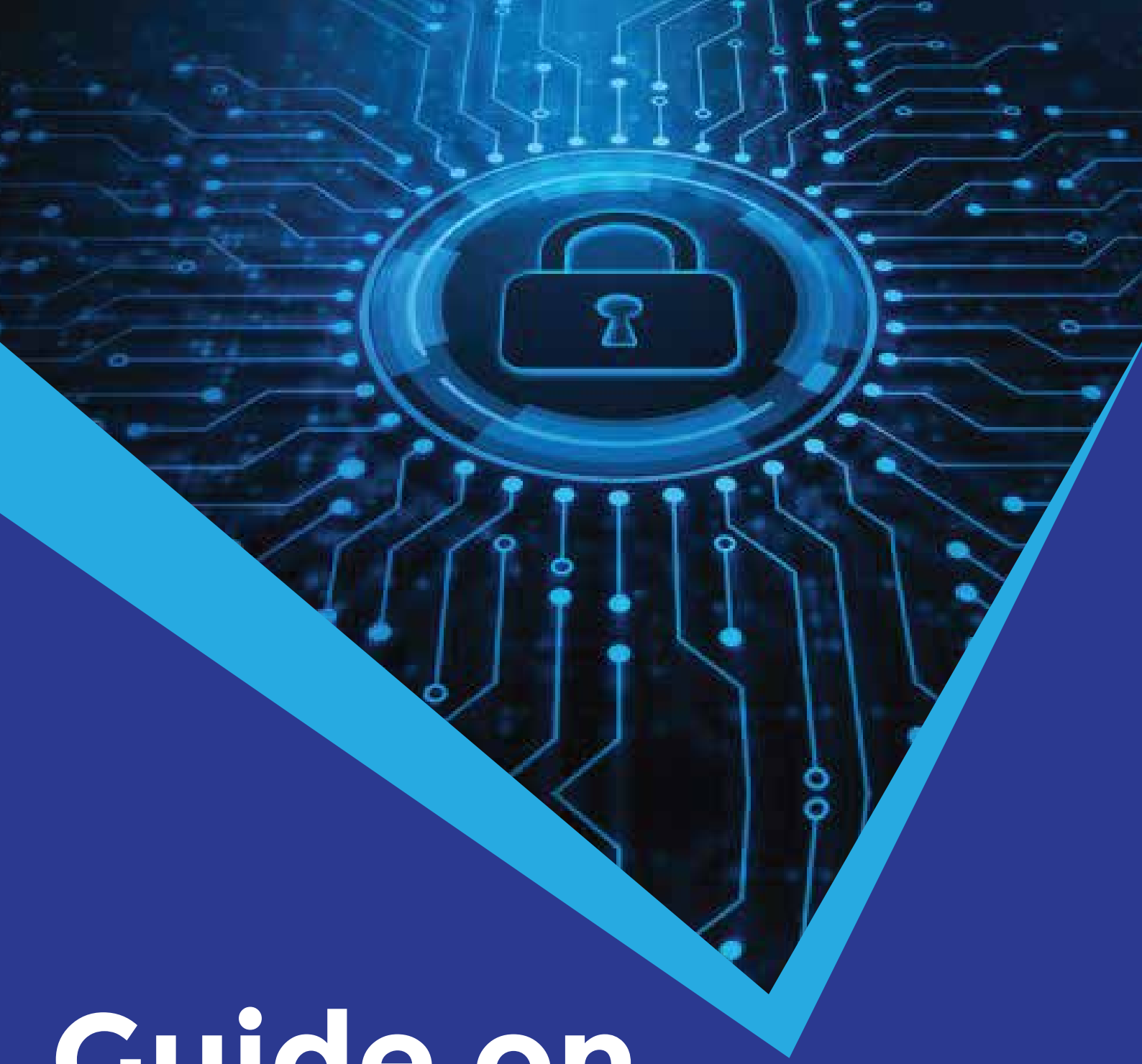

Guide on Data Protection for Nonprofits

Nigeria Network of NGOs

nnngo.org

nnngo

Introduction

Civil society organisations collects a lot of personal data such as names, addresses, emails, telephone numbers, website addresses, social media handles and posts. These data are mostly collected from beneficiaries, staff, volunteers, donors, vendors, board and individuals who are only interested in receiving information (newsletters) about what your organisation does.

In developing the Nigeria Data Protection Regulation (NDPR), it is clear that the regulators were not thinking about nonprofits, their primary target seem to be companies in the business of collecting data however a further analysis of the broad scope of the rules capture almost any organisation who touches or processes data.

When linked with the European Union General Data Protection Regulation (GDPR) which by extension have implications for the work of nonprofits. The GDPR defines personal data as "any information relating to an identified or identifiable natural person". It applies to any organisation that collects the data of EU residents, irrespective of whether payment is required.

As soon as the personal data of an EU resident is collected, it triggers the GDPR and the associated fines for non-compliance regardless of a company's location. For example, if an EU resident signed up for your newsletter because they were interested in your research, course or programs and you send them information material, then the GDPR applies to you.

