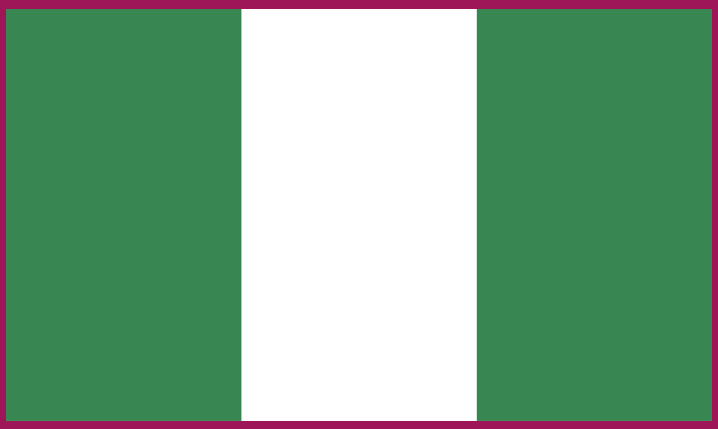


Comparing privacy laws:

GDPR v. Nigeria Data Protection Regulation

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Contributors

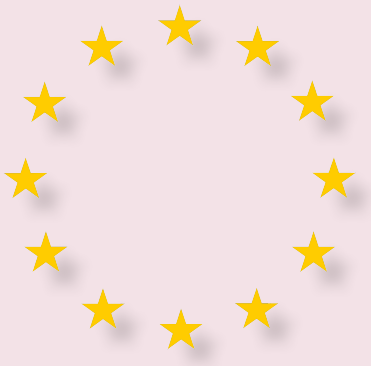
OneTrust DataGuidance™

Rhiannon Gibbs-Harris, Matteo Quartieri, Petra Molnar, Lea Busch, Amelia Williams, Alahi Kazi, Alexis Galanis, Marina Ioannou, Suzanna Georgopoulou, Victoria Ashcroft, Holly Highams, Alexis Kateifides

Image production credits:

Cover/p.5/p.51: alexsl / Signature collection / istockphoto.com | cnythzl / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.35-44: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Nigeria Data Protection Regulation ('NDPR') both aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share personal data, whether the information is obtained online or offline.

The GDPR, which went into effect on 25 May 2018, is one of the most comprehensive data protection laws in the world to date. The National Information Technology Development Agency ('NITDA') released the NDPR on 25 January 2019 and it is strongly influenced by the GDPR, with several articles containing very similar, or identical phrasing. Both the GDPR and the NDPR provide for data controllers and data processors which are referred to as 'data administrators' under the NDPR, for definitions of data breaches, for accountability requirements, and for the right to erasure.

The material scope of the two laws is also very consistent and both provide similar definitions for 'processing,' 'personal data' and 'sensitive personal data'. However, the GDPR applies to the processing activities of data controllers and data processors that do not have any presence in the EU, but where their processing activities are related to the offering of goods or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU. The personal and territorial scope of the NDPR is, however, defined by citizenship and physical presence, with the NDPR applying to residents of Nigeria, as well as Nigerian citizens abroad. In addition, the NDPR does not explicitly require any of the record-keeping obligations required by the GDPR, and does not outline how NITDA will calculate fines.

In July 2019, NITDA released the Draft Data Protection Implementation Framework ('the Draft Framework'). The Draft Framework refers to provisions which are not included in the NDPR. In particular, the Draft Framework requires data handlers to report data breaches to NITDA within 72 hours of their knowledge of the breach, and also outlines the information which must be included in such a report. Furthermore, the Draft Framework highlights the conditions under which a DPO must be appointed, and lists countries which have adequate data protection law or regulation that can guarantee minimum privacy for Nigerian citizens' data. The Draft Framework also stipulates which documentation is required to demonstrate compliance with the NDPR, and expands on NITDA's supervisory role. However, it is important to note that the Draft Framework has not been approved and is therefore not in effect.

This guide aims to highlight the similarities and differences between the NDPR and the GDPR to assist organisations in their compliance programs with both.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the NDPR.

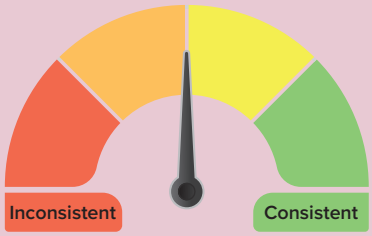
Key for giving the consistency rate

Consistent: The GDPR and NDPR bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and NDPR bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.

Fairly inconsistent: The GDPR and NDPR bear several differences with regard to scope and application of the provision considered, however its rationale and core presents some similarities.

Inconsistent: The GDPR and NDPR bear a high degree of difference with regard to the rationale, core, scope and application of the provision considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

Both the GDPR and the NDPR apply to data controllers and data processors, although the NDPR refers to data processors as 'data administrators.' However, while the GDPR applies to natural persons regardless of their nationality, the NDPR only applies to natural persons residing in Nigeria or to Nigerian citizens residing outside the national territory. Furthermore, while the GDPR applies to public bodies, the NDPR does not make a distinction between private and public bodies. .

GDPR	NDPR
Articles 3, 4(1) Recitals 2, 14, 22-25	Sections 1.1, 1.2, 1.3, 4.1

Similarities

The GDPR **only** protects **living individuals**. The GDPR does not protect the personal data of **deceased individuals**, this being left to Member States to regulate.

The NDPR aims to safeguard the rights of **natural persons** relating to data privacy. The NDPR **does not** explicitly refer to the living or **deceased status of individuals**.

The GDPR defines a **data controller** as a 'natural and legal person, public authority, agency or other body which, alone or jointly, with others, **determines the purposes and means** of the processing of personal data.'

The NDPR defines a **data controller** as 'a person who either alone, jointly with other persons or in common with other persons or a statutory body **determines the purposes for and the manner in which** personal data is processed or is to be processed.'

The GDPR defines a **data processor** as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'

The NDPR defines a **data administrator** as a 'person or an organization that processes data.' However, the term 'data processor' is used in Sections 2.4 and 4.1 of the NDPR.

Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'

The NDPR defines a **data subject** as 'any person who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.'

Differences

The GDPR **applies** to data controllers and data processors who may be **public bodies**.

The NDPR does not make a distinction between **private** and **public bodies**.

The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'

The NDPR applies to natural persons **residing** in Nigeria or to **Nigerian citizens** residing outside Nigeria's territory.

1.2. Territorial scope

Inconsistent

The GDPR applies to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. In particular, the GDPR applies to the processing of personal data of data subjects who are in the EU. The NDPR applies to all processing of personal data in respect of persons in Nigeria, or Nigerian citizens living abroad.

The GDPR applies extraterritorially if data controllers and data processors do not have a presence in the EU but their processing activities take place in the EU, or if the processing is related to the offering of goods or services to EU individuals or the monitoring of EU individuals' behaviour, whereas the NDPR has no equivalent provisions.

GDPR	NDPR
Articles 3, 4, 11 Recitals 2, 14, 22-25	Section 1.2

Similarities

GDPR	NDPR
Not applicable.	Not applicable.

Differences

GDPR	NDPR
The GDPR applies to organisations that have a presence in the EU, notably entities that have an '**establishment**' in the EU. Therefore, the GDPR applies to the processing of personal data by organisations **established** in the EU, regardless of **whether the processing takes place in the EU or not**.	There is **no equivalent** provision to '**establishment**' in the NDPR.
In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, but where their processing activities are related to the **offering of goods or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.	In relation to **extraterritorial** scope, the NDPR applies to persons residing **outside Nigeria** but only those who are **Nigerian citizens**, however has no further provisions on extraterritorial scope in respect of controllers and processors.

1.3. Material scope

The NDPR and the GDPR provide similar definitions for 'processing,' 'personal data' and 'sensitive personal data.'

Unlike the GDPR, the NDPR does not define or have any provisions on anonymous data or data processed by automated means. Although the NDPR provides a definition of 'sensitive personal data' which is similar to the GDPR's definition of 'special category data', it does not include specific provisions for the processing of sensitive personal data.

