

# **DRAFT CODE OF CONDUCT FOR DATA PROTECTION COMPLIANCE ORGANIZATIONS (DPCOS)**

## **TABLE OF CONTENTS**

### **PREAMBLE**

ARTICLE 1: OBJECTIVES

ARTICLE 2: PRINCIPLES

ARTICLE 3: REGISTRATION OF DPCOS

ARTICLE 4: COMPLIANCE SERVICES

ARTICLE 5: RESPONSIBILITY TO DATA SUBJECTS

ARTICLE 6: RESPONSIBILITY TO THE BUREAU

ARTICLE 7: RESPONSIBILITY TO CLIENTS.

ARTICLE 8: PERSONAL RESPONSIBILITY

ARTICLE 9: RESPONSIBILITY TO OTHER DPCOs

ARTICLE 10: TERMINATION

**WHEREAS,** the Nigeria Data Protection Regulation (NDPR) 2019 under Article 4.1(4) provides for the registration and licensing of Data Protection Compliance Organizations (hereafter referred to as DPCOs) to carry out specific compliance services in respect of data privacy and protection;

**NOTING** that the concept of DPCO is novel in data processing ecosystem and the Bureau is desirous of providing a code of conduct that shall foster the development of the DPCO models as a concept that holds the potential for strengthening professionalism, integrity and trust in the data governance processes of Nigeria's digital economy;

## **ARTICLE 1: OBJECTIVES**

The objectives of this code of conduct are to:

- 1.1 Promote professionalism in compliance service delivery within the data privacy and protection ecosystem;
- 1.2 Ensure fundamental uniformity in compliance processes under extant regulatory framework for data processing;
- 1.3 Encourage the adoption of data ethics as a guiding principle in data protection compliance services.
- 1.4 Foster discipline and uphold accountability among Data Protection Compliance Organizations (DPCOs); and
- 1.5 Prescribe fundamental standards in continuous capacity building and awareness creation services which may be carried out by DPCOs
- 1.6 Encourage Corporate Social Responsibility for the advancement of Data Privacy and Protection in Nigeria.
- 1.7 Foster trust in the data governance processes of Nigeria's digital economy.

## **ARTICLE 2: PRINCIPLES**

- 2.1 This Code of conduct shall be read in conjunction with extant legal regulatory framework on data protection in Nigeria.
- 2.2 A DPCO shall foster the advancement of fundamental rights and freedoms of data subjects whenever such rights and freedoms may be adversely impacted by data processing.
- 2.3 A DPCO shall make deliberate effort to encourage the adoption of data ethics particularly where a data controller or processor is permitted to exercise its discretion, as it were, in data processing.
- 2.4 This Code of Conduct acknowledges and upholds relevant rules of professional conduct which are binding on a professional prior to his engagement in data protection compliances; consequently, such professional shall be held accountable under such antecedent rules of professional conduct that seek to promote integrity and professionalism in the practice of his core profession.
- 2.5 In all transactions and circumstances, a DPCO shall uphold high ethical and professional standard and shall particularly abide by the Core Values of the Bureau, namely:- Accountability, Integrity, Fairness and Transparency.
- 2.6 A DPCO is solely responsible for its acts and omissions in the execution of its contract with a data controller and processor. Accordingly, no representation of a DPCO shall suggest or imply that it has been designated or appointed directly or indirectly to any data controller or data processor.
- 2.7 A DPCO shall eschew all acts and omissions that are likely to engender hostile relations with another DPCO.

## **ARTICLE 3:- REGISTRATION OF DPCOS**

- 3.1 A Data Protection Compliance Organization (DPCO) shall be duly registered with the Bureau as a condition precedent to rendering compliance services to a data controller or a data processor on the regulatory platforms of the Bureau.
- 3.2 Regulatory platforms may be created by the Bureau to, among others, facilitate:
  - a) Filing of regulatory Compliance Audit Returns,
  - b) Filing of Basic Data Risk Mitigation and Accountability Returns,
  - c) Data Privacy Impact Assessments,
  - d) Standard Contractual Clauses
  - e) Binding Corporate Rules, and
  - f) Data Breach Notification
  - g) Certification Process for Data Protection Officers
- 3.3 At the point of registration and at all times, the Bureau may demand, a DPCO to provide accurate and honest information in respect of all questions and requirements pertaining to its registration.
- 3.4 The following categories of service providers are eligible for registration as DPCOs:
  - a) Professional Service Consultancy firm
  - b) IT Service Provider
  - c) Audit firm
  - d) Law firm
- 3.5 A firm that is desiring to be registered as a DPCO shall have at least one personnel who is verifiably competent in any of the following fields:
  - a) Data Protection and Privacy
  - b) Information Privacy
  - c) Data Science
  - d) Information Audit

- e) Data Management
- f) Information security
- g) Data protection legal services
- h) Information Technology Due Diligence
- i) EU GDPR implementation and compliance
- j) Cyber Security/Cyber Security law
- k) Data Analytics
- l) Data Governance

3.6 On no account shall a DPCO carry out any compliance service under extant regulatory framework on data privacy and protection without having at least one personnel who is verifiably competent in any of the fields listed in Article 3.5.

