Project Management Institute. Ghana

PROJECT STAKEHOLDER DATA MANAGEMENT ACCORDING TO ACT 843

the role of the Project Manager

Emmanuel K. Gadasu | CEH, CDPS, CIPM, MSc IT and Law*

09 04 2023

Data Protection Laws

Data Protection is a **legal requirement** in many countries, including Ghana where the **Data Protection Act 843** (Data Protection Act 2012) sets strict rules on how personal data should be collected, processed, and stored.

Failure to comply with data protection laws can result in significant fines and reputational damage to organizations

Importance of Data Protection

Organizations that take data protection seriously can reap these benefits and mitigate the risks associated with mishandling personal data:

- Protecting Individual Privacy
- Builds Trust
- Regulatory Compliance
- Prevents Data Breaches
- Improves Data Quality
- Supports Innovation

Key Definitions

Personal Data

is any data that can be used to identify an individual, such as a name, home address or credit card number.

Data Subject

The term 'data subject' refers to any living individual whose personal data is collected, held or processed by an organisation.

Data Controller

The data controller determines the purposes for which and the means by which personal data is processed. So, if your company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller

Data Processor

A data processor is a person, company, or other body which processes personal data on the data controller's behalf.

Processing

It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data

Consent

of the data subject means 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

Act 843 - Principles

- Accountability – Section 18
  - requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested
- Lawfulness of Processing – Section 19, 20, 21, 24, 29
  - Consent, Contract, Legal obligation, Vital interests, Public task, Legitimate interests
- Specification of Purpose – Section 22 & 23
  - purpose limitation is a requirement that personal data be collected for specified, explicit, and legitimate purposes, and not be processed further in a manner incompatible with those purposes
- Compatibility of Further Processing – Section 25
  - The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected

