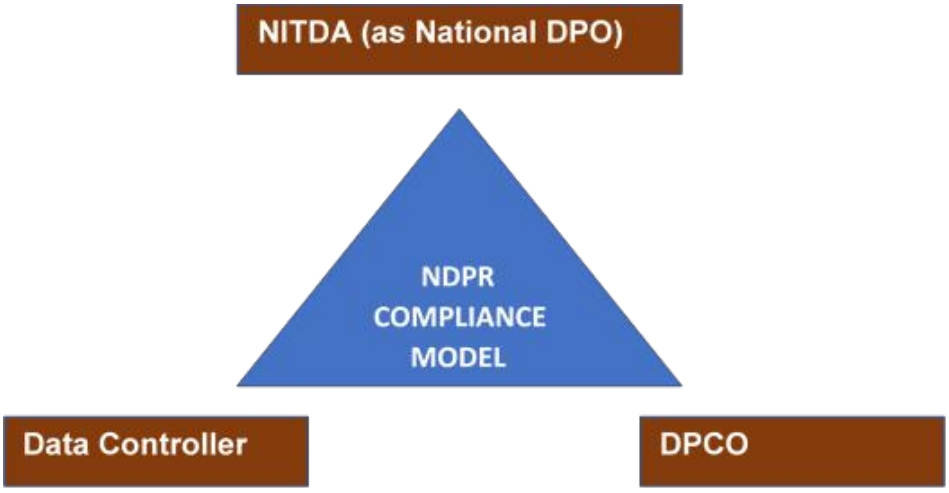
NDPR - A Guide to Compliance

Understanding the Data Protection Law in Nigeria

Introduction

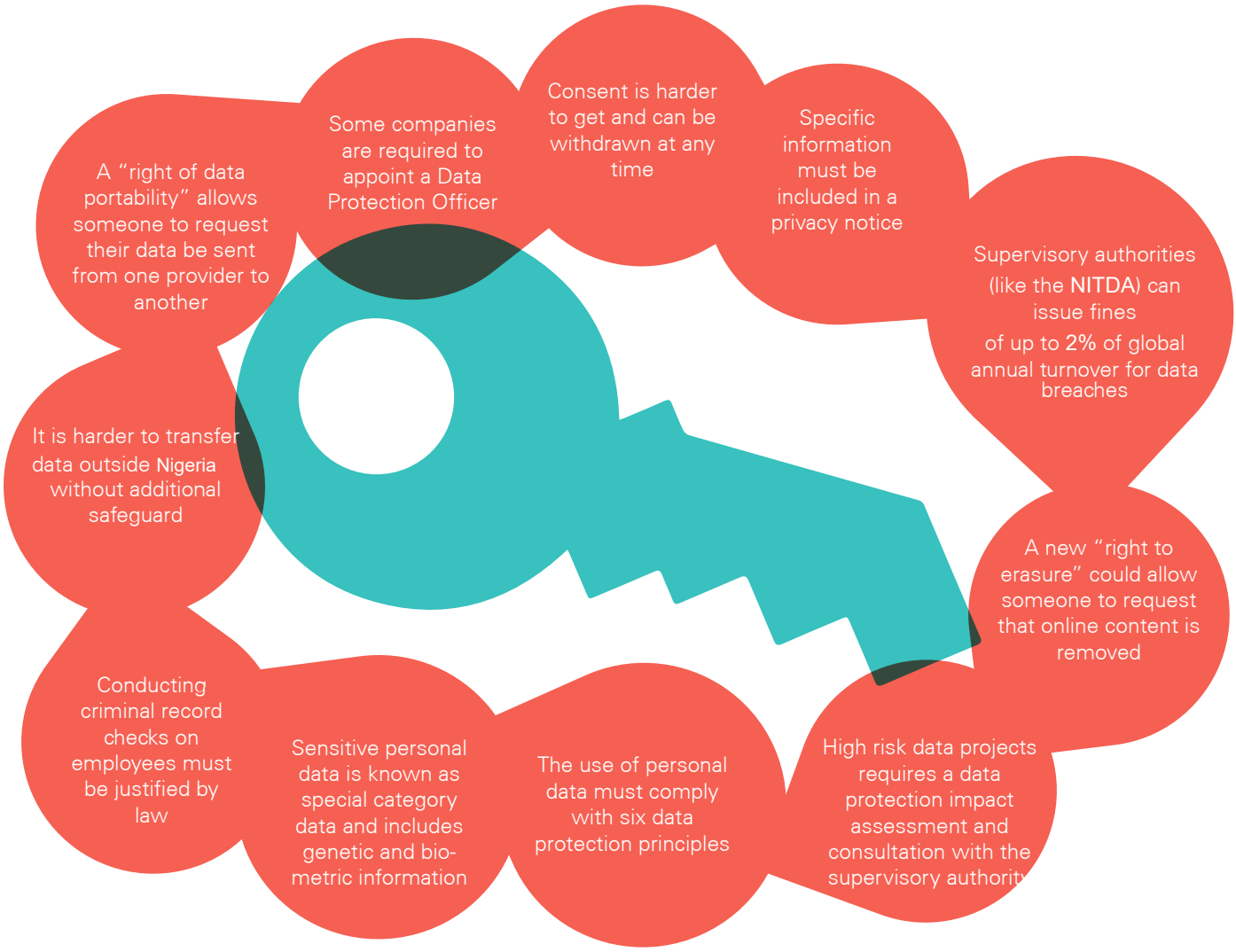
The The Nigerian Data Protection Regulation (NDPR) officially came into force in January 2019. This Regulation addresses Data Privacy and Protection in Nigeria and solely applies to all transactions intended for the processing of personal data and to actual processing of personal data belonging to natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent. Businesses are required to appoint a representative, generally referred to as a Data Protection Officer (DPO), who will be accountable for compliance with the data protection regulations within their organisation.