GDPR	NDPR
Articles 2-4, 9, 26 Recitals 14-21, 26	Sections 1.2, 1.3, 2.6, 2.11, 4.1

Similarities

GDPR	NDPR
The GDPR applies to the '**processing**' of personal data.	The NDPR applies to '**transactions intended for the processing of personal data**, to the **processing of personal data** notwithstanding the means by which the data processing is being conducted or intended to be conducted.'
The definition of 'processing' covers '**any operation or set of operations** which is **performed on personal data** or on sets of personal data, **whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'	The definition of 'processing' covers '**any operation or set of operations** which is **performed on personal data** or on sets of personal data, **whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'
The GDPR defines a **filing system** as 'any **structured set of personal data** which are accessible according to specific criteria, whether centralised, **decentralised or dispersed on a functional or geographical basis**.'	The NDPR also defines a **filing system** as 'any **structured set of personal data** which are accessible according to specific criteria, whether centralised, **decentralised or dispersed on a functional or geographical basis**.'

Differences

GDPR	NDPR
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	The NDPR **does not** directly address the processing of personal data by **non-automated means that is part of a filing system**.
The GDPR excludes **anonymous data** from its application, which is defined as 'information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.'	The NDPR **does not** reference anonymous data.

Differences (cont'd)

The GDPR **excludes** from its application the processing of personal data by individuals for **purely personal or household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'	The NDPR **does not** explicitly provide an exemption regarding the processing of personal data for **personal or household purposes**.
The GDPR **excludes** from its application data processing in the context of **law enforcement or national security**.	The NDPR **does not** explicitly exclude **law enforcement or national security** from its scope of application.
The GDPR provides **specific requirements** for the processing of sensitive personal data.	The NDPR **does not** include specific requirements for the processing of sensitive personal data.

2. Key definitions

2.1. Personal data

The GDPR and the NDPR provide similar definitions of 'personal data,' and both pieces of legislation specify that 'online identifiers' may be considered personal data. However, the GDPR specifies that it does not apply to anonymised data, which the NDPR does not refer to.

GDPR	NDPR
Articles 4(1), 9, 10 Recitals 26-30	Section 1.3

Similarities

The GDPR defines '**personal data**' as 'any information relating to an **identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

The NDPR defines '**personal data**' as 'any information relating to an **identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; it can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, International Mobile Equipment Identification number ('IMEI'), IMSI number, SIM, personal identifiable information and others.'

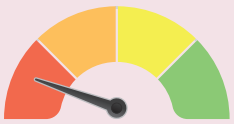
The GDPR defines **special categories of personal data** as data revealing a data subject's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'

The NDPR defines **sensitive personal data** as 'data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.'

The GDPR specifies that **online identifiers** may be considered as personal data, such as **IP addresses, cookie identifiers, and radio frequency identification tags**.

The NDPR provides that **online identifiers** may be considered as personal data, including unique identifiers such as **IP addresses, IMEI number, media access control address and IMSI number**, among others.

GDPR	NDPR
Differences	
The GDPR defines 'anonymised' data as data that can no longer be used to identify the data subject, and specifies that its provisions do not apply to such data.	The NDPR **does not** reference 'anonymised' data.
The GDPR notes that the processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.	'Criminal data' is categorised as sensitive personal data under the NDPR, but there are no explicit provisions on the processing of sensitive personal data under the NDPR.



Inconsistent

2.2. Pseudonymisation

Unlike the GDPR, the NDPR does not provide a definition for pseudonymised data.

GDPR Articles 4(5), 11 Recitals 26, 29	NDPR

Similarities

Not applicable.	Not applicable.

Differences

The GDPR defines **pseudonymised data** as 'the processing of personal data in such a manner that the personal data that can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'	The NDPR does not define **pseudonymised data**.

2.3. Controllers and processors

Fairly consistent

The NDPR and the GDPR provide for some similarities regarding the scope and responsibilities of data controllers. In addition, both the GDPR and the NDPR provide for data protection officer ('DPO') requirements, although the NDPR does not explicitly provide that a data processor must appoint a DPO. The NDPR does not define 'data processor' but provides the definition for 'data administrator' instead.

The GDPR specifically provides for a Data Protection Impact Assessments ('DPIAs') in certain circumstances, whereas the NDPR has no directly equivalent concept. However, the NDPR outlines that data controllers must have completed, within six months of the NDPR being issued, a detailed audit of privacy and data protection practices for assessing the impact of technology on privacy and security.

GDPR	NDPR
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38, 42 Recitals 64, 90, 93	Sections 1.3(x), 1.3(ix), 2.1, 2.3, 2.4(b), 2.6, 4.1

Similarities

A **data controller** is a natural or legal person, public authority, agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.	A **data controller** is a person who either alone, jointly with other persons, or in common with other persons, or a statutory body, determines the **purposes** for and the **manner** in which personal data is processed or is to be processed.
A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data on **behalf** of the controller.	Under the NDPR the definition of '**data administrator**' is provided and is defined as a person or an organisation that processes data. However, the term 'data processor' is used in Sections 2.4 and 4.1 of the NDPR.
Data controllers must comply with, among other things, the **purpose limitation and accuracy principles, and rectify** a data subject's personal data if it is **inaccurate** or **incomplete**.	The NDPR notes that personal data shall be collected and processed in accordance with a **specific, legitimate and lawful purpose consented to by the data subject** and that such data must be **adequate** and **accurate**.
Data controllers must implement **technical and organisational security measures**.	The NDPR **provides that anyone involved in data processing or the control of data shall develop security measures to protect data**; such measures include, protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing an organisational policy for handing personal data, protecting emailing systems, and providing continuous capacity building for staff

GDPR	NDPR

Similarities (cont'd)

The GDPR provides that where processing is to be carried out on behalf of a controller, the c**ontroller shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. In addition, the data processor shall not engage another data processor without prior specific or general written **authorisation** of the controller.	The NDPR provides, as part of due diligence and prohibition of improper motives, **that a party to any data processing contract, other than a data subject, must take reasonable measures to ensure that the other party does not have a record of violating data subject rights** outlined under Part 3 of the NDPR.
The GDPR provides where a sub-processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Data controllers and data processors may be held liable under the NDPR for the actions or inactions of third parties handling personal data under the NDPR.

Differences

The GDPR requires data controllers or data processors to designate a DPO in **certain specified circumstances**. Where an organisation is a **public authority**, or where their core activities consist of processing operations that require **regular and systematic monitoring** of the data subjects **on a large scale**, or where or where their core activities consist of **processing on a large scale** of **special categories of personal data** and data relating to **criminal convictions and offences**.	The NDPR requires **every data controller** to designate a DPO for the purpose of ensuring adherence to the NDPR.
Data controllers based outside the EU and involved in certain forms of processing, with exceptions based on the scale of processing and type of data, are obliged to **designate a representative based within the EU** in writing.	The NDPR **does not** provide an obligation to designate a representative within Nigeria.
The GDPR stipulates that data controllers and data processors keep **records of processing activities** and provides an exception from this obligation for small organisations.	The NDPR **does not** outline a specific requirement for data controllers or processors to keep records of processing activities.
The GDPR provides that a data controller or data processor conduct **DPIAs** in certain circumstances.	The NDPR **does not** expressly provide for DPIAs. However, the NDPR provides that within six months of its date of

GDPR	NDPR
Differences (cont'd)	
	issuance **organisations must have conducted a detailed audit of privacy and data protection practices** and its policy and procedure for assessing the impact of technologies on privacy and security. In addition, where data controllers process the personal data of **more than 1,000 data subjects** in a period of **six months**, they must submit a soft copy of the audit to NITDA. Furthermore, data controllers which process the personal data of more than **2,000** in a period of **12 months** must **submit a summary of the audit to NITDA on an annual basis**.
Data controllers must notify supervisory authorities of **data breaches**.	The NDPR **does not** provide a data breach notification requirement for data controllers.

2.4. Children

Unlike the GDPR, the NDPR does not grant special protection to children's personal data, nor does it specify whether the consent of a parent or guardian is needed when processing children's data. Whilst the GDPR provides protections in relation to the provision of information services, the NDPR appears to be wider in scope.

Both the GDPR and the NDPR mandate that controllers must take appropriate measures to provide information relating to processing that can be easily understood by a child.

The NDPR, unlike the GDPR, does not provide requirements for data controllers to make reasonable efforts to verify that consent is given by a parent or guardian when processing children's data.