DPC

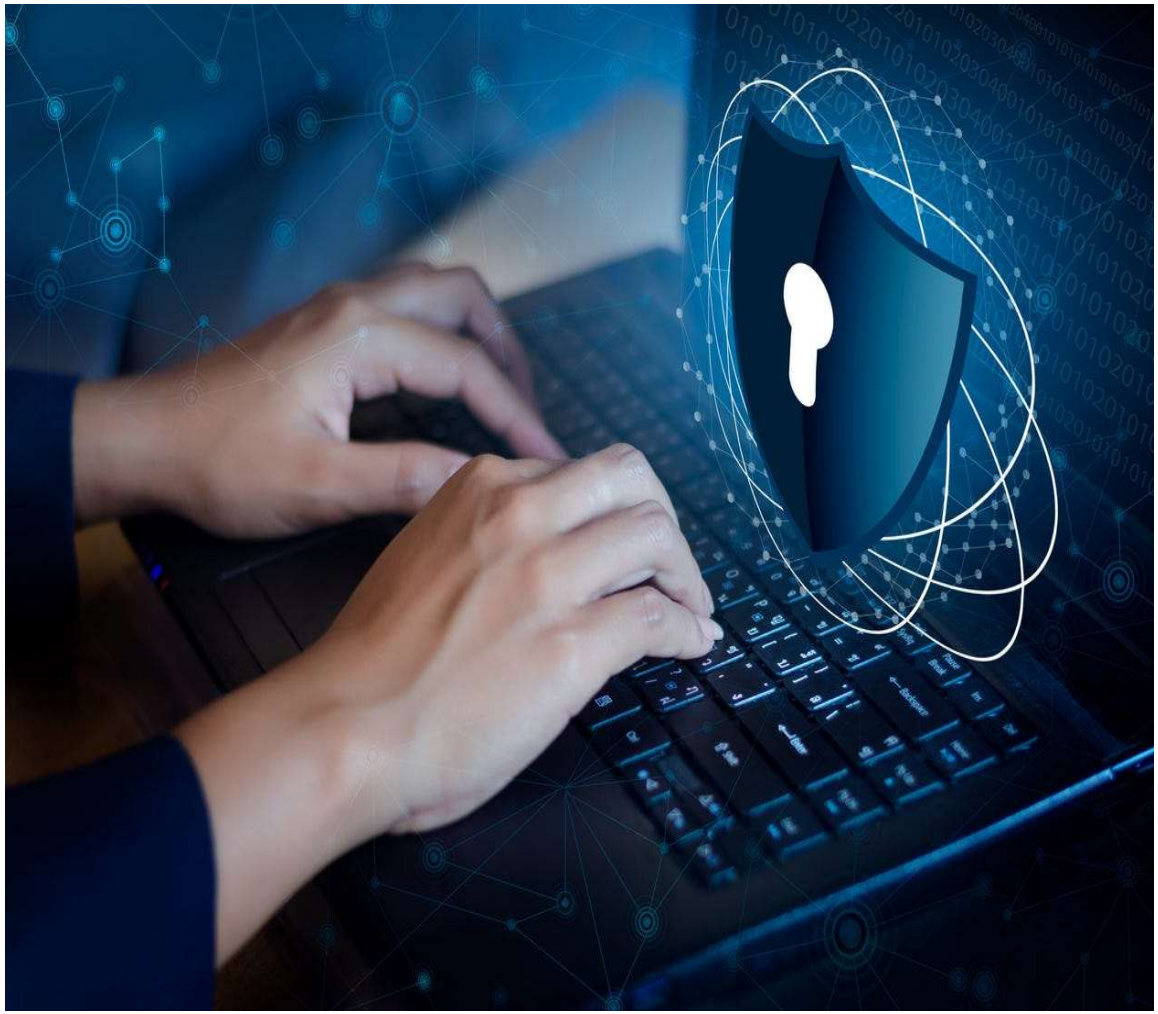
DATA PROTECTION COMMISSION

Act 843 - Principles

- Quality of Information – Section 26
  - The data quality principle comprises that data has to be of good quality, i.e. the data has to be complete, accurate and up-to-date. This implies that if you discover that personal data is inaccurate or not up-to-date, you have to take steps towards rectification or deletion of these data
- Openness/Transparency – Section 17&27
  - The principle of transparency requires that any information or communication relating to the processing of personal data is easily accessible and easy to understand, and that clear and plain language be used
- Data Security Safeguards – Section 28
  - You must ensure that you have appropriate security measures in place to protect the personal data you hold. Ensure the CIA of the data you process
- Data Subject Participation – Section 32
  - Data Subjects should have access to their personal data when they request for it

DPC

DATA PROTECTION COMMISSION



Organizational Measures

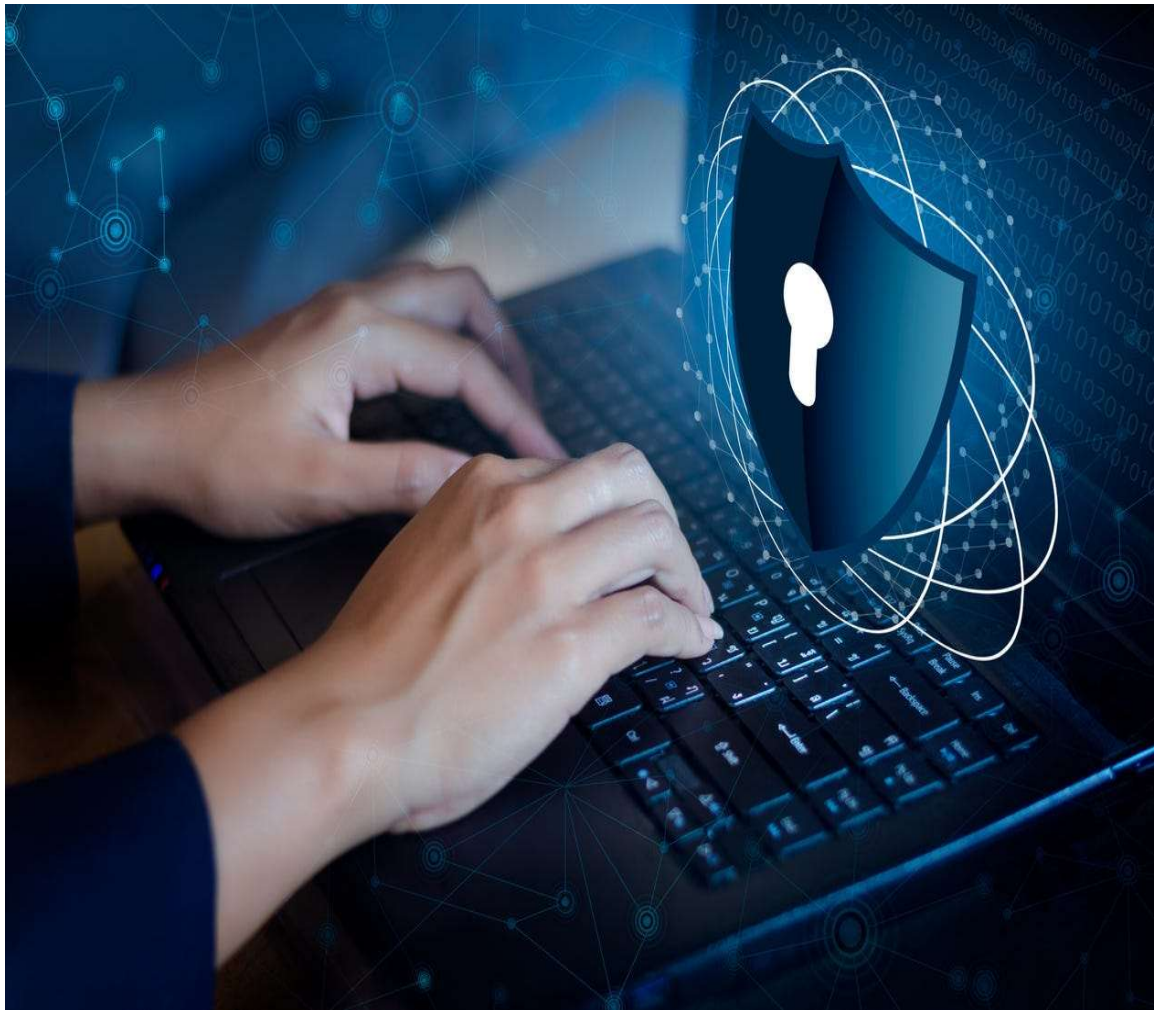
Organisational measures may consist of internal policies, organisational methods or standards, and controls and audits, that controllers and processors can apply to ensure the security of personal data.