The approach adopted with the Nigeria Data Protection Regulation (NDPR) considers the Nigerian context and seeks to be implemented with a non-obstructive, compliance promoting approach. The NDPR uses a triangular compliance model as shown in the graphic above.

NDPR's reach is global. Any company that offers goods or services to anyone in Nigeria will be required to comply.

Summary of NDPR



About people's rights

NDPR represents a fundamental shift in how the use of personal data is regulated. The people who give data, data subjects, own their data and are simply lending it to others for use. Carrying out activities with people's data that could cause them harm, not securely stored, used in a way they would not expect or were not told about, or packaged up and sold for profit, is expressly forbidden by NDPR.

Conditions for processing data

Use of any personal data must be justified using one of the following conditions for processing:

If the data is "special category data", i.e. about a person's race, religion, or health status, there must be an additional justification to process the data which can include explicit consent, employment law, or for medical purposes.

What to do:

- Document which conditions you can rely on for using data
- Ensure that you have additional justification for special category data

Where should these conditions be documented?

It is very important to identify which condition for processing is being relied on. This is the kind of information that is expected to be included in a privacy notice. If relying on consent, the person must be told they can withdraw their consent at any time.

What counts as legitimate interest?

To rely on this condition, you must properly balance the interest of the data controller with the right to privacy for the individual. One way to test if something may count as a legitimate interest is to consider whether the individual would reasonably expect and allow their data to be used in that way.

General data protection principles

In addition to being justified through the **conditions for processing**, using personal data must follow all of the six general principles.

1. **Lawful, fair, and transparent**
   Data collection must be fair, for a legal purpose and be open and transparent about how the data will be used
2. **Limited for its purpose**
   It can only be collected for a specific purpose
3. **Data minimisation**
   Data collected must be necessary and not excessive for its purpose
4. **Accurate**
   It must be accurate and kept up to date
5. **Retention**
   Data should not be stored any longer than necessary
6. **Integrity and confidentiality**
   Data must be kept safe and secure

It is not enough just to comply with all six of these principles; you must be able to show how you comply with them. This means having policies about how personal data is managed and making sure that there is a clear compliance structure, responsibilities are allocated, staff are trained and systems have been audited. It also means bringing in technical measures to improve safety and security, and ensuring individuals can properly access their data. Refresher training should be carried out at least once a year.

What to do:

- Ensure that up to date technical systems are being used
- Make sure company policies on personal data will be updated in reference to the six data protection principles

Consent

NDPR strengthens the level of consent that is required to justify using personal data.

Consent must be **freely given** and **specific**. There must be a **genuine choice**, the person cannot be **coerced** or unduly **incentivised** or **penalised** if consent is refused. If consent is taken as a **condition of subscribing** to a service, then the organisation must demonstrate how consent was freely given.

Will old consent still be valid?

Personal data that has been collected before NDPR comes into force will still be valid only if it meets the requirements of the new Regulation. This could be hard to check and it is likely that new consent will have to be secured, or a different condition relied upon.