GDPR	NDPR
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Section 3.1(1)

Similarities

GDPR	NDPR
The GDPR **does not** define 'child' nor 'children.'	The NDPR **does not** define 'child' nor 'children.'
When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.	The NDPR outlines that controllers must take **appropriate measures** to provide any information relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, and for any information relating to a child.

Differences

GDPR	NDPR
Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can provide by law for a lower age for those purposes provided that such lower age is **not below 13 years**.	The NDPR **does not** specify whether the consent of a parent or guardian is required for providing information society services to a child. Furthermore, the NDPR **does not** set an age limit for consent.
The GDPR considers children as 'vulnerable natural persons' that merit specific protection with regard to their personal data. In particular, specific protection should be given when children's personal data is used for marketing purposes or collected for information society services offered directly to children.	The NDPR **does not** specify whether specific protection should be given with regard to the processing of children's data.
The GPDR provides that data controllers are required to make reasonable efforts to **verify** that **consent** is given or authorised by a parent or guardian.	The NDPR **does not** specify whether data controllers are required to make reasonable efforts to verify that consent is given or authorised by a parent or guardian.

2.5. Research

Fairly consistent

Both the GDPR and the NDPR address the processing of personal data for research purposes. The GDPR has specific provisions regarding the processing of personal data for 'historical or scientific research,' as well as for 'statistical purposes.' Like the GDPR, the NDPR allowsthe further processingofpersonaldatafor 'archiving', 'scientificresearch' 'historical research' or 'statistical purposes,' but does not contain specific provisions on research related to data retention and derogations for data subject rights.

GDPR	NDPR
Articles 5(1)(b), 5(1)(e), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 156, 159-161	Section 2.1

Similarities

According to the GDPR, personal data shall be collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. However, further processing for **archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes** will not be considered to be incompatible with the initial purposes.

According to the NDPR personal data shall be collected and processed in accordance with **specific, legitimate and lawful purposes** consented to by the data subject with an exception permitting further processing only for **archiving, scientific research, historical research or statistical purposes for public interest**.

Differences

The GDPR clarifies that the processing of personal data for **scientific research** purposes should be interpreted 'in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.'

The NDPR **does not** provide an interpretation or definition of **scientific research**.

Under the GDPR, where personal data are processed for research purposes, it is possible for Member States to **derogate from some data subjects' rights**, including the right to access, the right to rectification, the right to object and the right to restrict processing, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such **derogations** are necessary for the fulfilment of those purposes.

Under the NDPR, there are **no derogations** for data subjects' rights when the processing is for research purposes.

The GDPR stipulates that data which is further processed for **archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes** may be **stored for longer** periods of time, subject to the implementation of appropriate technical and organisational measures.

The NDPR **does not reference** the retention period of data for **archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes** which is to be further processed, nor the implementation of technical or organisational measures.

GDPR	NDPR

Differences (cont'd)

Under the GDPR, the data subject has the **right to object** to the processing of personal data for research purposes **unless such research purposes are for reasons of public interest**.

Under the NDPR, data subjects have the right to be expressly and manifestly offered the mechanism for **objection to any form of data processing** free of charge.

3. Legal basis

Fairly consistent

Both the GDPR and the NDPR require a lawful basis for processing data, including consent, performance of a contract, legal obligation, vital interests, and public interest. Unlike the GDPR, the NDPR does not list legitimate interests as a lawful ground for processing data and does not restrict the processing of special categories of personal data.

GDPR	NDPR
Articles 5-10, 49 Recitals 39-48	Section 6

Similarities

The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds include:

- **consent**;
- when processing is necessary for the **performance of a contract** to which the data subject is party or in order to take **steps at the request of the data subject prior** to the entering into a contract;
- compliance with **legal obligations** to which the data controller is subject;
- to protect the **vital interests** of the data subject or of another natural person; or
- performance of a task carried out in the **public interest** or in the official authority vested in the data controller;

The NDPR states that processing is lawful only if one of the following applies:

- **consent**;
- when processing is necessary for the **performance of a contract** to which the data subject is party or in order to take **steps at the request of the data subject** prior to entering into a contract;
- compliance with a **legal obligation** to which the controller is subject;
- to protect the **vital interests** of the data subject or of another natural person; or
- performance of a task carried out in the **public interest** or in the exercise of official public mandate vested in the controller.

The GDPR recognises **consent** as a legal basis to process personal data and includes **specific information** on how consent must be obtained and can be withdrawn.

The NDPR recognises **consent** as a legal basis to process personal data and includes **specific information** on how consent must be obtained and can be withdrawn.

Differences (cont'd)

Under the GDPR, the processing of **special categories of personal data is restricted** unless an **exemption** applies, which includes the data subject's **explicit consent**.

Under the NDPR, there are **no specific requirements** for the processing of **sensitive personal data**.

The GDPR considers the **legitimate interests** of the data controller as legal grounds for processing when this does not override the fundamental rights of the data subject.

The NDPR **does not** recognise the legitimate interests of the data controller as legal grounds for processing. However, the controller must provide the data subject with information regarding the **legitimate interest** pursued by the controller or third party, prior to collecting personal data from a data subject. In addition, the right to erasure and right to restriction of processing apply where, among other things, there are no overriding legitimate grounds for the processing.

4. Controller and processor obligations

4.1. Data transfers

Both the GDPR and the NDPR provide for restrictions and exceptions to the cross-border transfer of personal data to a third country or international organisation. Such a transfer must be made based on legitimate grounds or to a third country or international organisation with an adequate level of data protection as prescribed by the relevant authority. However, under the NDPR, the grounds for a cross-border transfer do not include the transfer being made from a register which is accessible by the public, or by a person who can demonstrate legitimate interest.

GDPR	NDPR
Articles 44-50 Recitals 101, 112	Section 2.11, 2.12, 4.3

Similarities

The GDPR allows personal data to be transferred to a third country or international organisation that has an **adequate level of protection** as determined by the EU Commission. The GDPR further provides for specific criteria that the EU Commission will consider in determining the adequacy of a third country or international organisation, including the **rule of law, respect for human rights and fundamental freedoms, relevant legislation** of the third country, the existence and effective functioning of an **independent supervisory authority**, and the **international commitments** of the third country or international organisation concerned.

The NDPR allows personal data to be transferred to a foreign country, territory or one or more specified sectors within that foreign country, or an international organisation where NITDA has decided that the foreign country or international organisation ensures an **adequate level of protection**. The NDPR provides a similar list of criteria that NITDA or the Honourable Attorney General of the Federation ('HAGF') will consider in determining the adequacy of a third country or international organisation, including the **legal system of the third country**, the implementation of **data protection legislation**, the existence and functioning of an **independent supervisory authority**, and the **international commitments** of the third country or international organisation concerned.

Under the GDPR, in the absence of an adequacy decision, or the appropriate safeguards referred to below, the transfer of personal data to a third country or international organisation may only take place if one of the following legal grounds applies:

- when a data subject has **explicitly consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards;
- when the transfer is necessary for the performance of a **contract** between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

Under the NDPR, in the absence of any decision by NITDA or the HAGF as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of personal data to a foreign country or an international organisation shall take place only on one of the following conditions:

- the data subject has **explicitly consented** to the proposed transfer, after having been informed of the possible risks of such transfers;
- the transfer is necessary for the performance of a **contract** between the data subject and the controller or the implementation of precontractual measures taken at the data subject's request;

GDPR	NDPR

Similarities (cont'd)

- when the transfer is necessary for the conclusion or performance of a **contract** concluded in the interest of the data subject between the controller and another natural or legal person;
- when the transfer is necessary for important **public interest** reasons;
- when the transfer is necessary for the establishment, exercise, or defence of a **legal** claim; or
- when the transfer is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

- the transfer is necessary for the conclusion or performance of a **contract** concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of **public interest**;
- the transfer is necessary for the establishment, exercise or defence of **legal** claims; or
- the transfer is necessary in order to protect the **vital interests** of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Differences

The GDPR specifies that cross-border transfers based on **international agreements for judicial cooperation** are allowed.

The NDPR **does not** specify whether a cross-border transfer based on **international agreements for judicial cooperation** is allowed.

