GUIDANCE NOTICE

NDPC/HQ/GN/VOL.01/23

GUIDANCE NOTICE ON THE FILING OF DATA PROTECTION COMPLIANCE AUDIT RETURNS(CAR) FOR 2022.

(Pursuant to Section 6(c)-(d) of the Nigeria Data Protection Act)

PREAMBLE

WHEREAS, the Nigeria Data Protection Act (NDP Act) 2023 preserves the filing of Data Protection Compliance Audit Returns (CAR), which CAR is an obligation for data controllers and data processors under the Nigeria Data Protection Regulation (NDPR) 2019;

COGNIZANT of the purpose of CARs as tools for promoting transparency and accountability in the processing of personal data and for fostering a culture of respect for the privacy of data subjects; and that failure, refusal or negligence in filing CAR to demonstrate accountability may disqualify a data controller or data processor to be listed under the National Data Protection Adequacy Programme (NaDPAP) Whitelist;

NOTING that a new cycle of CAR filing will commence in 2024 under the NDP Act and its General Application and Implementation Directive (GAID); and desiring to give Data Controllers and Data Processors the opportunity to demonstrate accountability and be included on the NaDPAP Whitelist in line with the compliance metric (more particularly described in the schedule to this Guidance Notice;

THUS, the Nigeria Data Protection Commission (hereafter referred to as the Commission) provides the following Guidance:

1. **RELIANCE ON NDPR FOR FILING OF CAR**

   Data Controllers and Data Processors are to rely on Articles 4.1(5) and (7) of the NDPR to file CAR with the Commission. Note that by virtue of Section 64(2)(f) of the NDP Act, the NDPR subsists - subject to any overriding provision of the NDP Act or regulatory instruments issued pursuant to the NDP Act.

2. THE ROLE OF DATA PROTECTION COMPLIANCE ORGANIZATIONS

a) Data Protection Compliance Organizations (DPCOs) are to facilitate the filing of CAR with the Commission with minimum financial constraints to Data Controllers and Data Processors.

b) Where occasions warrant, DPCO may undertake CAR work as a Corporate Social Responsibility (CSR) particularly for start-ups, not-for-profit-organizations and low revenue organizations - taking into consideration the need to promote a culture of voluntary compliance.

c) CAR should be used as an opportunity for practical training of designated Data Protection Officers (DPOs) and other members of staff.

d) Evidence of practical training will entitle a designated DPO to Continuous Professional Development (CPD) Credit. CPD is an essential audit parameter under the NDP Act GAID which will be issued in the 1st Quarter of 2024.

e) DPCOs are to bring this Guidance Notice to the attention of their clients or prospective clients.

3. CAR FOCUS AREA

a) In the report accompanying the audit questions, emphasis should be on:

i. Awareness,
ii. Capacity Building,
iii. Privacy Policy,
iv. Compliance Directives to Employees, Contractors, Agents, etc.
v. Availability of Data Protection Officers,
vi. Categories of Personal Data being processed (the Principles applied and the Lawful Basis for Processing,
vii. Technical Measures for ensuring Confidentiality, Integrity and Availability of Personal Data (with focus on Privacy by Design and by Default),
viii. Grievances Redress Mechanism, and
ix. List of agents or contactors being engaged for data processing and the due diligence as to their training and general compliance with the NDP Act.

b) For the year 2022, agents or contractors of data controllers who carry out data processing for data controllers shall only provide details of their Technical and Organizational Measures (TOM) for data protection in the Digital TOM form provided by the Commission.

4. COMPLIANCE MEMORANDUM

a) A data controller or data processor may outline a time bound intention to regularize its data processing activities in line with the NDP Act in a memorandum.
b) The memorandum should contain the focus areas under paragraph 3 above, signed by the designated DPO of the data controller or processor and sent to the Commission as part of the CAR.
c) The Commission shall take note of the Memorandum as a *bona fide* commitment to NDP Act Compliance
d) A time bound intention shall not be later than 31st of March, 2024.

5. FREE INDUCTION TRAINING FOR DESIGNATED DPOs

a) All designated DPOs are required to participate in an induction training to be organized by the Commission in January 2024.
b) The training will focus on data subjects' rights and compliance obligations of data controllers and data processors under the NDP Act and its GAID.