Civil society data protection is essential. Clearly, organisations within this space must comply with data protection policies either with the NDPR or the EU-GDPR. Anecdotal evidence suggests that very few civil society organisations are aware of the impact of NDPR or GDPR to their operations.

As already noted, civil society organisations were not the targets of regulators(NITDA OR EU regulators) and it could take some time for NDPR which was issued in 2019 to establish the regulatory mechanism to enforce the policy, nonprofits especially those critical of government could be a target of implementation if and when this is done.

Board and management of nonprofits must work together to review and raise organisational awareness on data protection , what data the organisation collects, where they are stored and how to protect them including seeking informed consent for various use of data collected and processed.

In essence, civil society organisations must approach data collection with care while ensuring that anyone visiting their organisation's website, attending their events or doing I business with them regardless of where they come from will be protected as required by the NDPR or GDPR.

Reference: Report on enhancing the digital rights of nonprofits in Nigeria. This report was developed to help civil society organisations understand their digital rights and interpret the pros and cons of artificial intelligence (AI), Machine Learning (ML) and big data within the civic space. https://nnngo.org/enhancing-the-digital-rights-of-nonprofits-in-nigeria/

This Guide is for Nonprofit Organisations who have day to day Responsibility for Data Protection.

It also covers the Nigeria Data Protection Regulation 2019 as it applies in Nigeria.

This guide is divided into 2 sections:

1. **Scope and key definitions**
This section describes some basic concepts, scope of the regulation and key definitions as explained by the NDPR 2019

2. **Data Protection Officers**
This section explains how data protection officers are appointed and their duties/tasks

Section One

What is data protection?
Data protection is about ensuring people can trust you to use their data fairly and responsibly. It also means the fair and proper use of information about people. It's part of the fundamental right to privacy but on a more practical level, data protection is really about building trust between people and organisations.

Does it apply to nonprofits?
Yes, if as a nonprofit organisation you collect personal data such as names, addresses, emails, telephone numbers, website addresses, social media handles and posts; this data protection guide applies to your organisation.

1. Some basic concepts at a glance

- Personal information collected about individuals or beneficiaries would only be used for the purpose for which it was collected.

- Beneficiaries and individuals have the right to review, amend, correct, supplement and delete personal information provided to nonprofit organisations.

- Nonprofits must be committed to monitoring, maintaining and improving the quality of their organisation's database and the services rendered to beneficiaries.

- Personal information collected must be protected from misuse, interference, loss and kept in utmost confidentiality.

- Nonprofits must take reasonable and appropriate security measures to protect personal data collected (such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption).

- The National Information Technology Development Agency(NITDA) regulates data protection in Nigeria with the promulgation of the Nigeria Data Protection Regulation which offers advice and guidance, promote good ICT practice, ensure that organisation carry out a detailed audit of its privacy and data protection practices.

- According to the NDPR a data controller/processor means a legal entity (companies, organisations, government agencies excluding law enforcement agencies) who either alone, jointly with others or in common with others or as a statutory body determines the purpose to which data is processed or is to be processed.

- A data controller or processor shall ensure continuous capacity building for DPOs and the generality of her personnel involved in any form of data processing.

- The NDPR mandates data controllers to file an annual audit report.

- The NITDA is saddled with the responsibility to register and license Data Protection Compliance Organisations (DPCOs) who shall on behalf of the Agency monitor, audit, conduct training and data protection compliance with all data controllers.

- Data protection audit must be conducted: it must include how nonprofit organisations collect personal information, use of personal information, access to and correction of personal information, data quality, how personal data is protected, storage/data security and how beneficiaries can make complaints in cases of bridge.

- The audit report shall be accompanied with a requisite payment to be submitted through a Data Protection Compliance Organisation (DPCO) to NITDA.

- Fee for filing of report of less than 5,000 data subjects cost #10,000 while more than 5,000 data subjects cost #20,000.

- A data controller who processes more than 1000 personal data in a period of six months shall submit an audited data protection document to the NITDA.

- While a data controller who processes more than 2000 personal data in a period of 12 months shall not later than 15th of March of the following year submit an audited data protection document.

2. Scope

- The Nigeria Data Protection Regulation applies to all transactions intended for the processing of personal data, notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria

- The Regulation applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria.

- The Regulation shall not operate to deny any Nigerian or any natural person the privacy rights he/she is entitled to under any law, regulation, policy, contract for the time being in force in Nigeria or in any foreign jurisdiction.

3. Key Definitions

- **Data protection** means the fair and proper use of information about people. It's part of the fundamental right to privacy but on a more practical level, it's really about building trust between people and organisations.

- **Computer** means Information Technology systems and devices, networked or not

- **Consent of the Data Subject** means any freely given, specific, informed and unambiguous indication of the Data subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- **Data** means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.

- **Database** means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type databases.

- **A Data Administrator** means a person or an organisation that processes data.

