NDPR ACADEMY

NDPR Academy® Foundation Course

MODULE 7:
NDPR LIABILITIES, PENALTIES AND REMEDIES

Module 7: Overview

In this Module, we will learn about:

7.1. Enforcement Framework; and

7.2. Liabilities, Penalties and Remedies

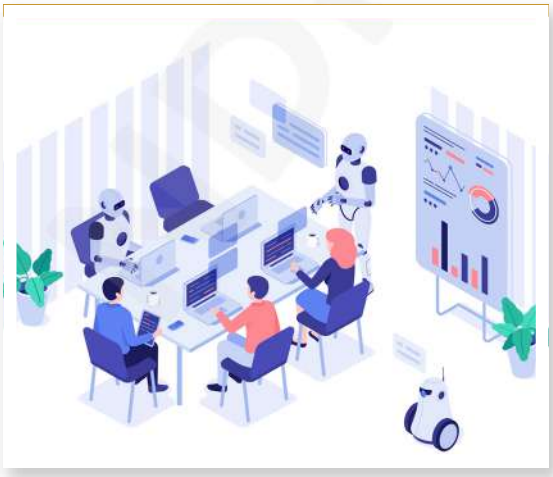
7.1 NITDA'S Enforcement Framework

7.1.1 NITDA's enforcement framework for NDPR is comprised of the following 5: Surveillance, Complaint Filing, Investigations, Administrative Sanctions; and Criminal Prosecution. We shall now turn to understanding each.

7.1.2 Surveillance: Surveillance refers to NITDA's specific and deliberate monitoring activity for the purpose of identifying a breach of the NDPR. This becomes necessary in the circumstance that Data Controllers or Data Administrators may or may not be in deliberate breach of the NDPR. A non-deliberate breach of the NDPR is however still a breach. NITDA adopts surveillance to also co-opt other relevant stakeholders to identify NDPR breaches and report such breaches to NITDA.

7.1.3 Complaint Filings: The Data Subject, a compliance officer, civil society, government agency or any person who believes that a Data Controller or Data Administrator is not complying with the NDPR can file a Complaint with NITDA.

7.1.4



Data Controllers and Data Administrators also have a duty to self-report Personal Data breaches. You may recall from Modules 2 and 4, the obligations placed on Data Controllers and Data Administrators to have policies and procedures for monitoring and reporting violations of privacy and Personal Data protection policies.[1] The NDPR Draft Implementation Framework sets the time-threshold for Data Controllers or Data Administrators at 72 (seventy-two) hours of their knowledge of the Personal Data breach. The Data Controller or Data Administrator's report must include, the:

[1] Article 4.2 (5) of NDPR

7.1.4.1

date or time/period during which the violating acts or omissions occurred;

7.1.4.2

description of the circumstances of the loss or unauthorised access or disclosure, for example, the cause of the breach;

7.1.4.3

an assessment of the risk of harm to Data Subjects as a result of the loss or unauthorised access or disclosure;

7.1.4.4

an estimate of the number of Personal Data and or Data Subjects that are at real risk of significant harm as a result of the loss or unauthorised access or disclosure;

7.1.4.5

description of remedial actions or any steps the Data Controller or Data Administrator has taken to reduce the risk of harm to Data Subjects;

7.1.4.6

description of any steps the Data Controller or Data Administrator has taken to notify the Data Subject of the loss or unauthorised access or disclosure; and

7.1.4.7

name and contact information of the Data Controller or Data Administrator's personnel or other person who can attend to NITDA's queries on the loss or unauthorised access or disclosure.

7.1.5 Complaints must be in writing and can be filed in paper format or electronically, for example, by email. NITDA may prescribe additional procedures for filing Complaints, as well as the place, manner and other details of filing.

7.1.6 The Complaint must disclose, the:

7.1.6.1 the name of the Data Controller, Data Administrator, Third Party or other person that is the subject of the Complaint (altogether Concerned Entity);

7.1.6.2 the violating acts or omissions of the Concerned Entity must be described;

7.1.7 Upon receipt of a Complaint, NITDA may take any of the following actions:

7.1.7.1 contact the Concerned Entity for enquiry;

7.1.7.2 review of earlier filed Annual DPA Report, if any, of the Concerned

7.1.7.3 issue a Personal Data protection compliance query;

7.1.7.4 impose administrative sanctions;[2] and

7.1.7.5 prosecute[3] the Concerned Entity.

