THE DATA PROTECTION ACT, 2019.

THE DATA PROTECTION (CONDUCT OF COMPLIANCE AUDIT) REGULATIONS, 2024.

ARRANGEMENT OF REGULATIONS

PART IV – CONDUCT OF DATA PROTECTION COMPLIANCE AUDIT

PART 1 – PRELIMINARIES

Citation.

1. These Regulations may be cited as the Data Protection (Conduct of Compliance Audit) Regulations, 2024.

Interpretation

2. In these Regulations, unless the context otherwise requires—

"Act" means the Data Protection Act, 2019;

"auditor" means a person accredited in accordance with regulation 12 to conduct data protection compliance audit;

"Data Controller" has the meaning assigned to it under the Act;

"Data Processor" has the meaning assigned to it under the Act; and

"Data Protection Audit" means the systematic and independent examination of data protection practices, policies, and procedures of a data processor or data controller to assess compliance with data protection laws; and

"Office" means the Office of the Data Protection Commissioner.

Objects of the Regulations.

3. The objects of these Regulations are to—

(a) provide a framework for the conduct of data protection audits;

(b) promote the quality and consistency of data protection audits;

(c) establish a framework for the accreditation of data protection auditors by the Office; and

(d) provide guidance to the Office in its role of overseeing and monitoring data protection audit activities conducted by accredited firms.

Application.

4. These Regulations shall apply to the manner of conducting data protection compliance audits.

PART II—ADMINISTRATION OF DATA PROTECTION AUDITS

Conduct of Audits by the Office.

5. (1) In accordance with Section 23 of the Act, the Office may conduct a data protection audit on a data controller as maybe necessary to ensure compliance with the Act and the Regulations.

(2) A data protection audit may be a periodic audit or a special audit.

(3) The Office may—

(a) conduct a data protection audit on its own;

(b) outsource the conduct of the audit; or

(c) affirm a data protection audit report submitted to the Office by an accredited auditor.

Engaging external data protection auditors

6. (1) The Office may engage an external data protection auditor to conduct a data protection audit when necessary.

(2) In determining whether to engage an external data protection auditor, the Data Commissioner may be guided by the following criteria—

(a) complex or specialized nature of the audit requiring specific expertise;

(b) internal resources available within the Office;

(c) situations where outsourcing is more cost-effective than internal audit execution.

Recognition of Privately Initiated Audits.

7. (1) The Office may recognize an audit that has been privately initiated and conducted by an accredited auditor, subject to the conditions and criteria set out in these Regulations.

(2) For a privately conducted audit to be recognized under this provision, it shall—

(a) be conducted by an auditor who is duly accredited under these Regulations;

(b) comply with all relevant standards, procedures, and methodologies as required for data protection audits;

(c) be comprehensive in its scope, adequately addressing the compliance requirements as stipulated in the Act and the Regulations;

(d) be accompanied by a detailed report, documenting the audit process, findings, and recommendations; and

(e) submitted to the Office for review and recognition in accordance with Regulation 8.

Procedure for Seeking Recognition

8. (1) An accredited auditor seeking recognition for a privately initiated audit shall submit a request to the Office along with the audit report and any supporting documentation within 30 days upon completion of the audit.

(2) The request for recognition shall be made in writing to the Office.

(3) Upon receipt of a request for recognition, the Office shall review the submitted audit report and supporting documentation to ascertain its compliance with the stipulated standards and requirements.

(4) The Office may recognize the audit report if it meets the required standards.

(5)Where the report fails to meet the required standards, the Office shall decline the recognition audit report and communicate with reasons to the auditor.

Effect of Recognition.

9. (1) A recognition of a privately initiated audit by the Office shall affirm that the audit has met the standards and requirements equivalent to those of an audit directly overseen by the Office.

(2) The recognition shall serve to fulfil certain regulatory or compliance obligations of the audited entity under the Data Protection Act, 2019.

PART III—ACCREDATATION OF DATA PROTECTION AUDITORS

Power to Grant Accreditation.

10. The Data Commissioner may, upon application and subject to this Part, grant accreditation to a qualified person to conduct data protection compliance audits in place of the Officer as required under Section 23 of the Act.

Application for accreditation.

11. (1) A person desiring to be accredited as a data protection auditor may apply to the Office.

(2) An application for accreditation shall be made to the Office and shall—

(a) be in a Form DP1 set out in the first schedule; and

(b) be accompanied by an application fee of Kshs. 5,000

(3) An application for accreditation shall include the following documents or information—

(a) a copy of establishment documents;

(b) a demonstration of the applicant's understanding of relevant audit methodologies and best practices;

(c) evidence of the applicant's professional indemnity insurance policy with sufficient coverage for compliance audit activities;

(d) a completed declaration form signed by the applicant on their commitment to ethical conduct;

Considerations for Accreditation.