The grounds for a cross-border transfer include **the transfer being made from a register** which, according to EU or Member State law, is intended to provide information to the public, and which is open for consultation either to the public in general or to any person who can demonstrate a **legitimate interest**, but only to the extent that the conditions laid down by EU or Member State law are fulfilled in the particular case.

The NDPR **does not** provide for a similar register.

Under the GDPR, in the absence of a decision on an adequate level of protection, a transfer is permitted when **the data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure data subjects' rights as prescribed under the GDPR. **Appropriate safeguards include**:

- **Binding Corporate Rules** ('BCRs') with specific requirements, for example, a legal basis for processing, a retention period, and complaint procedures, among other things ;
- **Standard Contractual Clauses** ('SCC') adopted by the EU Commission or by a supervisory authority;
- an approved **code of conduct**; or
- an approved **certification mechanism**.

The NDPR **does not** provide for **safeguards** such as BCRs for the transfer of personal data.

GDPR	NDPR

Differences (cont'd)

The GDPR permits the transfer of personal data where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. However, there is **no requirement** to make the data subject **understand the specific principle(s)** of data protection which are likely to be violated.

Under the NDPR, the transfer of personal data to a foreign country or an international organisation may take place if the transfer is necessary in order to protect the **vital interests** of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent, provided, in all circumstances, that the data subject has been **manifestly made to understand** through clear warnings of the **specific principle(s) of data protection that are likely to be violated** in the event of transfer to a third country. However, this provision **does not apply** to any instance where the data subject is answerable in duly established legal action for any civil or criminal claim in a third country.

4.2. Data processing records

Inconsistent

The GDPR imposes an obligation to both controllers and processors to maintain a record of the processing activities under their responsibility and specifies what needs to be included in such records. The NDPR does not impose any obligations related to recordkeeping.

GDPR Articles 30 Recitals 82	NDPR

Similarities

GDPR	NDPR
Not applicable.	Not applicable.

Differences

GDPR	NDPR
Data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility. The GDPR **prescribes a list of information that a data controller** must record for **international transfers** of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards. The GDPR **prescribes a list of information that a data processor** must record: • the name and contact details of the data processor; • the **categories of processing** carried out on behalf of each controller; • international transfers of personal data, with the **identification of third countries or international organisations**, and the **documentation of adopted suitable safeguards**; and • a **general description** of the technical and organisational security measures that have been adopted. The GDPR **prescribes a list of information that a data controller** must record: • the name and contact details of the **data controller**; • the **purposes of the processing**; • a description of the categories of **personal data**; • the categories of recipients to whom the personal data will be **disclosed**; • the **estimated period for erasure** of the categories of data; and • a general description of the technical and organisational **security measures** that have been adopted.	The NDPR **does not** impose the obligation to maintain a record of processing activities on either the controller or the processor. The NDPR does not prescribe a list of **information that a data controller or data processor** must record for **international transfers** of personal data.

GDPR	NDPR

Differences (cont'd)

The obligations in relation to data processing records are also imposed on the **representatives of data controllers**.

The processing on information recorded by a data controller shall be in **writing or electronic form**.

The requirements around data processing records shall not apply to **an organisation with less than 250 employees**, unless the processing:

- is likely to result in a risk to the rights and freedoms of data subjects;
- is not occasional; or
- includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.

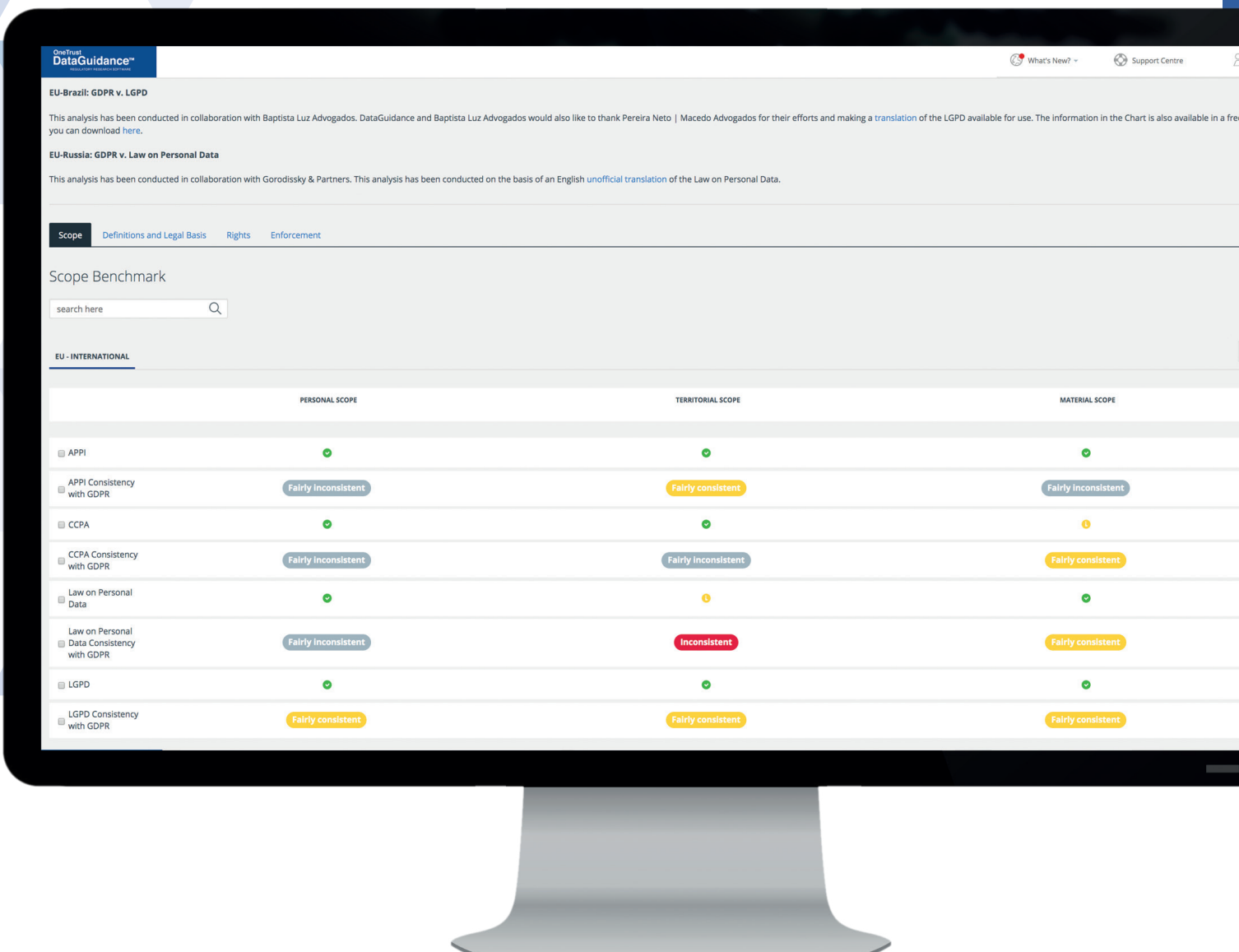
OneTrust DataGuidance™

REGULATORY RESEARCH SOFTWARE

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers
Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk
and achieve global compliance.

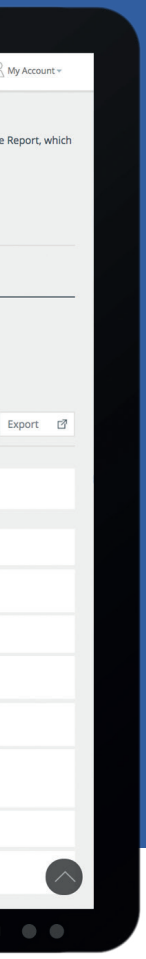


Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan

Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe.

The GDPR Benchmarking tool provides a comparison of the various pieces of legislation on the following key provisions.



- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

Start your **free trial** today at **dataguidance.com**

4.3. Data protection impact assessment

Inconsistent

The GDPR specifically provides for DPIAs in certain circumstances. Although the NDPR does not specifically refer to DPIAs, the NDPR requires controllers to conduct a detailed audit which must include an assessment of the impact of technologies on privacy and security policies.

Unlike the GDPR, the NDPR does not require controllers to notify the supervisory authority when the processing would result in a high risk to data subjects.

