GUIDELINES TO DEMONSTRATE DATA PROTECTION COMPLIANCE

INTRODUCTION

The office of the Data Protection Commission (herein referred to as 'the office 'or 'DPC') is a state office or Public Corporation in accordance with Article 190 of the Constitution of Ghana[1]. The Data Protection Act, 2012 (Act 843) was introduced to give effect to Article 18(2) of the Constitution of the Republic of Ghana, 1992.[2]

MANDATE OF THE DATA PROTECTION COMMISSION

"The mandate of the Data Protection Commission is to"[3]:

a) Implement and monitor compliance with the provisions of the Act.
b) Make the administrative arrangements it considers appropriate for the discharge of its duties
c) Investigate any compliant under the Data Protection Act, 2012 and determine it in the manner the Commission considers fair; and
d) Keep and maintain the Data Protection Register

OUR VISION

To protect the Privacy of the individual and Personal Data by regulating the people, processes and the technology

OUR MISSION

To ensure the responsible and accountable processing of personal data of all living individuals, in compliance with statutory requirements; efficiently and effectively; as a regular in Ghana and beyond.

OUR GOALS

[1] Constitution of the Republic of Ghana 1992, art 190
[2] Ibid, art 18(2)
[3] Data Protection Act 2012 (Act 843), s 3

1. Independence: establish an independent, operational and sustainable Data Protection Commission
2. Growth: increase the number of data protection responsive organisations who collect and use personal data
3. Awareness: increase individuals' awareness of data protection rights and empower them to assert their data protection right
4. Pace Setter: to make Ghana the leading example of Data Protection in Africa.

GUIDELINES TO PROMOTE THE OBSERVANCE OF GOOD PRACTICES FOR ENSURING COMPLIANCE WITH THE DATA PROTECTION ACT, 2012 (ACT 843)

The aim of these guidelines is to help Data Controllers and Processors demonstrate compliance with the Data Protection Act, 2012, by meeting the requirements outlined below in accordance with the provisions of the law:

1. REGISTRATION WITH THE DATA PROTECTION COMMISSION PROCEDURE

The section 27 of the data protection act mandate that a data controller (organisations) who intends to process personal data shall register with the Commission.[4]

a) The following details are required by the organisation to satisfy the registration requirements:

1. Business certificate of Incorporation/Registration

2. Entity Category e.g. Limited Liability Company

3. Address

4. Sector

5. Description of services provided

6. What is your annual turnover in Ghana Cedis

[4] Data Protection Act 2012 (Act 843), s 27

7. Average number of data subjects whose personal data you process

8. Average annual number of records of personal data that you process

9. Is this part of a group of companies with at least one entity as a large Data Controller or Data Processor.

10. Reason for processing data

11. Which countries outside of Ghana do you process data in.

b) The Commission shall register an applicant if it is satisfied that the applicant has met the conditions required for registration. Upon registration, the applicant shall pay the prescribed fee.[5]

c) The Commission shall issue a certificate of registration to the applicant upon approval of the application.[6]

2. RENEWAL OF REGISTRATION WITH THE DATA PROTECTION COMMISSION PROCEDURES

The section 50 of the Data Protection Act Mandate that a registration shall be renewed every two years.[7] A Data Controller is advised to implement the following measures upon the grant of registration and before the due date for renewal:

a) Appoint and train a Data Protection Supervisor.[8] The DPC's administrative arrangements exempt small Data Controllers from appointing a Data Protection Supervisor. However, it is recommended that they seek support from a Certified Supervisor to demonstrate compliance. Medium and large Data Controllers are required to appoint a designated Supervisor, as determined by the DPC under section 3(b) of the Data Protection Act, 2012, in the discharge of its duties[9].