12. The Data Commissioner shall only accredit an applicant if the Data Commissioner is satisfied that the applicant—

(a) is a fit and proper person to be accredited, considering factors such as their professional conduct;

(b) possesses the necessary qualifications or experience to conduct data protection audits;

(c) maintains adequate professional indemnity insurance to cover potential liabilities arising from their audit activities;

(d) has not engaged in any conduct that would bring the Office or the accreditation process into disrepute.

Granting of Accreditation.

13. (1) Upon being satisfied that the applicant meets all the criteria set, the Data Commissioner shall grant an accreditation upon the applicant paying an accreditation fee of Kshs. 150,000

(2) The accreditation shall be valid for a period of three years from the date of issuance.

Refusal to accredit

14. (1) The Office may refuse to accredit where the Applicant—

(a) Submits false or misleading information in their application;

(b) Does not meet the requirements for accreditation under these Regulations;

(c) Fails to provide any other information required for accreditation

(2) The Office shall notify the applicant of its decision to refuse the application

Renewal of accreditation.

15. (1) An auditor may apply for renewal of their accreditation on the expiry date of the current accreditation

(2) An application for renewal of accreditation shall be made pursuant to Form DP 2 set out in the First Schedule.

(3) The Data Commissioner may renew an accreditation if the accredited auditor continues to meet the criteria set out under these regulations

(4) An application for renewal of accreditation shall pay an application processing fee of Kshs. 5,000

(5) Upon being satisfied that the applicant continues to meet all the criteria set out in this Part, the Data Commissioner shall renew the accreditation upon payment of the accreditation renew fee of Kshs. 100,000

Revocation of Accreditation

16. (1) The Data Commissioner may revoke an accreditation granted under these Regulations if the accredited auditor—

(a) fails to comply with the terms and conditions of the accreditation;

(b) Engages in conduct that is detrimental to the objectives of the Act and these Regulations;
(c) Provides false or misleading information in their application or during the accreditation process;
(d) Ceases to meet the criteria set out in regulation 11; or
(e) is found liable of an offense related to data protection.

(2) The Data Commissioner shall give the auditor a written notice of 14 days of the intention to revoke their accreditation, outlining the reasons for the proposed revocation and offering an opportunity to be heard.

(3) The Data Commissioner shall make a final decision on the revocation of accreditation following consideration of any representations made by the auditor.

Register of Accredited Data Protection Auditors

17. (1) The Data Commissioner shall maintain a public register of all auditors.

(2) The register may contain the following information—

(a) Name and contact details of the auditor;

(b) Date of accreditation and expiry date;

(c) Any limitations or conditions imposed on the accreditation; and

(d) Any other relevant information that may be required by the Office

(3) The Office shall update the register regularly to reflect any changes in the status of auditors.

PART IV – CONDUCT OF DATA PROTECTION COMPLIANCE AUDIT

Initiation of a Data Protection

18. (1) The Data Commissioner may initiate a compliance audit—

Compliance Audit by the office

(a) upon receiving complaints from individuals regarding an entity's data protection practices;

(b) as part of a broader regulatory investigation or enforcement action; or

(c) based on a risk assessment, complaint, or other information indicating potential non-compliance; or

(d) in response to a perceived or real privacy risk, data breach notification, significant changes in data processing activities, a petition or the initiative of the Office.

(2) The Data Commissioner shall give a 30-day notice to the data controller or the data processor of the decision to initiate an audit, outlining the—

(a) scope and purpose of the audit.

(b) expected timeframe for the audit.

(c) information and documentation required from the data controller or data processors .

Initiation of an Audit by a data controller or data processors

19. (1) A data controller may on their own volition undertake a data protection audit—

(a) to proactively assess their data protection posture and compliance with the Act.

(b) as part of a corrective measure following a data breach or other data protection compliance concerns.

(2) A data controller or data processor initiating a voluntary data protection audit may engage an auditor to conduct an audit.

Manner of Conduct of the Data Protection Audit.

20. (1) The Data Commissioner or the accredited data protection auditor, as applicable, may—

(a) develop a detailed audit plan outlining the methodology, scope, and timeline for the audit.

(b) conduct interviews with relevant personnel of the data controller or data processor.

(c) Review relevant documentation and records related to data processing activities, including—

(i) data protection policies and procedures;

(ii) records of data processing activities;

(iii) data security measures;

(iv) records of data subject requests and responses;

(d) Perform any necessary tests or assessments to evaluate compliance with the Act's requirements.

Responsibilities of the Data Controller

21. (1) The data controller or data processor shall provide the auditor with reasonable access to all relevant information and documentation necessary for conducting the audit.

(2) The data controller or data processor shall designate a contact person to facilitate communication and coordination with the auditor throughout the audit process.

(3) The data controller or data processors shall cooperate fully with the auditor and address any identified non-compliance issues in a timely manner.

Responsibilities of the Auditor

22. (1) The data protection auditor shall conduct the audit in accordance with professional standards and best practices.