3.7 The Registration of a DPCO and Certificate issued to it shall be valid for 2 years only.

#### **ARTICLE 4: COMPLIANCE SERVICES**

4.1 Upon agreement with a Data controller or a Data processor, a DPCO may carry out one more of the following services:-

- a) Data protection regulations compliance and breach services for Data Controllers and Data Administrators
- b) Data protection and privacy advisory services
- c) Data protection training and awareness services
- d) Data Regulations Contracts drafting and advisory
- e) Data protection and privacy breach remediation planning and support services
- f) Information privacy audit
- g) Data privacy breach impact assessment
- h) Data Protection and Privacy Due Diligence Investigation
- i) Outsourced Data Protection Officer etc

## **ARTICLE 5: RESPONSIBILITY TO DATA SUBJECTS**

- 5.1 A DPCO shall take appropriate technical and organizational measures to uphold data subject rights as contained or contemplated in relevant regulatory frameworks on data privacy.
- 5.2 A DPCO owes a duty of care to data subjects where such DPCO engages directly with data subjects for the purpose of providing expert advice or information on behalf of a data controller or a data processor to the data subjects.
- 5.3 A DPCO shall, without delay, notify a data controller or a data processor of any complaint or request it received from a data subject on behalf the data controller or data processor.
- 5.4 A DPCO shall without delay notify a data subject of any relevant action taken in response to his complaint or request.

## **ARTICLE 6: RESPONSIBILITY TO THE BUREAU**

- 6.1 A DPCO shall:-
  - a) Conduct its transactions with the Bureau in a transparent and efficient manner. Such transactions include audit filed with the Bureau.
  - b) Make transparent disclosures in all documents pertaining to audit, registration, data privacy impact assessment or any other processes required by the Bureau to carry out its regulatory mandate.
  - c) Attend meetings of DPCOs as may from time to time be required by the Bureau, provided that whenever practicable the Bureau shall make provisions for virtual attendance.
  - d) Inform the Bureau of any matter or development which in the opinion of the DPCO is beneficial to the work of the Bureau.

- e) Carry out awareness programmes for members of the general public on data privacy and protection as a corporate social responsibility.
- 6.2 It is the responsibility of a DPCO to notify the Bureau of any corporate restructuring such as mergers or acquisition, winding up processes and major judicial proceedings that may lead to changes in the record of the DPCO which had been submitted to the Bureau.
- 6.3 A DPCO shall relay general or relevant, specific notices to data controllers and data processors, provided that data a data controller or a data processor shall not claim ignorance of any relevant information only for the reason that such information was not provided by its appointed DPCO.
- 6.4 DPCOs should at intervals update their information registered with the Bureau; Email address and Contact number.

#### **ARTICLE 7: RESPONSIBILITY TO CLIENTS.**

- 7.1 A DPCO owes a duty of care to the data controller or data processor that engages it to carry out compliance services in respect of data privacy and protection,
- 7.2 A DPCO shall:
- a) Provide adequate information to clients on scope of work to be done in compliance with extant data privacy and protection regulation.
  - b) Carry out its task promptly, diligently and in accordance with high professional standards.
  - c) Notify the data controller or data processor - in whose service it is engaged – of any relevant regulatory notice or processes.

- d) Provide advice to a data controller or data processor - in whose service it is engaged – on the adoption of the principles of data ethics for the purposes of data processing.
- e) Provide compliance services through verifiably competent personnel – taking into consideration the intricacies of legal, organizational and technological aspects of data privacy and protection.

## **ARTICLE 8: PERSONAL RESPONSIBILITY**

8.1 A DPCO shall:

- a) Regularly undertake trainings for its personnel.
- b) Ensure it carries out its work in an environment that is conducive to data privacy and protection.
- c) Be knowledgeable about practices, rules and procedures of data privacy and protection.
- d) Subject to operation of law, ensure confidentiality of information that may come to its knowledge
- e) Ensure high professionalism and integrity on the part of its personnel.
- f) Take appropriate disciplinary measures against erring personnel as may be permitted by relevant employment laws.

8.2 It is prudent for a DPCO to file compliance audit returns in respect of its own data processing activities due to the sensitivity of its compliance services to data controllers and data processors.

## **ARTICLE 9: RESPONSIBILITY TO OTHER DPCOs**



- 9.1 A DPCO shall at all times promote friendly relationship with other DPCOs.
- 9.2 Where a data processor intends to hire a former officer of another DPCO, it is ethical and prudent to request a reference letter from the former DPCO who was the employer of the prospective employee.
- 9.3 Care must be taken by each DPCO to avoid using former employees to divert the clients of their former employers to their new employers.
- 9.4 A DPCO is encouraged to be involved in the activities of the Association of Data Protection Compliance Organization of Nigeria.

#### **ARTICLE 10: TERMINATION**

- 10.1 In the event of negligence, failure or refusal on the part of a DPCO to comply with the provision of this code of conduct, The Bureau after investigation may revoke or suspend the license of the said DPCO.