Consent can be withdrawn at any time without the person suffering any negative consequences as a result. If this is not the case, then consent is not the right condition.

Not consent:

- A pre-ticked box
- Silence or inactivity
- Complex or technical language
- Tied to a contract
- Bundled with consent for other purposes
- Will be detrimental to the individual if they do not give consent or withdraw it

Consent

- Separate from any other parts of a form or contract
- Specific consent for each activity to be undertaken with the data
- Authorised by a parent for someone under 16 years old
- Explicitly given to process sensitive data as well as personal data

Example:

WRONG

If you do not wish to receive further marketing information from us, please tick "opt-out".

RIGHT

Tick if you would like to receive information about our products and special offers by post ❑ | by email ❑ | by telephone ❑ | by text ❑ | by fax ❑

Consent and criminal record checks

NDPR will make it harder to justify routine criminal background checks. It is not satisfactory to rely on the consent of the individual to process their criminal record, it must instead be authorised by law.

What to do:

- Review the ways you obtain consent and assess whether these will be valid under NDPR. If not, change your procedures.
- Make sure there is a procedure in place for acting on a request to withdraw consent

Marketing

Consent and marketing can be complicated. To prove consent has been given, some firms operate a "double opt-in" model. After initial consent is given, an email is sent to to the individual asking them to click a link to validate that consent.

It will be more difficult to justify automated targeting or profiling of people using their personal information. The reasons for making automated decisions about a person must be explained. For example, targeting adverts for baby products at someone who searches for 'morning sickness' online may be unlawful profiling based on the collection of sensitive personal information.

Often other conditions for processing, such as legitimate interest, can work better for marketing than consent. Marketing similar products of services to customers can be justified under legitimate interest. However email marketing is dying, and many companies are avoiding this entire issue by engaging with their customers directly on social media.

Data subject rights

Data portability

There is a new right called data portability under NDPR. While people already had the right to access their data through a subject access request, now it will have to be provided in a way that makes it easy for a computer to read (e.g. via a spreadsheet). A person can also request for their data to be transferred directly to another system for free. This could mean transferring all of your photos from one social network to another, or content from one cloud provider to another.

Right to erasure

Sometimes referred to as the "right to be forgotten", this is one of the most talked-about innovations of NDPR. Also known as the right to erasure, it means that someone can request the deletion or removal of their personal data, including information published or processed online.

The Regulator is serious about Compliance

The NDPR is being enforced with seriousness by NITDA. Evidence of this is the current investigation of TrueCaller for data privacy breaches and the recent investigation of the Lagos Internal Revenue Service (LIRS) for publishing some Lagos State taxpayers' personal information on its website. Also, judicial decisions are an integral source of law in Nigeria and there have been court decisions on data privacy and protection. In two separate cases brought against MTN Nigeria Ltd and Airtel Nigeria Ltd, the courts held that the unauthorized disclosure of the claimants' mobile phone numbers by their telecommunications service providers (the defendants) and the subsequent unsolicited text messages they received from unknown third parties were violations of their constitutional rights to privacy and both claimants were awarded damages of N5,000,000 (five million naira) each.

What to do: Ensure there are procedures for dealing with data subject rights

Privacy

Privacy notices, or "how we use your information" guides must be given at the point of data collection. The condition for processing must be included in the privacy notice, as well as the person's rights and how they can make a complaint. For instance, if you rely on consent for using their data, you must inform the person of their right to withdraw consent at any time. Organisations must undertake Privacy Impact Assessments when conducting risky or large scale processing of personal data.

Privacy by design

Privacy by design means that each new service or business process that makes use of personal data must take the protection of such data into consideration during the design phase.

Privacy by default

Organisations must ensure that, by default, privacy settings should be set to high. Only personal data that has a purpose should be collected and retained; and only for the minimum time necessary for those purposes. In particular, personal data should not be automatically accessible to anyone on the internet. No manual change to the privacy settings should be required on the part of the user.

What to do:

- Ensure privacy by design and privacy by default procedures are fully implemented
- Ensure privacy notices contain all necessary information and are given at the right time

Data processors and controllers

Some industries and positions, such as payroll or accountancy, generally deal with data collected by third parties. These are known as **data processors**, as opposed to **data controllers** who collect personal information and decide what it is used for. Processors only use data collected from another company.

NDPR applies directly to data processors. There must be a contract in place between a data controller and processor, including specific clauses relating to data protection, and processors may be liable for compensation claims.