- Information security policies
- Business continuity plan
- Other policies and procedures
- Awareness & training
- Reviews & audits
- Due diligence

Technical Measures

Technical measures can be defined as the measures and controls afforded to systems and any technological aspect of an organisation, such as devices, networks and hardware.

- Cybersecurity
- Encryption and Pseudonymisation
- Physical Security
- Appropriate Disposal
- Passwords/Authentication
- Access Management



OFFENCES AND PENALTIES

- False registration information - **Section 47(2)**
- Failure to register as a data controller but processes personal data - **Section 56**
- Failure to comply with notice – **Section 80(1)**
- Materially reckless and false statement to compliance notice - **Section 80 2(a)(b)**
- Conditional request for goods and services – **Section 82**
- Knowingly obtain, purchase or disclose personal data - **Section 88**
- Sale of personal data – **Section 89**

OFFENCE: Unspecified offence penalty

PENALTY: Where a person commits an offence under this Act in respect of which a penalty is not specified, the person is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

What Must Organizations Must Have

For a successful data protection compliance, organizations must have:

- Data Protection Privacy Policy or Notice/Statement
- ROPA/Data Maps
- Data Protection Impact Assessment (DPIA) Process
- Privacy Risk Register
- Data Subject Access Request (DSAR) Process
- Functional Information Security Systems
- Data Protection Professionals and Champions

How to Implement DP in Project

The PM is a great stakeholder in ensuring that products or services delivered by the organization is safe and ensures the privacy of the users

- Conduct a DPIA
- Identify and map personal data
- Define roles and responsibilities
- Ensure Privacy By Design and By Default
- Ensure Legal Basis of Processing Data Is Appropriate
- Train Employees
- Regular Review and Updates

What PMs Must Look For

The PM is a great stakeholder in ensuring that products or services delivered by the organization is safe and ensures the privacy of the users

