
DATA PROTECTION COMMISSION
Building Integrity and Trust
MINISTRY OF COMMUNICATIONS
2017
DATA PROTECTION
CONFERENCE

BREAKOUT SESSION 2

Contracting a Data Processor

AGENDA

- The 7th Principle: Data Security Safeguards, Data Processor Registration
- The 2nd Principle (Section 29): Confidentiality Measures
- Security Measures: Risk Assessment & Review of Safeguards
- Monitoring

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

The 7th Principle

defines the processing of personal data

by a Data Processor for a Data Controller

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

The 7th Principle: Data Security Safeguards

- This relationship is governed by a **written contract** which instructs the Data Processor to establish and maintain **confidentiality** & **security** measures requisite to ensure **integrity** of personal data.

- The Data Processor is under obligation to comply with the relevant data protection requirements of Ghana, if they are not based in here.

The 7th Principle: Data Processor Registration

- The Data Controller has the responsibility to ensure that the Data Processor is dully registered.

- The registration of the Data Processor loses validity…
  - if the Data Processor knowingly provides false information
  - when it is cancelled by the DPC
  - on expiration

The 2nd Principle: Confidentiality Measures

The 2nd Principle (Section 29), requires the Data Processor

- to process personal data only as instructed by the Data Controller
- to treat personal data as confidential. Special Personal Data, for example health or financial information, requires even higher level of security.
- not to disclose personal data to any 3rd parties unless required by law

These should be integrated into the contractual agreement between the 2 parties.

Security Measures

Adequate measures should be in place *before* personal data is entrusted to the Data Processor for processing. In addition, the Data Controller may consider a compliance assessment audit of the Data Processor before any contractual agreements are signed.

Security Measures – The Requirements

Data Processor

- Should have security measures in place prior to the contract
- The measures should adequately cover the needs of the Data Controller
- Can only process data on behalf of the Data Controller

Data Controller

- Should carefully review the documentation of the Data Processor, including provisions for personal data processing
- Is required to have compliance & security measures in place

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Security Measures – Further Requirements

The 7th Principle (Sec.28) - The Data Controller is required to

- identify internal and external risks to personal data
- establish appropriate safeguards against the identified risks
- regularly verify that the safeguards are effectively implemented and
- are continually updated in response to new risks or deficiencies
- Data Processors are required to undertake risk assessment – this should be integrated into the contract

Security Measures: Risk Assessment

- Rationale: to identify potential risks to personal data and eliminate or mitigate those risks

- Failure to manage risks may cause
  - Individual risk of harm
  - Organisational risk of harm

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Security Measures: Review of Safeguards

- If the Data Processor does not have any existing review documents, the Data Controller should instruct the Data Processor:
  - to monitor safeguards
  - undertake initial review within an agreed timescale
  - perform subsequent reviews also within agreed periods
  - review safeguards in response to new risks

- In this regard, the Data Controller should always ensure that they review and approve all data processing review documentations.

Monitoring

Data Controllers are responsible for monitoring the security and confidentiality measures. They are required to…

- Keep documented copies of confidentiality and security measures e.g. compliance assessment, risk assessment, reviews, policies et-c.
- Review documents, keep issue log and follow-up actions. An audit should be requested if there is any cause for concern.
- Keep copies of all documents well organised and safe as proof of personal data protection.

Thank you

NTSS Solutions

2017 DATA PROTECTION CONFERENCE