If you have contracts with data processors, check if they are compliant with NDPR. Data processing agreements between controllers and processors can either be a separate agreement, or included in standard contracts.

What to do:

- Ensure there are data processing agreements between controllers and processors

Data Protection Officers

Data Protection Officers are responsible for everything related to keeping data secure in the company. They report directly to the highest levels of management and cannot easily be dismissed. DPO's cannot be shareholders, executives or board members. They must act independently. External organisations can also be appointed as DPO.

Data Protection Officer job descriptions

"The DPO should achieve efficient management of information, while optimising its effectiveness and maintaining compliance with global information-related laws and regulations."

The DPO will provide pragmatic and commercially-focused privacy and data protection advice.

A DPO must be appointed when:

- Processing is carried out by a public authority
- Large scale regular and systematic monitoring is the core of the processing activities of the controller
- Sensitive data on a large scale is at the core of the processing activity

What to do: Consider if a DPO must be appointed and keep this under regular review

International data transfers

Transferring data outside Nigeria is subject to strict restrictions under NDPR. Essentially it cannot be done unless there are specific protections put in place.

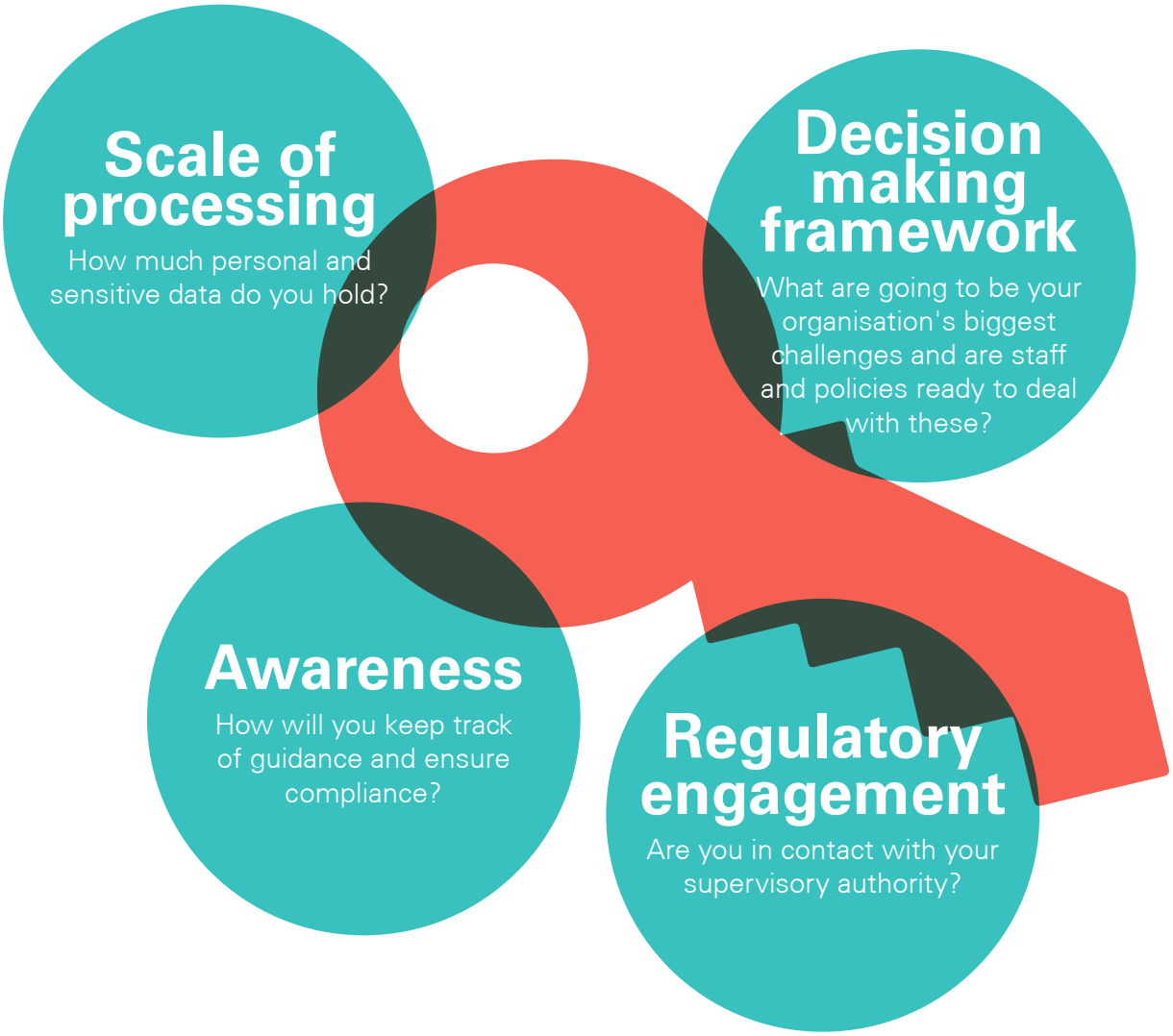
Transferring data

Where data is being transferred outside Nigeria, the following information is required:
1 The List of Countries where Nigerian citizens personally identifiable information are transferred in the regular course of business.
2. The Data Protection laws and contact of National Data Protection Office/Administration of such countries listed in 1 above.
3. The privacy policy of the Data Controller, compliant with the provisions of the NDPR.
4. Overview of encryption method and data security standard
5. Any other detail that assures the privacy of personal data is adequately protected in the target country.

What to do: Consider how NDPR may impact on any international data transfers you carry out

Managing risk

It is recommended that organisations carry out an audit of all the data they hold around once a year. This should include reviewing how the data is processed and stored. Some key things to consider:



Auditing the information you hold and compiling a data register including what data you do hold, where it is stored, how it is used and by whom, can be a helpful tool.

What to do:

- Think about how you manage risk and how data protection is dealt with in your risk assessment framework
- Consider a data audit and data register

Breaches and sanctions

NDPR has a strict sanctions regime. **Supervisory authorities** can fine a company up to 2% of annual worldwide turnover, or N10m, whichever is greater. Sanctions can also include audits, warnings, and temporary or permanent bans from processing data.

Reportable

The loss of an unencrypted laptop or digital media with the names, addresses, and dates of birth of people.