GDPR Articles 35, 36 Recitals 75, 84, 89-93	NDPR Section 4.1(5)(j)
Similarities	
Not applicable.	Not applicable.
Differences	
The GDPR requires controllers and processors to conduct a DPIA in certain circumstances, including when processing is likely to result in a **high risk** for the rights and freedoms of individuals, in particular if a data controller utilises **new technologies** to process personal data.	The NDPR **does not** make any reference to DPIAs. However, it does require a detailed audit to be conducted stating the policies and procedures of the organisation for **assessing the impact of technologies** on the stated privacy and security policies.
A data controller **must consult** the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation measures as indicated by the DPIA.	The NDPR **does not** require the data controller **to consult** the supervisory authority prior to any processing that would result in a high risk.

4.4. Data protection officer appointment

The NDPR and the GDPR both provide for an obligation to appoint a DPO. In addition, both laws stipulate that the contact details of the DPO must be communicated to the data subjects. However, compared to the GDPR, the NDPR does not provide such detailed provisions on DPOs and does not provide that the contact details of the DPO must be communicated to the supervisory authority.

GDPR	NDPR
Articles 13-14, 37-39 Recital 97	Sections 3.1(7), 4.1(2), 4.1(3)

Similarities

GDPR	NDPR
The GDPR establishes the role of a DPO.	The NDPR establishes the role of a DPO.
The DPO must be **provided with the resources necessary** to carry out his or her obligations under the GDPR.	The NDPR requires controllers to provide for the **continuous capacity building** of DPOs.
Contact details of the DPO must be included in the privacy notice for data subjects, and they must be communicated to the supervisory authority.	The NDPR addresses the duty of the data controller to provide the data subject with the contact details of the DPO.

Differences

GDPR	NDPR
Under the GDPR, data controllers and data processors, including their representatives, are required to **appoint** a DPO **in certain circumstances**. The data controller and the data processor shall designate a DPO in any case where: • the processing is **carried out by a public authority or body**, except for courts acting int heir judicial capacity; • the core activities of a data controller or data process or consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring** of data subjects on a **large scale**; or • the core activities of the controller or the processor relate to a large scale of **special categories of personal data** (e.g. religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims etc.)	The NDPR requires **every** controller to appoint a DPO, but **does not specify any requirement for processors to appoint a DPO**.
Under the GDPR, the DPO shall perform a list of tasks including: • **to inform and advise** the controller or the data processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;	The NDPR **does not address** the **tasks**, **nor the role of a DPO within an organisation**.

GDPR	NDPR

Differences (cont'd)

- **to monitor** compliance with the GDPR with other Union or Member State data protection provisions and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; and
- **to act as a contact point** the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The DPO shall be designated on the basis of **professional qualities and expert knowledge** of data protection law and practices. The DPO can be a **staff member** of the data controller or data processor, or can perform tasks based on a **service contract**.

The controller and the processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The DPO shall directly report to the highest management level of the controller or the processor.

The GDPR recognises the **independence** of DPOs. The DPO must not receive any instructions regarding the exercise of their tasks from the data controller or processor. In addition, the DPO cannot be dismissed or penalised by the controller or the processor for the performance of their tasks.

The DPO shall be designated on the basis of **professional qualities and expert knowledge** of data protection law and practices.

The DPO can be a **staff member** of the data controller or data processor, or can perform tasks based on a **service contract**.

4.5. Data security and data breaches

Fairly inconsistent

Both the GDPR and the NDPR recognise data security as a fundamental principle, and prescribe the development of technical and organisational measures on the same.

Unlike the GDPR, which mandates the notification of data breaches to the competent supervisory authority, the data controller, and the data subject, in certain situations and within specified timeframes, the NDPR does not require such notification in case of a breach.

GDPR	NDPR
Articles 5, 24, 32-34 Recitals 74-77, 83-88	Sections 2.1, 2.6

Similarities

The GDPR recognises **integrity** and **confidentiality** as **fundamental principles** of data protection by stating that personal data must be processed in a manner that ensures **appropriate security** of the personal data.

The NDPR recognises **security** as a governing **principle** of data protection.

The GDPR states that **data controllers and data processors are required to implement appropriate technical and organisational security measures** to ensure that the processing of personal data complies with the obligations of the GDPR.

The NDPR states that **data controllers and data processors shall develop security measures** to protect data.

Under the GDPR, a '**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The NDPR defines '**personal data breach**' as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

The GDPR provides a **list** of **technical and organisational measures**, where appropriate, that data controllers and data processors must implement such as pseudonymisation, encryption and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.

The NDPR provides a **list** of **technical and organisational measures** for data controllers and processors to implement. Under the NDPR, 'Such measures include but are not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.'

GDPR	NDPR
Differences	
Under the GDPR, a personal data breach must be notified to the supervisory authority **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.	Under the NDPR there is no requirement for data controllers to notify the supervisory authority of a breach, and therefore the NDPR **does not** provide a timeframe for such notification.
Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, **is exempted in certain circumstances** such as where: • appropriate technical and organisational protective measures have been implemented; • any subsequent measures have been taken in order to ensure that the risks are no longer likely to materialise; or • it would involve is proportionate effort.	The NDPR **does not** provide a requirement of notification, therefore there are **no exemptions**.
The GDPR **provides a list of information** that must be, at minimum, **included in the notification** of a personal data breach. For example, a notification must describe the nature of a breach, the approximate number of data subject concerned, and the consequences of the breach.	The NDPR **does not** establish a requirement of notification, therefore the NDPR does not provide a list of information.
The GDPR states that **data processors must notify** the data controller without **undue delay** after becoming aware of the personal data breach.	Under the NDPR, there is **no obligation** for data processors to notify the data controller of the breach.
The controller must **notify** the **data subject** of a data breach without undue delay if the data breach is likely to result in a **high risk** to the rights and freedoms of natural persons.	The NDPR **does not** provide an obligation to notify the data subject of a breach.

4.6. Accountability

Fairly inconsistent

Both the GDPR and the NDPR recognise accountability with respect to data processing as a fundamental principle of data protection. In addition, both the GDPR and the NDPR refer to the data controller's obligation to designate a DPO.

Unlike the GDPR, the NDPR provides that parties to a processing contract, apart from the data subject, are accountable to data protection authorities both inside and outside Nigeria. Moreover, the NDPR does not refer to an obligation to conduct a DPIA.

GDPR	NDPR
Articles 5, 24-25, 35, 37 Recital 39	Sections 2.1, 2.4, 4.1

Similarities

The GDPR recognises **accountability** as a fundamental principle of **data protection**. Article 5 states that 'the data controller shall be **responsible** and able to **demonstrate compliance** with, [accountability].' In addition, the principle of accountability can be taken to apply to several other principles as mentioned in other sections of this report..

The NDPR recognises **accountability** as a governing principle of data processing. In particular, Section 2.1(3) states 'anyone **who is entrusted with personal data of a data subject** or who is **in possession of personal data** of a data subject shall be **accountable** for his acts and omissions in respect of data processing.' This provision does not refer specifically to data controllers. However, as it refers to a person entrusted with personal data, this provision may cover data controllers.

In terms of **measures to ensure accountability** for data protection, the GDPR provides, among other things, that controllers and processors must **appoint a DPO** in certain circumstances, and lays down requirements for **processor contracts**.

In terms of **measures to ensure accountability** for data protection, the NDPR addresses the obligation of the data controller **to designate a DPO**, and lays down requirements for **processing contracts**.

Differences

In terms of measures to ensure accountability, the GDPR **requires DPIAs** to be conducted in certain circumstances, and requires controllers and processors to **maintain records of processing**. Unlike the NDPR, the GDPR **does not expressly** require organisations to conduct **audits** covering the impact of technology on privacy and security policies.

In terms of measures to ensure accountability, the NDPR does **not require DPIAs** to be performed, nor does it create the obligation to **maintain records of processing**. However, the NDPR refers to the obligation of an organisation to conduct a **detailed audit** covering the impact of technology on privacy and security policies.

The GDPR lays down several requirements with respect to **the content of processor contracts** to ensure the **accountability of processors**. However, it does **not expressly require** parties to such contracts to ensure that the other party has **not violated data subject rights**.