[5] Data Protection Act 2012 (Act 843), s 27
[6] Ibid, s 49
[7] Ibid, s 50
[8] Ibid, s 58
[9] Ibid, s 3(b)

b) The DPC reserves the right to determine which Data Controllers are required to appoint a Data Protection Supervisor, based on the size of the organisation and the volume of records processed
c) The Certified Data Protection Supervisor must initiate the process of monitoring compliance by conducting a Data Protection Compliance Assessment to identify potential areas of noncompliance.
d) Data Controllers and Data Protection Supervisors are advised to seek assistance deemed necessary from institutions accredited by the DPC, including certified Data Protection Experts.
e) Data Controllers and Data Protection Supervisors are advised to seek assistance from only institutions or experts accredited by the DPC to provide support to the organisation.
f) Develop strategies to address areas of non-compliance.
g) The Data Controller/Processor must take necessary steps to document and implement technical and organizational measures to demonstrate data protection accountability[10]
h) Establish an organisational data protection programme, such as Data Protection Awareness Training for management and staff.
i) Be prepared for renewal

3. GUIDANCE ON PERFORMING GAP ANLYSIS/COMPLIANCE ASSESSMENT

Data Controller/Processor (Businesses) must understand whether they act as Data Controllers or Processors, as both have legal responsibilities under the Data Protection Act, 2012 (Act 843) and may face penalties for non-compliance. These guidelines, issued under Section 86, help promote good data protection practices. Completing a Compliance Assessment enables organisations to evaluate their level of compliance and identify gaps

Step-by-Step Process to Assess Non-Compliance:

1. Review Legal Requirements

Study the key obligations under Act 843, including:

a) Registration (s 27,45,46(b),47(3),50,90,91)

[10] Ibid, s 28

b) Appointment of a Data Protection Supervisor (s 58)
c) Lawful processing (s 18–23)
d) Privacy principles (s 17)
e) Further processing to be compatible with purpose of collection(25)
f) Data subject rights (s 32–35, s 39– 44)
g) Security measures/safeguards (s 28)
h) Retention of records (s 24)
i) Data processor to comply with the Data Protection Act,2012(s 29 - 30)
j) Conditional Request for Personal Data Prohibited (82)
k) Prohibition to purchase, obtain or disclose personal data (88)
l) Prohibition of sale of personal data (89)
m) Demand for health records (s 83)
n) Cross border transfer (s 28(3b))
o) Duty to Notify Changes (s 55)
p) Notification of security compromises (31)
q) Quality of information (s 27)

2. Conduct a Compliance Self-Assessment

Use a checklist or toolkit that covers:

a) Accountability and Governance
b) Policies and procedures in place
c) Data Protection Supervisor
d) Roles and Responsibilities
e) Lawful basis for processing (Record of Processing Activities (ROPA))
f) Staff training and awareness
g) Data Subject Participation – (Respecting Individuals' rights)
h) Contracts with processors or third parties
i) Risk assessments and Data Protection Impact Assessment
j) Data Protection by design and by default
k) Handling of subject access requests

Guidelines provide advice on how to comply with regulatory requirements, policies, procedures and controls (section 86)

l) Incident/breach response mechanisms

3. Identify Gaps

Mark areas where:

a) Required controls are missing
b) Documentation is incomplete
c) Staff are unaware of obligations
d) Legal bases are unclear or unjustified
e) Security or data retention measures are weak

4. Score the Risk Level

Assign a risk rating (e.g. low, medium, and high) to each area of non-compliance based on:

a) Likelihood of a breach
b) Sensitivity of the data
c) Impact on data subjects
d) Legal/regulatory consequences

5. Document Your Findings

Summarise:

a) Areas of non-compliance
b) Evidence or indicators
c) Severity and urgency
d) Actions needed and responsible persons

6. Develop an Action Plan

a) Prioritise high-risk areas
b) Assign timelines and responsibilities
c) Monitor progress

4. SUBMISSION OF COMPLIANCE ASSESSMENT REPORT AND READINESS FOR AUDIT OR INSPECTION

Data Controllers and Processors are required to submit a completed Gap Analysis/Compliance Assessment Report for review and approval by the Commission. This process demonstrates organisational readiness and accountability, and serves as the basis for potential compliance audits or inspections in fulfilment of the Commission's mandate to monitor compliance with the provisions of the Data Protection Act, 2012.

5. REVIEW AND UPDATES OF THE GUIDELINES

These guidelines are subject to periodic review and may be updated by the Data Protection Commission to reflect changes in law, regulatory practice, or emerging data protection risks. Data Controllers and Processors are encouraged to consult the most recent version published by the Commission.

6. NEED HELP?

For more information on how the Compliance Team can provide guidance to your organisation, please contact us on

- Phone Number: 0256302031
- Email : compliance@dataprotection.org.gh
- Website: www.dataprotection.org.gh