misused
- not kept securely



Individual at risk of

- physical harm
- threat to emotional wellbeing
- financial loss
- fear of identity theft
- damage to personal relationships
- humiliation/ embarrassment
- harassment
- annoyance

Risk of Organisational Harm

- Operational disruption - Diverted time and resources
- Loss of consumer confidence
- Legal/regulatory sanctions, liability and financial penalties
- Reputational damage
- Financial loss

Data Protection Act

- To protect the privacy of individuals by regulating how organisations process personal data.
- Gives meaning to:
 - Article 8 (1) of the Human Rights Act 1998 (UK), *“Everyone has the right to respect for his private and family life, his home and his correspondence*
 - Article 18 (2) of the Constitution of the Republic of Ghana 1992, *“No person shall be subjected to interference with the privacy of his home, property, correspondence or communication...”*

Principles of the UK Data Protection Act

- Principle 1 – fair and lawful
- Principle 2 – purposes
- Principle 3 – adequacy
- Principle 4 – accuracy
- Principle 5 – retention
- Principle 6 – rights
- Principle 7 – security
- Principle 8 – international

Key Terminology

- Personal data: information that can be used on its own or with other information to identify and individual
- Processing: collection, use, disclosure, retention or disposal of personal data
- Sensitive personal data: personal data that may put an individual at substantial risk of harm should their privacy not be respected
- Privacy: Informational privacy. Right of individual to decide how, when and to what extent their personal data is processed

The Role of the Data Protection Supervisor (DPS)

To promote awareness and maintain high standards of practice in data protection and privacy by undertaking the following duties across the business:

- Manage Data Protection and Privacy Compliance
- Facilitate training
- Develop, implement and enforce a Data Protection Policy
- Provide advice and guidance to managers and staff
- Produce best practice guides
- Process, co-ordinate and respond to Subject Access Requests and any Complaints under the Act
- ...and any other duties related to the Data Protection Act

Managing Data Protection Compliance

- Ensure compliance with the Principles of the Data Protection Act.
- Ensure your data controller registration is valid and details are up to date
- Ensure data processor compliance
- Personal data breaches – reporting to the data protection regulator is mandatory for some business sectors

Develop, Implement and enforce Data Protection policy

- Should be suitable and relevant to your business
- Review annually
- Policy should set out clear commitment

Data Protection Policy

Our data protection policy below sets out our clear commitment to protecting personal data and shows how we have carried out that commitment. We are committed to ensuring that we comply with the 8 data protection principles, as listed below:

[List principles here]

We have demonstrated that commitment by:

- Putting adequate security measures in place to protect personal data
- Putting measures in place to ensure that the personal data we process is accurate and up to date
- Establishing a retention period of ... so that personal data that is out of date is safely archived/deleted.....

Subject Access Requests & Complaints

The individual has the right to determine how, when and to what extent their personal data is processed. The data subject is the individual that the personal data is about.