The NDPR **does not** lay down **express requirements** as to **the content of a processing contract**. However, it does address the obligation of a party to any **processing contract**, apart from the data subject, to take reasonable measures to **ensure that the other party has not violated data subject rights**. Furthermore,

GDPR	NDPR
Differences	
	the NDPR states that 'every data processor or controller shall be **liable for** the actions or inactions of **third parties** who handle the personal data of data subjects under the NDPR'.
Under the GDPR, processors and controllers are accountable to competent supervisory authorities in the EU.	The NDPR provides that parties to the processing contract are accountable to NITDA or any regulatory authority for data protection **either inside or outside Nigeria**.

5. Rights

5.1. Right to erasure

The GDPR and the NDPR both provide data subjects with the right to erasure of their personal data, where a specific condition is met, such as the data no longer being necessary for its initial purpose, or the data subject withdrawing their consent.

Unlike the GDPR, the NDPR does not provide exceptions to the right to erasure. In addition, while the GDPR mandates that certain mechanisms be put in place to comply with this right, the NDPR does not require controllers to establish any such mechanisms.

GDPR	NDPR
Articles 12, 17 Recitals 57, 59, 65-66	Section 3.1

Similarities

The GDPR outlines the right of the data subject to obtain from the controller the **erasure of personal data** concerning him or her without undue delay.

Under the NDPR, the data subject shall have the **right to request** the controller to **delete personal data** without delay.

Under the GDPR, the right to erasure applies when one of the following grounds are met:

- the personal data **is no longer necessary** for the purpose forwhich it was collected;
- the **consent of the data subject is withdrawn** and there is **no other legal ground for processing**;
- the data subject **objects to the processing and there are no overriding legitimate grounds for the processing**; and
- the personal data has been **unlawfully processed**;or
- the personal data has to be erased in compliance with a **legal obligation in EU or Member State law**.

Under the NDPR, the right to erasure applies when one of the following grounds are met:

- the personal data is **no longer necessary**;
- the data subject **withdraws consent** on which the processing is based;
- the data subject **objects to the processing** and there are **no overriding legitimate grounds** for the processing;
- the personal data has been **unlawfully processed**; or
- the personal data must be erased for **compliance with a legal obligation** in Nigeria.

Data subjects **must be informed** that they have the right to request for their data to be deleted.

Data subjects **must be informed** of the existence of the right to request from the controller erasure of their personal data.

The right to erasure can be exercised **free of charge**. There may be some instances, however, where a fee may be requested, notably when requests are **unfounded, excessive, or have a repetitive character**.

The right can be exercised **free of charge**. However, if the request is **manifestly unfounded or excessive**, the controller may charge a **reasonable fee considering the administrative costs** of taking the action.

A request can be made in **writing, orally, and through other means including electronic means** where appropriate.

The information shall be provided in **writing, orally, or by other means**, including, where appropriate, by **electronic means**.

GDPR	NDPR

Similarities (cont'd)

If the data controller has made personal data public and is obliged to erase the personal data, the data controller, taking into account the available technology and the cost of implementation, must take reasonable steps, including **technical measures**, to **inform controllers** processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	The data controller who has made the personal data public and is therefore obliged to delete the personal data, must take all reasonable steps to **inform controllers** processing the personal data of the data subject's request.

Differences

Under the GDPR, the right to erasure also applies where the personal data has been collected **in relation to the offer of information society services**.	The NDPR **does not** provide the right to erasure when personal data has been collected in relation to the offer of information society services.
Exceptions to the right of erasure provided by the GDPR include: • **freedom of expression** and freedom of information; • complying with **public interest purposes in the area of public health**; • establishment, exercise, or defence of **legal claims**; and • **complying with legal obligations** for a public interest purpose.	The NDPR **does not** provide exceptions to the right of erasure.
The **deadline** for responding to erasure requests can be extended by **two additional months**, taking into account the complexity and number of requests. In any case, the data subject must be informed of such an extension within one month from the receipt of the request.	The NDPR **does not** provide for an **extension** to the deadline for erasure requests under any circumstances.
A data controller must have **mechanisms** in place to ensure that the request is made by the data subject whose personal data is to be deleted.	The NDPR **does not require** a data controller to have **mechanisms** in place to ensure that the request is made by the data subject whose personal data is to be deleted.

5.2. Right to be informed

The GDPR and the NDPR require that data subjects are informed of the legal basis and scope of processing of their personal data as well as data subject rights. Information can be provided to data subjects orally, in written form or by electronic means. In addition, data subjects must be informed of the possible consequences of a failure to provide personal data, whether in complying with statutory or contractual requirements, or a requirement necessary to enter into a contract.

According to both laws, a data controller cannot collect and process personal data for purposes other than those which the data subjects were originally informed of, unless further information is provided. In addition, special information must be provided regarding the existence of automated decision-making, including profiling, at the time when personal data is obtained.

Whereas the GDPR details that in the case of indirect collection of personal data, a data controller must provide information relating to such collection to data subjects within a reasonable period after obtaining the data, the NDPR does not reference such a timeframe.

GDPR	NDPR
Articles 5-14, 47 Recitals 58-63	Sections 2.3(2)(c), 2.5, 2.12(a), 3.1

Similarities

The GDPR states that data subjects must be provided with information relating to the processing of personal data in order to validate their consent, including:

- **details of personal data** to be processed;
- **purposes** of processing, including the legal basis for processing;
- **data subjects' rights**;
- the **data subject's obligation to provide personal data**, the legal basis and the possible consequences of failure to provide such data; and
- the **period** for which the personal **data will be stored**;
- the **existence of automated decision-making**, including profiling, and meaningful information about the logic involved, as well as the **significance and the envisaged consequences** for the data subject;
- **recipients or their categories** of personal data; and
- **contact details** of the data controller or its representative and the DPO.

The NDPR states that data subjects must be provided with information about the collection or processing of their personal data, including:

- the **legal basis and purposes** of the processing of personal data as well as the **legitimate interests** pursued;
- the **recipients or categories of recipients of the personal data**;
- the **period** for which the personal **data will be stored**;
- **data subjects' rights** (e.g. the right to erasure, right to object, right of withdrawal, right to lodge a complaint to a relevant authority, etc.);
- the **data subject's obligation to provide personal data**, the legal basis and the possible consequences of failure to provide such data; and
- the **existence of automated decision-making**, including profiling, and meaningful information about the logic involved, as well as the **significance and the envisaged consequences** for the data subject.
- **contact details** of the data controller or its representative and the DPO.

Information must be provided to data subjects in an easily accessible form with clear and plain language, which can be in **writing or other means such as in electronic format**.

Information must be provided in a **concise and easily accessible form, using clear and plain language**, especially when **children** are concerned. The information shall be provided

GDPR	NDPR

Similarities (cont'd)

GDPR	NDPR
In addition, where data is obtained directly, information relating to processing, such as the purpose of the processing, and the rights of data subjects, must be provided to data subjects **at the time when personal data is obtained**.	in writing including, where appropriate, by electronic means and upon oral request from the data subject. Privacy policies must be drafted in a way that the **class of data subjects targeted can understand it**. In addition, information relating to personal data processing, such as the purpose of the processing, and the rights of data subjects, must be provided to data subjects by the data controller **prior to the collection of data**.
A data controller must **inform** data subjects of the existence or absence of an adequacy decision, or reference the **appropriate or suitable safeguards** and the means by which to obtain a copy of them or where they have been made available.	A data controller must **inform** data subjects of the intention to **transfer personal data to a third country** or international organisation and the existence or **absence of an adequacy decision, potential risks and appropriate safeguards**.
The GDPR provides specific information that must be given to data subjects when their personal data has been **collected from a third party**, which includes the sources from which the data was collected.	The NDPR requires the data subject to be provided with information about **third-party access** to their personal data and the **purpose** for such access.
Information provided to data subjects must be provided **free of charge**. If requests are manifestly unfounded or excessive a reasonable administrative fee may be requested.	Information provided to data subjects must be provided **free of charge**. If requests are manifestly unfounded or excessive a reasonable administrative fee may be requested.