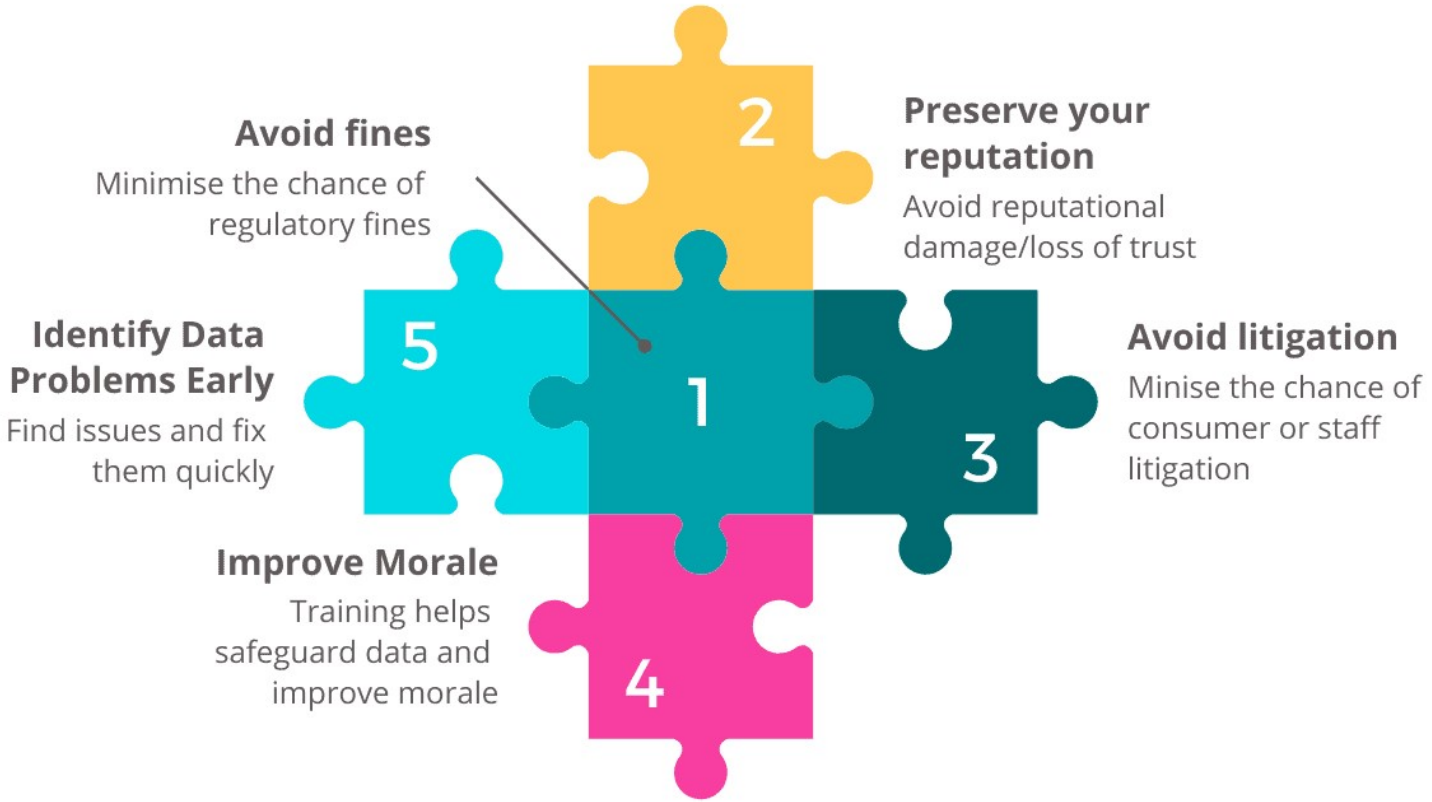
- Does the organization have relevant data protection policies in place?
- Does the organization have an appointed DPO or subscribed to DPaaS?
- Did the organization carry out a Data Protection Impact Assessment (DPIA)?
- What are the privacy risk mitigating measures?
- Are there provisions for data subjects to exercise their rights?
- Do the project stakeholders have the relevant data protection knowledge?

Before You Start A New Project

1. Do we have a Data Protection Officer?
2. Have we conducted Data Privacy Impact Assessment?
3. Will there be transfer of personal data?
4. What Does The Privacy Notice Say?
5. What is The Retention Policy for Data?
6. What Impact Does Right to Portability Have?
7. Does Your Project Rely on Profiling?
8. Are You Using Opt In Forms? What is the legal basis?
9. Can You Find Data in Your New Software?
10. What's the Data Protection Risk?

You are good to go if you can answer these questions

How Data Protection Can Reduce Project Cost



Project Management Institute Ghana

THANK YOU

EMMANUEL K. GADASU
DATA PROTECTION AND CYBERSECURITY EXPERT
ekgadasu@gmail.com +233 24391 3077