Not reportable

The loss of a marketing list with names and addresses where there is no particular sensitivity of the data.

Even if small amounts of sensitive data are at risk, such as health records, there should be a presumption to report. Consider if the release of such data could cause significant risk of individuals suffering substantial detriment or distress.

Breaches are not made public. However if regulatory action is taken, such as a fine or warning, then this could be made public.

How do I demonstrate compliance?

1 Review and, when necessary, update company policies that deal with how personal data is collected, handled and stored.

2 Document a clear compliance structure that includes: allocation of staff responsibility, auditing of current practices, and crucially, training for all relevant staff.

What to do: Ensure all staff are adequately trained on NDPR for their specific job role and re-train at least once per year.

NDPR compliance checklist

- Review the ways you obtain consent and assess if these will be valid under NDPR. If not, change your procedures.
- Check if you collect any genetic or biometric information and implement procedures for protecting sensitive personal data.
- Make sure company policies on personal data have been updated to comply with the six data protection principles.
- Ensure there are procedures for dealing with data portability and right to be forgotten requests.
- Review and update your privacy notices.
- Think about setting up a central data breach management register.
- Consider how NDPR impacts on any international data transfers you carry out.
- Consider how you manage risk and how data protection is dealt with in your risk assessment framework.
- Consider what alternative conditions you can rely on for using personal data.
- Make sure there is a procedure in place for acting on a request to withdraw consent.
- Consider privacy by design and privacy by default in new and existing applications.
- Consider the role of your Data Protection Officer, whether they have sufficient budget and authority. If you do not have a DPO, consider whether to appoint one.
- Review any current or future contracts with data processors.
- Understand where your main establishment is and who your lead supervisory authority will be.
- Think about a data audit and data register for your organisation.
- Ensure staff train on NDPR at least once a year.

Our Data Privacy Services

Consulting Services

- ☐ NDPR readiness assessment
- ☐ Privacy risk and impact assessment
- ☐ Data classification and retention policy definition
- ☐ Privacy and data protection awareness training

Audit Services

- ☐ Project initiation and Scoping
- ☐ Project planning and Execution
- ☐ Compliance reporting and filing at NITDA
- ☐ Ongoing Data Protection Compliance Management

Compliance Support

- ☐ Drafting of policies and procedure documents
- ☐ Gap analysis and data protection impact assessments
- ☐ Data Breach Remediation and Support
- ☐ Continuous Staff Training & Capacity Development

Tros Technologies Ltd

W: www.trostechnologies.com

E: hello@trostechnologies.com

T: +234 (0)818 775 7792 +234 (0)1 229 3005