Differences

GDPR	NDPR
If personal data is not obtained from the data subject, a data subject must be provided information within a reasonable period of time, but at the latest within one month, or **at the time of the first communication with the data subject, or when personal data is first disclosed to the recipient**.	The NDPR does not refer to the indirect collection of personal data. However, it states that where the controller intends to further process personal data for a **purpose other than that for which the personal data were collected**, the controller shall provide the data subject, prior to that further processing, information on that other purpose, and with any relevant further information.

5.3. Right to object

Fairly consistent

The GDPR and the NDPR guarantee data subjects the right to ask organisations to cease the processing and sale of their personal data. Under both the NDPR and the GDPR, the right to object to direct marketing is an absolute right. However, the GDPR provides that the right to object may apply in several additional processing activities. The NDPR and the GDPR also recognise data subjects' right to restrict processing and include an exception for where the controller demonstrates compelling legitimate grounds for the processing that overrides the rights and interests of the data subject. However, the timeframe to respond to the objection to the processing of data differs slightly. While the NDPR requires the deletion of data without undue delay, the GDPR explicitly provides for a timeframe of one month, with the possibility for an extension of two months.

GDPR	NDPR
Articles 7, 12, 18, 21	Sections 2.3(2)(c), 2.8, 3.1(7)(h), 7(i), 9(c), 11

Similarities

GDPR	NDPR
Data subjects have the right to **withdraw** their **consent** to the processing of their personal data **at any time**.	Data subjects have the right to **withdraw** their **consent** to the processing of their personal data **at any time**.
Under the GDPR, data subjects must be provided with **modalities to exercise the right to object, free of charge**.	Under the NDPR, data subjects must be explicitly and manifestly provided with a **mechanism to object** to any form of data processing, **free of charge**.
Under the GDPR, data subjects are provided with the **right to object** to the processing of personal data for **direct marketing purposes**.	Data subjects have the **right to object** to the processing of their personal data for **marketing purposes**.
The data subject has the **right to be informed** about the right to object.	Prior to the processing of personal data, the data subject must be **informed** of their **right to object** to the processing of their data as well as of the right to the **restriction of processing** concerning the data subject.
Upon the receipt of an objection request, a data controller shall **no longer process** the personal data unless: • the processing is based on a legitimate ground that overrides the data subjects' interests; or • it is for the establishment, exercise, or defence of a legal claim.	Upon the receipt of an objection request, the controller **must delete** the personal data unless there are **overriding legitimate reasons** for the processing such as: • the **exercise or defence of legal claims**; • for the protection of **the rights of another natural or legal person**; or; or • for reasons of important **public interest** in Nigeria.

GDPR	NDPR

Similarities (cont'd)

The data subject shall have the **right to** obtain from the controller **restriction** of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to processing pending the verification of whether the legitimate grounds of the controller override those of the data subject.

Furthermore, the data subject has the **right to** obtain from the data controller **restriction** of processing if:

- the accuracy of the personal data is contested by the data subject for a period enabling the data controller to verify the accuracy of the personal data;
- the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to processing, pending the verification of whether the legitimate grounds of the data controller override those of the data subject.

Differences

A request to restrict the processing of personal data must be responded to without undue delay and in any event within **one month** from the receipt of request. The deadline can be extended by **two additional months** taking into account the complexity and number of requests.

If the data subject objects to the processing of their data and there are no overriding legitimate grounds, the controller must delete the personal data **without delay**.

Under the GDPR, data subjects have the right to object to the processing of data in the following circumstances:

- if the processing of personal data is due to **tasks carried out in the public interest** or **based on a legitimate interest pursued by the data controller** or **third party**; or
- if the processing of personal data is for **scientific, historical research or statistical purposes**.

The NDPR does not specify that data subject have the right to object in such circumstances.

5.4. Right to access

Fairly consistent

The NDPR and GPDR both contain provisions regarding the data subject's right to access and the data controller's response to the same. The NDPR differs in its details on the format and content of the response.

GDPR	NDPR
Article 15 Recitals 59-64	Sections 1.3(ev), 3.1, 4.1(5)

Similarities

The GDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

The NDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

The GDPR specifies that a data controller must **have in place mechanisms** to **identify** that a request is made by a **data subject** whose **personal data is to be deleted**.

Under the NDPR, where the data controller has reasonable doubts concerning **the identity of the individual** making the request, the controller may **request the provision of additional information** for the purposes of **identification**.

Under the GDPR, a data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character**.

Under the NDPR, a data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character.**

The right to access can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are **unfounded, excessive, or have a repetitive character**.

Except as otherwise provided by any public policy or the NDPR, or if the requests are **unfounded, excessive, or have a repetitive character**, information provided to the data subject and any communication and actions taken will be **provided free of charge**.

Data subjects' requests under this right must be replied to **without 'undue delay** and in any event **within one month** from the receipt of a request.'

Under the NDPR, if the data controller does not act on the data subject request, the controller must inform the data subject **without undue delay** and at latest **within one month** of receipt of the request, of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority.

Differences

The GDPR specifies that, **when responding to an access request**, the data controller must indicate the following information:

- the **purposes** of the processing;
- the **categories** of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be **disclosed**, in particular, recipients in third countries or international organisations;

The NDPR **does not specify requirements** for the information to be included in the **response to data subject access requests**. However, the NDPR indicates that the data controller must take **appropriate measures** to provide any information relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form**, using clear and plain language, and for any information relating to a child. Information must be provided in **writing**,

GDPR	NDPR
Differences (cont'd)	
• where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period; • the existence of the right to request from the controller **rectification or erasure** of personal data or restriction of processing of personal data concerning the data subject or the right to object to such processing; • the right to lodge a **complaint** with a supervisory authority; • where the personal data are not collected from the data subject, any available information as to their **source**; and • the existence of **automated decision-making**, including profiling.	or by other means, including, where appropriate, by **electronic means**. When requested by the data subject, the information may be provided **orally**, provided that the identity of the data subject is proven by other means.
The GDPR provides that the right of access must not **adversely affect the rights** or freedoms of others, including those related to trade secrets.	The NDPR does not expressly state that the right of access must not adversely affect the rights or freedoms of others. However, under the NDPR, the exercise of data subject rights must conform with constitutionally guaranteed principles of law for the general protection and enforcement of fundamental rights.
The deadline for responding to data subjects' requests can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such an extension within one month from the receipt of a request.	The **deadline** for responding to data subjects' access requests **cannot be extended**.
Data subjects must have a variety of means through which they can make their request, including **orally and through electronic means**. In addition, when a request is made through electronic means, a data controller should submit a response through the same means.	The NDPR does not address the means by which data subjects can make their requests.

5.5. Right not to be subject to automated decision-making

Neither the GDPR nor the NDPR explicitly address the right not to be subject to discrimination. However, some provisions based on this principle can be found in both laws.

GDPR Articles 5, 13	NDPR Sections 2.1(1)(b), 3.1(3)(l)

Similarities

The GDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.

The NDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.

Although the GDPR does not include a specific provision stating that a data subject must not be discriminated against on the basis of their choices on how to exercise their data protection rights, it is implicit from the principles of the GDPR that individuals must be protected from discriminatory consequences derived from the processing of their personal data. For example, Article 5 states that personal data must be processed '**fairly**'.

Although the NDPR does not include a specific provision stating that a data subject must not be discriminated against on the basis of their choices on how to exercise their data protection rights, it is implicit from the principles of the NDPR that individuals must be protected from discriminatory consequences derived from the processing of their personal data. For instance, Section 2.1(1)(b) states that personal data must be processed '**without prejudice to the dignity of human person**.

Furthermore, Article 13 of the GDPR states that data subjects must be informed of the consequences derived from automated decision-making.

Similarly, Section 3.1(3)(l) of the NDPR states that the controller shall inform the data subject about the existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Differences

The GDPR specifies that individuals have the right not to be subject to automated decision-making that has a legal or significant effect upon them.

The NDPR does not provide for a specific right not to be subject to automated decision-making.

5.6. Right to data portability

Fairly consistent

Both the GDPR and the NDPR recognise the right to data portability, however, the two laws define the right to data portability differently.

GDPR	NDPR
Articles 12, 20, 28 Recitals 68, 73	Sections 1.3xii, 3.1(7)(h), 3.1(15)

Similarities

The GDPR provides individuals with the **right to data portability.**

The NDPR provides individuals with the **right to data portability**.