6. DEFAULT FEE

Under the NDP Act and the NDPR, the deadline for filing is the month of March. The applicable date for 2022 CAR under this Guidance is 15th of March, 2023. Default fee which is 50% of the filing fee applies when a data controller could not file on or before the said deadline for 2022 CAR.

SCHEDULE

The Compliance Metrics under National Data Protection Programme (NaDPAP) Whitelist are rated as follows:

S/N	METRICS	NDP ACT SECTIONS	POINT
1	*Verifiable Evidence of Conformity with Data Protection Principles and Lawful Basis. (Privacy Policies and Notices, Consent forms, Visitors Book, audio visual evidence of compliant data processing, etc may be used)*	**24 & 25**	**15**

2	Accountability and Prompt Responsiveness to Regulatory Processes. *(Timely filing of CAR, Resolution of Complaints, Registration and Data Subjects Access Request are focal areas)*	**24, 6(d), 24(3) & 61(2) (g),**	15
3	Sensitization of Data Subjects on Data Subjects Rights	**27 & 34-38**	10
4	Appointment of A Verifiably Competent DPO	**32**	5
5	Engagement of a DPCO	**33**	5
6	Filing of Compliance Audit Returns	**6(d) & 61(2)(g)**	10
7	Data Privacy Impact Assessment	**28**	10
8	Accessible and Functional Internal Remediation Mechanism	**40(8)**	10
9	Globally Acceptable Information Security Certifications. Privacy by design is pivotal.	**24(2) & 39**	10
10	Continuous Awareness / Capacity Building Programme for Staff, Contractors, Licensees, etc (This in furtherance of the overall objectives of the Act	**1**	10
	TOTAL		**100**

NOTE THAT

i. The NaDPAP Whitelist is not an immunity list or a shield against data subjects' complaints.

ii. The Whitelist is a tool of accountability because it contains functional data of data controllers and processors. It is a rebuttable presumption that a data controller or a data processor on the list is committed to taking adequate technical and organizational measures in safeguarding data-subjects rights.

7. EFFECT OF NON-COMPLIANCE

Guidance Notices explains provisions of the Act and Good Practices. Where contravention of Guidance Notice relates to specific provision of the NDP Act, the liability for violation of the Act applies. For ease of reference, the liabilities prescribed under the NDP Act are as follows:

> 48.—(1) Notwithstanding any criminal sanctions under this Act, if the Commission, after completing an investigation under section 46 of this Act, is satisfied that a data controller or data processor has violated any provision of this Act or subsidiary legislation made under this Act, it —
>
> (a) may make any appropriate enforcement order or impose a sanction on the data controller or data processor; and
>
> (b) shall inform the data controller or data processor, and if applicable, any data subject who lodged a complaint leading to the investigation, in writing of its decision.
>
> (2) An enforcement order made or sanction imposed under subsection (1) shall include —
>
> (a) requiring the data controller or data processor to remedy the violation;
>
> (b) ordering the data controller or data processor to pay compensation to a data subject, who has suffered injury, loss, or harm as a result of a violation;
>
> (c) ordering the data controller or data processor to account for the profits realised from the violation; or (d) ordering the data controller or data processor to pay a penalty or remedial fee.
>
> (3) A penalty or remedial fee under subsection (2)(d) may be an amount up to the —
>
> (a) higher maximum amount, in the case of a data controller or data processor of major importance; or (b) standard maximum amount, in the case of a data controller or data processor not of major importance.
>
> (4) The "higher maximum amount" shall be the greater of — (a) N10,000,000, and (b) 2% of its annual gross revenue in the preceding financial year.
>
> (5) The "standard maximum amount" shall be the greater of — (a) N2,000,000, and (b) 2% of its annual gross revenue in the preceding financial year

For Enquiries, contact the Commission via info@ndpc.gov.ng You may visit www.ndpc.gov.ng. for the list of Data Protection Compliance Organizations licensed by the Commission.

Babatunde Bamigboye, Esq. CDPRP
Head of Legal, Enforcement and Regulations