7.1.8 **Investigations:** NITDA may by itself, or through an Administrative Redress Panel (ARP)[4] set up for that purpose, investigate any Complaint filed against a Concerned Entity when a preliminary review of the facts indicates a possible violation of the provisions of any regulatory instrument, especially the NDPR by the Concerned Entity. NITDA may by its officers or through designated DPCOs, investigate any filed complaint and may also do so based on a special audit or spot check.

Investigations may include a review of the policies, procedures, or practices of the Concerned Entity and of the circumstances of the alleged violation. NITDA will, at the time of the initial written communication to the Concerned Entity, indicate the basis of its audit or investigation.

7.1.9 **Administrative Sanctions:** NITDA can impose administrative sanctions for any breach of the NDPR. NITDA will do this through an ARP that may be set up for such purpose. An ARP is set up with the mandate of investigating and hearing of Complaints. To this end, the ARP:

7.1.9.1 will invite the Concerned Entity to respond to the Complaint within 7 (seven) days;[5] and

7.1.9.2 may, pending the outcome of the investigation, make administrative orders to protect the subject-matter of the Complaint.

2 Paragraphs 7.1.6 to 7.1.9 discusses Administrative Sanctions in detail.
3 Paragraph 7.1.10 discusses Prosecution.
4 Paragraphs 7.1.6 to 7.1.9 discusses the ARP in detail.
5 Article 4.2(3) of NDPR

7.1.10 ARPs, which will be comprised of accomplished information technology professionals, public administrators and lawyers, has 28 (twenty-eight) days to investigate, conclude and determine the appropriate redress on any Complaint.[6]

7.1.11 ARP's procedural rules is to be drawn up by a panel of experts. The rules are to feature the following principles:

7.1.11.1 preference for online dispute resolution mechanism;

7.1.11.2 fair hearing, fairness and transparency;

7.1.11.3 written processes, such that oral presentations are limited to the barest

7.1.11.4 decisions must clearly:

7.1.11.4.1 state the proof of violation;

7.1.11.4.2 identify the Concerned Entities in an anonymised, pseudonymised or summarised format;

7.1.11.4.3 state the violated NDPR provision and the acts or omissions which exacerbated the breach.

7.1.11.5 in reaching its decision, the ARP, NITDA or a Court may consider:

7.1.11.5.1 the nature, gravity and severity of the breach complained of;

7.1.11.5.2 the number of Data Subjects affected and damages suffered by them;

7.1.11.5.3 opportunities for curtailment left unexplored by the Concerned Entity;

7.1.11.5.4 whether the Concerned Entity has a reputation or history of data or other criminal or corporate breaches;

7.1.11.5.5 the number of employees in the Concerned Entity's establishment;

7.1.11.5.6 the possible impact of a fine on the Concerned Entity's overall contribution to the Nigerian economy.

6 Article 4.2 (5) of NDPR

7.1.12 The administrative sanctions or orders that can be made by any of the ARP, NITDA or the Court could include any of the following:

7.1.12.1

suspension of the Concerned Entity's service pending further investigations;

7.1.12.2

issuance of a public notice to warn the public to desist from patronizing or doing business with the Concerned Entity;

7.1.12.3

refer the Concerned Entity to its self-regulatory organization (SRO) for appropriate sanctions; a SRO in this case may be a trade association of self-interest organisation that the Concerned Entity is a member of.

7.1.13 **Criminal Prosecution:** Where NITDA has determined that a Concerned Entity's breach of the NDPR affects national security, sovereignty and cohesion, it may seek to prosecute the officers of the Concerned Entity pursuant to its criminal prosecution powers.[7] In this regard, NITDA will seek a fiat of the Honourable Attorney General of the Federation. It may also file a petition with any prosecuting authority in Nigeria. These prosecuting authorities include, the; Economic and Financial Crimes Commission, Department of State Security, Nigerian Police Force, Independent Corrupt Practices Commission; and Office of National Security Adviser to the President of the Federal Republic of Nigeria.

7.2 Liabilities, Penalties and Remedies:

7.2.1 A Data Controller that is found to be in breach of the Personal Data rights of a Data Subject, will be liable, in addition to any other criminal liability, to the following penalties:[8]

Number of Data Subjects	Penalty
<10,000 (Less than ten thousand)	1% (one percent) of the Data Controller's annual gross revenue of the preceding year or N2million (Two Million Naira), whichever is higher.
>10,000 (More than ten thousand)	2% (two percent) of the Data Controller's annual gross revenue of the preceding year or N10million (Ten Million Naira), whichever is higher.