Differences

The GDPR defines the right to data portability as the **right to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller **without hindrance**.

The NDPR defines data portability as the ability for data to be **transferred easily from one IT system or computer to another** through a **safe and secured means** in a **standard format**. In addition, when exercising the right to data portability, the data subject has the **right to have personal data transmitted directly from one controller to another, where technically feasible**, provided that this right does not apply to processing necessary for the performance of a task carried out in the **public interest** or in the **exercise of official authority vested in the data controller**.

6. Enforcement

6.1. Monetary penalties

Both the GDPR and the NDPR provide for monetary penalties to be issued in cases of non-compliance. However, unlike the GDPR, the NDPR does not provide specific requirements that NITDA must consider before issuing a fine.

In addition, the amounts of the monetary penalties differ significantly between the NDPR and the GDPR.

GDPR	NDPR
Articles 83, 84 Recitals 148-149	Section 2.10

Similarities

The GDPR provides for the possibility of administrative, **monetary penalties** to be issued by the supervisory authorities in cases of non-compliance.

The NDPR provides for the possibility of **monetary penalties** to be issued by the supervisory authority in cases of non-compliance.

Differences

Depending on the violation, the penalty may be up to either: **2% of global annual turnover or €10 million**, whichever is higher; or **4% of global annual turnover or €20 million**, whichever is higher.

The NDPR outlines that depending on the violation, a penalty may be up to either: **2% of annual gross revenue** of the preceding year or payment of the sum of **NGN 10 million (approx. €25,000)**, whichever is greater where the data controller is dealing with more than 10,000 data subjects; or payment of a fine of **1% of the annual gross revenue** of the preceding year or payment of the sum of **NGN 2 million (approx. €5,000)** whichever is greater where the data controller is dealing with fewer than 10,000 data subjects.

When applying an administrative sanction, the supervisory authority must consider:

- the **nature, gravity and duration** of the infringement;
- the **intentional or negligent character** of the infringement;
- any action taken to **mitigate** the damage;
- the **degree of responsibility** of the controller or processor;
- any relevant **previous infringements**;
- the degree of **cooperation with the supervisory authority**
- the **categories of personal data** affected by the infringement;
- the manner in which the infringement **became known** to the supervisory authority;
- where measures referred to in Article 58(2) have **previously been ordered** against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

The NDPR **does not** explicitly outline what NITDA must consider when applying an administrative sanction.

GDPR	NDPR
Differences (cont'd)	
• adherence to **approved codes of conduct or approved certification mechanisms**; and • any other **aggravating or mitigating factor** applicable to the circumstances of the case.	
Supervisory authorities may develop **guidelines** that establish **further criteria** to calculate the amount of the monetary penalty.	The NDPR **does not** provide a similar provision.

6.2. Supervisory authority

Fairly inconsistent

The NDPR and the GDPR differ in their provisions regarding the responsibilities of supervisory authorities.

Whereas the GDPR's approach designates specific investigatory and corrective powers for Member States, the NDPR focuses on the powers of the issuing body of the NDPR, NITDA, of the HAGF, and the Administrative Redress Panel. The NDPR assigns NITDA, the HAGF, and the Administrative Redress Panel with different responsibilities regarding the supervision of data protection activities and enforcement of provisions of the NDPR.

Rather than specifying supervisory authorities of Member States like the GDPR, the NDPR defines 'relevant authorities' as NITDA or 'any other statutory body or establishment having government's mandate to deal solely or partly with matters relating to personal data.'

GDPR	NDPR
Articles 50-84 Recitals 117-140	Sections 1.3, 2.11-2.12, 4.1(4), 4.2, 4.3

Similarities

Under the GDPR, supervisory authorities are given specific **investigatory powers** which include:

- ordering a controller and processor to provide any information required;
- conducting data protection audits;
- carrying out a review of certifications issued; and
- obtaining access to all personal data and to any premises.

The NDPR does not specifically refer to such **investigatory powers**. However, under its NDPR mandate, NITDA inaugurated the **Administrative Redress Panel** in October 2019, which will:

- **investigate alleged breaches** of the NDPR;
- **invite parties to respond to allegations** within seven days;
- **issue administrative orders** to protect the subject matter of the allegation pending the outcome of investigation; and
- **conclude investigations** and determinations of **appropriate redress within 28 working days**.

Furthermore, NITDA registers and licenses **Data Protection Compliance Organisations** who act on behalf of NITDA, to monitor, audit and conduct training and data protection compliance consulting with all concerned data controllers.

The GDPR provides **mechanisms for international cooperation** between supervisory authorities. In particular, n relation to third countries and international organisations, Article 50 of the GDPR provides that, the Commission and supervisory authorities shall take appropriate steps to:

- develop **international cooperation mechanisms** to facilitate the effective enforcement of legislation for the protection of personal data;
- provide international **mutual assistance** in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to

The NDPR also provides **mechanisms for international cooperation** between NITDA and other supervisory authorities. In particular, in relation to foreign countries and international organisations, Article 4.3 of the NDPR states that NITDA and relevant authorities shall take appropriate steps to:

"a) Develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

b) Provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject

GDPR	NDPR

Similarities (cont'd)

appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; • **engage relevant stakeholders** in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; • **promote the exchange** and documentation of personal **data protection legislation and practice**, including on jurisdictional conflicts with third countries.	appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; c) Engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and d) Promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries."

Differences

Under the GDPR, it is left to each Member State to **establish a supervisory authority**, and to determine the qualifications required to be a member, and the obligations related to the work, such as duration of term as well as conditions for reappointment.	Under the NDPR, the relevant supervisory authorities are **NITDA or any other statutory body or establishment having mandate to deal solely or partly with matters relating to personal data**. In particular, the **Administrative Redress Panel** inaugurated by NITDA under the NDPR is granted the **investigatory powers** outlined above. In addition, under the NDPR, **the HAGF** is given mandate to **supervise any transfer of personal data** which is undergoing processing or is intended for processing after transfer to a foreign country or to an international organisation.
Supervisory authorities **may be subject to financial control only if it does not affect its independence**. They have separate, public annual budgets, which may be part of the overall national budget.	The NDPR **does not address the budget or financing** for NITDA.
Under the GDPR, supervisory authorities have c**orrective powers** which include: (i) issuing warnings and reprimands; (ii) imposing a temporary or definitive limitation including a ban on processing; (iii) ordering the rectification or erasure of personal data; and (iv) imposing administrative fines.	The NDPR does not specifically refer to NITDA's **corrective powers**. However, it does provide for administrative fines in cases of violation of its provisions (see section 6.1).

6.3. Civil remedies for individuals, including other remedies

Both the NDPR and the GDPR provide the right for a data subject to lodge a complaint with the supervisory authority.

However, unlike the GDPR, the NDPR does not explicitly provide for individuals with a cause of action to seek compensation from a data controller or a data processor for a violation of its provisions.

GDPR	NDPR
Articles 79, 80, 82 Recitals 131, 146-147, 149	Sections 2.4, 3.1(2)

Similarities

GDPR	NDPR
Under the GDPR, the data subject has the right to **lodge a complaint** with the supervisory authority.	Under the NDPR, the data subject has the right to **lodge a complaint** with NITDA.

Differences

GDPR	NDPR
The GDPR provides individuals with a cause of action to **seek compensation** from a data controller or data processor for a violation of the GDPR.	The NDPR **does not** explicitly provide for individuals to seek compensation from a data controller or data processor for a violation of the NDPR.
The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to **a not-for-profit body, association, or organisation** that has, as its statutory objective, the protection of data subject rights.	The NDPR **does not** provide for such a right.
The supervisory authority must inform the data subject of the progress and outcome of his or her complaint.	The NDPR **does not explicitly** outline that the NITDA inform the data subject of the progress and outcome of his or her complaint.
The GDPR provides that a data controller or processor shall be **exempt from liability to provide compensation** if it proves that it is not in any way responsible for the event giving rise to the damage.	The NDPR **does not** explicitly provide that a data controller or processer be exempt from liability if it proves it is not in any way responsible. In addition, the NDPR outlines that **every data controller** will be **liable** for the **actions or inactions of third parties** who handle the personal data of data subjects.