(2) The auditor shall—

(a) plan and scope the audit effectively based on the specific needs and context of the data controller or data processors.

(b) employ appropriate audit methodologies to assess compliance with data protection requirements.

(c) Maintain the confidentiality and security of all information received during the audit process.

(3) The auditor shall not engage in any activities that may create a conflict of interest with their role as an independent auditor.

Reporting of Audit Findings.

23. (1) After completing the audit, the auditor shall prepare a written report outlining—

(a) scope and methodology of the audit;

(b) findings of the audit, including any identified non-compliance issues;

(c) Recommendations for corrective actions to address any non-compliance identified any identified areas for further review

(2) The data controller or data processor shall be provided with a copy of the draft audit report and be given a reasonable timeframe to respond to the findings and recommendations.

Publishing audit reports.

24. The Office may publish a summary of the audit findings to promote public awareness and enhance compliance with the Act.

Follow-up and Enforcement Actions

25. Based on the audit findings, the Data Commissioner may—

(a) issue recommendations for improvement to the data controller or data processors

(b) issue an enforcement notice or penalty notices requiring the data controller or data processor to take specific corrective actions;

(c) initiate further investigation or enforcement proceedings in cases of serious non-compliance.

(2) The data controller or data processor shall implement the recommended corrective actions within a timeframe proposed in the audit report or specified by the Data Commissioner.

(3) In the follow-up process, the Data Commissioner may conduct further audits or require the data controller or data processor to submit evidence of compliance with the recommendations.

Cooperation and Confidentiality

26. (1) The Data Commissioner, the auditor, and the data controller or data processor shall all cooperate in a professional and timely manner throughout the audit process.

(2) All information obtained during a data protection compliance audit shall be treated as confidential, except for information:

(a) disclosed with the authorization of the data controller or data processor; or

(b) Required to be disclosed by law; or

(3) The Office and auditors shall implement appropriate safeguards to protect the confidentiality of personal data accessed during the audit process.

Reporting and Accountability

27. (1) The Office shall prepare and publish an annual report on the implementation of these Regulations, including the number of audits conducted, audit findings, and actions taken.

(2) The report shall be made available to the public to promote transparency and accountability.

SCHEDULE

FORM DPA 1

APPLICATION FOR ACCREDATION OF DATA PROTECTION AUDITORS

SECTION 1: ESTABLISHMENT DETAILS

1. Address

Name of Establishment: ……

Postal Address: …… Physical Address……

County……. Country: ……

Telephone Number: ……. Email Address……

2. Firm Registration

Business Entity: [ ] Sole Proprietor [ ] Partnership [ ] Registered Company

Certificate of Incorporation Number (Attach copy of certificate) ……..

Current Business Licence/Practising Licence Number (Attach certified copy)
……

3. Evidence of the applicants academic and professional qualifications in data protection

(*Attach Copies of Academic Certificates and CVs. For foreign staff attach certified copies of work permits*)

No.	Full Names	Nationality	Highest Qualification	Years of Experience

SECTION 3: FIRMS EXPERIENCE

1) Attach particulars (Award letters, Completion Certificate, Acceptance Certificate, Recommendation Letter) of ongoing and past audits executed before by the firm.

No.	Name and Location of Client/ Employer	Type of audit	Scope of the audit.	Start and Completion Dates	Contact Details of the Client

SECTION 5: DECLARATION

Note, any attempt to falsify the information provided through misinterpretation may result in prosecution.

☐ I certify that the information given in this application is accurate to the best of my knowledge.

Name _____ Position _____

Signature _____ Date _____

FORM DPA 2

RENEWAL FORM FOR ACCREDATION OF DATA PROTECTION AUDITORS

SECTION 1: ESTABLISHMENT DETAILS

1. **Address**

Name of Establishment: ……

Postal Address: …… Physical Address……

County……. Country: ……

Telephone Number: …… Email Address……

4. **Firm Registration**

Business Entity: [ ]Sole Proprietor [ ] Partnership [ ] Registered Company

Certificate of Incorporation Number (Attach copy of certificate) ……..

Current Business Licence/Practising Licence Number (Attach certified copy)
…….

5. **Evidence of the applicants academic and professional qualifications in data protection**

(*Attach Copies of Academic Certificates and CVs. For foreign staff attach certified copies of work permits*)

No.	Full Names	Nationality	Highest Qualification	Years of Experience

SECTION 3: FIRMS EXPERIENCE

2) Attach particulars (Award letters, Completion Certificate, Acceptance Certificate, Recommendation Letter) of ongoing and past audits executed by the firm in the last three years.

No.	Name and Location of Client/ Employer	Type of audit	Scope of the audit.	Start and Completion Dates	Contact Details of the Client

Note, any attempt to falsify the information provided through misinterpretation may result in prosecution.

☐ I certify that the information given in this application is accurate to the best of my knowledge.

Name

Position

Signature

Date