[7] Section 17(1) and (3) of NITDA Act
[8] Article 2.10 of NDPR

7.2.2 The NDPR Draft Implementation Framework which is currently being discussed ahead of its release proposes that breach of a Data Subject's privacy rights be a strict liability offence.[9] What this means is that the intent, knowledge or otherwise of the Data Controller is not required to establish its culpability. Accordingly, the fact that the breach of a Data Subject's privacy rights occurred is conclusive of the commission of an offence and for which the above penalties will be imposed. Concerns have been raised on this issue and it appears that NITDA may move to de-classify the breach of a Data Subject's privacy rights as a strict liability offence in the final version of the Draft Implementation Framework.

7.2.3 The Data Subject may also seek redress for the violation of his or her privacy rights in a civil court of competent jurisdiction.[10] The Data Subject may in such instances sue both or either of the Data Controller or Data Administrator in tort, for the wrong.

7.2.4

A Data Administrator that breaches the terms of its contract with a Data Controller can similarly be sued for breach of contract by the Data Controller.

7.2.5

For Public Institutions that are Data Controllers, a breach of the NITDA Act, NDPR and NPIG is classified as an offence and punishable in line with Section 17 of the NITDA Act.[11]

9 Paragraph 4.2(iv) of the Draft Implementation Framework.
10 Article 4.2(1) of NDPR
11 Section 17 of NITDA Act provides:

17. Offences

(1)Except as otherwise provided in this Act, any person or corporate body who contravenes or fails to comply with the provisions of this Act commits an offence.

(2) Where a body corporate fails to make payment within two months after a demand note for unpaid levy plus a sum which is equal to 2 percent of this levy has been served on the body corporate, the body corporate commits an offence under this Act.

(3) Where an offence under this Act is committed by a body corporate or firm or other association of individuals

(a) Every Chief Executive Officer of the body corporate or any officer acting in that capacity or on his behalf; and

(b) Every person purporting to act n any capacity mentioned under paragraph (a) of this subsection (3);

commits an offence, unless he proves that the act or omission constituting the offence took place without his knowledge, consent or connivance.

(4) Where a person or body corporate fails to comply with the guidelines and standards prescribed by the Agency in the discharge of its duties under this Act, such person or body corporate commits an offence.

(5) The Agency shall collaborate with the Standards Organisation of Nigeria to enforce the guidelines and standards formulated by the Agency in the discharge of its duties under the Act.

7.2.6 In the spirit of the NITDA Act, NPIG expressly states that the Principal Officers of erring Public Institutions will be personally liable for breaches or any misuse of Personal Data. Their liabilities extends to both the duration and after the expiration of their term in office. A Principal Officer is a Public Officer who is responsible for leadership, management or administration of a Public Institution. Typically, the Principal Officer gives directives that other Public Officers are mandated to act on.

7.3 Definitions of Common Terms in Module 7:

We set out below, a glossary of the new terms and abbreviations used in this Module

	Term	Meaning
7.3.1	ARP	The Administrative Redress Panel, set up for the purpose of investigating any Complaint.
7.3.2	Compliant	A formal notification of the breach of the NDPR submitted to NITDA by any of a Data Subject, a compliance officer, civil society, government agency or any person who believes that a Data Controller or Data Administrator is not compliant with the NDPR
7.3.3	Concerned Entity	Any of the Data Controller, Data Administrator, Third Party or other person that is the subject of a Complaint
7.3.4	Principal Officer	A Public Officer who is responsible for leadership, management or administration of a Public Institution; and or upon whose directive other Public Officers are mandated to act or discharge their duties.
7.3.5	SRO	Self-Regulating Organisation, a trade association of self-interest organisation that a Concerned Entity is a member of

[12] Paragraph 7.0(a) of NPIG.

[13] Paragraph 9.0 of NPIG

7.4 Module 3: Summary

7.4.1 NDPR's enforcement framework is comprised of the following 5: Surveillance, Complaint Filing, Investigations, Administrative Sanctions; and Criminal Prosecution.

7.4.2 A Data Controller that is found to be in breach of the Personal Data rights of a Data Subject, will be liable, in addition to any other criminal liability to fines that could be up to 2% of its annual gross revenue in the preceding year or N10million, whichever is higher.

Further Reading:

1. 2019 Nigeria Data Protection Regulation [14]
2. National Information Technology Development Act 2007 [15]
3. NDPR Implementation Framework (Discussion Draft) [16]
4. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 [17]

[14] Available at: ndpracademy.ng/resources/Nigeria Data Protection Regulation.pdf
[15] Available at: https://ndpracademy.ng/resources/NITDA-act-2007.pdf
[16] Available at : ndpracademy.ng/resources
[17] Available at: https://ndpracademy.ng/resources/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal.pdf