The Nigeria Data Protection Regulation
Journey to Compliance
The Nigeria Data Protection Regulation (NDPR)

The National Information Technology Development Agency (NITDA) is statutorily mandated by the NITDA Act of 2007 to develop regulations for electronic governance and monitoring of the use of information technology and electronic data. Conscious of the concerns around privacy and protection of Personal Data and the grave consequences of leaving Personal Data processing unregulated, NITDA has issued the Nigeria Data Protection Regulation (NDPR). The objectives of the regulation are as follows:

- to safeguard the rights of natural persons to data privacy;
- to foster safe conduct for transactions involving the exchange of Personal Data;
- to prevent manipulation of Personal Data; and
- to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a sound data protection regulation.

The regulation applies to all storage and processing of Personal Data conducted in respect of Nigerian citizens and residents.

Examples of Personal Data:

- Employee information as managed by HR
- Customer and subscribers data
- Vendors and services providers information

Personal data may contain one or more of the following:

- Name, phone numbers, contact information
- Location information, financial information, transaction history
- Gender, ethnicity, health records, sexual orientation

Compliance Requirements:

The NDPR regulation requires that Data Controllers and Data Processors:

- Engage a Data Protection Compliance Organization (DPCO) to perform a Data Protection Audit and file a report with NITDA within the stipulated timeline
- Designate a Data Protection Officer (DPO) who will be responsible for driving NDPR compliance initiatives within the organization
- Document and publish a data protection policy in line with the requirements of the Data Protection Regulation
- Ensure continuous capacity building and training for Data Protection Officer and other personnel involved in processing personal data
Key Features of the NDPR

The Nigerian Data Protection Regulation introduces new restrictions on collection and processing of personal data and requires such activities to be in accordance with a lawful purpose consent by the Data subject. Compliance with these requirements will impact Data Protection Governance, Information Systems & Security Configuration, as well as Documented Policies & Processes.

Data Protection Governance

<table>
<thead>
<tr>
<th>Clarity of Privacy Policy</th>
<th>International Data Transfer</th>
<th>Explicit Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any medium through which Personal Data is being collected or processed shall display a simple and conspicuous privacy policy that the class of Data Subject being targeted can understand.</td>
<td>Transfer of Personal Data to a foreign country may be allowed where NITDA has decided that the affected country ensures adequate data protection. Transfer activities are subject to the supervision of the Honorable Attorney General of the Federation.</td>
<td>Consent is one of the lawful basis for obtaining and processing personal data. Consent must be informed, freely given and unambiguous.</td>
</tr>
</tbody>
</table>

Rights of Data Subject

The Controller shall communicate any information on processing relating to the Data Subject in a concise and accessible form.

Third Party Processing

Data processing by a third party shall be governed by a written contract between the third party and the Data Controller.

Prohibition of Improper Motives

No consent shall be sought, given or accepted in any circumstance that may engender propagation of atrocities, hate, child rights violation, criminal and anti-social acts.

Data Security

Data controllers and processors should implement security measures (including firewalls, data encryption technologies, etc.) to protect data from theft, cyber attack, manipulations, environmental hazards, etc.

Lawful Processing

Processing of data is lawful if, at least, one of the following applies: consent has been given; processing is necessary for the performance of a contract; compliance with a legal obligation; to protect the vital interests of the Data Subject or any public interests.

Data Integrity and Storage Limitation

Personal data should be:
- adequate, accurate and without prejudice to the dignity of human person;
- stored only for the period within which it is reasonably needed.

Information Systems & Security Configuration

Documented Policies & Processes

Potential Consequences for Non-Compliance with NDPR

Fines

Maximum penalty for breaches of data privacy rights on international transfers can be up to ₦10M or 2% of annual gross revenue of the preceding year, whichever is higher and based on the number of Data Subjects dealt with.

Reputational Damage

Negative publicity and damage to brand and reputation.

Prosecution

Prosecution of principal officers in the event of a severe data breach.
How KPMG Can Support

Why KPMG

DPCO License
KPMG has been licensed by NITDA as a Data Protection Compliance Organization (DPCO) to provide Data Protection Services in Nigeria

Global Centre-of-Excellence
We have a global Data Protection Center-of-Excellence providing compliance support for global standards on data protection, including GDPR

Experienced Team
We have an experienced team of Cybersecurity & Data Privacy consultants as well as Legal & Regulatory experts that have provided data protection services to clients within Nigeria.

Thought Leaders
We are active in producing thought leadership and studies on the data privacy, compliance and future of cyber security.

Our Services

Data Protection Compliance Support
- Drafting and review of policy documents & Gap assessment
- Remediation Support
- Training & Capacity Development

Data Protection Audit Services
- Scoping
- Execution
- Reporting & DPCO Verification

Outsourced Data Protection Officer
- Continuous DPO Support