- **A Data Controller** means 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.

- **Database Management System** means a software that allows a computer to create a database; add, change or delete data in the database; allows data in the database to be processed, sorted or retrieved.

- **Data Portability** means 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.

- **Data Protection Compliance Organisation(DPCO)** means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this regulation or any Foreign Data Protection Law or Regulation having effect in Nigeria.

- **Data Subject** means 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.

- **Data Subject Access Request** means the mechanism for an individual to request a copy of their data under a formal process which may include payment of a fee.

- **Filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

- **Foreign country** means other sovereign states, autonomous or semi-autonomous territories within the international community.

- **Regulation** means this regulation and its subsequent amendments, and where circumstance requires it shall also mean any other regulations on the processing of information relating to identifiable individual's, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, or disclosure.

- **Personal Data** means 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, address, photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier.

- **Personal Identifiable Information (PII)** means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context.

- **Processing** means 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 and dissemination.

  Almost anything you do with data counts as processing; including collecting, recording, storing, using, analyzing, combining, disclosing or deleting it.

- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

- **Recipient** means a natural or legal person, public authority who accepts data.

- **Relevant Authorities** means The National Information Technology Development Agency (NITDA) or any statutory body or establishment having government's mandate to deal solely or partly with matters relating to personal data.

- **Sensitive Personal Data** means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, criminal records or any other sensitive personal information.

- **Third Party** means any natural or legal person, public authority, establishment or any other body other than the data subject, the data controller, the data administrator and the persons who are engaged by the data controller or the data administrator to process personal data.

3. Key Definitions

- **Data protection** means the fair and proper use of information about people. It's part of the fundamental right to privacy but on a more practical level, it's really about building trust between people and organisations.

- **Computer** means Information Technology systems and devices, networked or not

- **Consent of the Data Subject** means any freely given, specific, informed and unambiguous indication of the Data subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- **Data** means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.

- **Database** means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type databases.

- **A Data Administrator** means a person or an organisation that processes data.

- **A Data Controller** means 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.

- **Database Management System** means a software that allows a computer to create a database; add, change or delete data in the database; allows data in the database to be processed, sorted or retrieved.

- **Data Portability** means 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.

- **Data Protection Compliance Organisation(DPCO)** means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this regulation or any Foreign Data Protection Law or Regulation having effect in Nigeria.

- **Data Subject** means 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.

- **Data Subject Access Request** means the mechanism for an individual to request a copy of their data under a formal process which may include payment of a fee

- **Filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

- **Foreign country** means other sovereign states, autonomous or semi-autonomous territories within the international community.

- **Regulation** means this regulation and its subsequent amendments, and where circumstance requires it shall also mean any other regulations on the processing of information relating to identifiable individual's, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, or disclosure.

- **Personal Data** means 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, address, photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier.

- **Personal Identifiable Information (PII)** means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context.

- Processing means 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 and dissemination.

  Almost anything you do with data counts as processing; including collecting, recording, storing, using, analyzing, combining, disclosing or deleting it.

- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

- **Recipient** means a natural or legal person, public authority who accepts data.

- **Relevant Authorities** means The National Information Technology Development Agency (NITDA) or any statutory body or establishment having government's mandate to deal solely or partly with matters relating to personal data.

- **Sensitive Personal Data** means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, criminal records or any other sensitive personal information.

- **Third Party** means any natural or legal person, public authority, establishment or any other body other than the data subject, the data controller, the data administrator and the persons who are engaged by the data controller or the data administrator to process personal data.

Section Two

4. DATA PROTECTION OFFICERS

At a glance

- The Nigeria Data Protection Regulation (NDPR) introduces a duty for all public and private organisations in Nigeria to designate a Data Protection Officer (DPO) if they control data of natural persons or carry out certain types of data processing activities.

- DPOs assist you to monitor and audit internal compliance, inform and advise on your data protection compliance.

- The data protection officer is appointed by a data controller.

- DPOs can be an existing employee or externally appointed.

- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

- DPOs play a key role in your organisation's data protection governance structure and also help to improve data accountability.

What professional qualities should the DPO have?

- The NDPR says that you should appoint a DPO on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection laws in Nigeria.
- It doesn't specify the precise credentials they are expected to have, but it does say that this should be proportionate to the type of processing your organisation carry out, taking into consideration the level of protection the personal data requires.
- It states that DPOs must be a verifiable competent person or firm.
- It would be an advantage for your DPO to also have a good knowledge of the nonprofit sector, as well as your data protection needs and processing activities.
- A DPO can be an existing employee as long as the professional duties of the employee are compatible with the duties of the data protection officer and do not lead to a conflict of interests.

What are the tasks of the DPO?

- The DPO's tasks as defined in Part 4.1 of the Nigeria Data Protection Regulation are:
- To inform and advise you and your employees about your obligations to comply and adhere with the NDPR and other data protection laws.
- Produce relevant data privacy instruments and follow data protection directives of the data controller.
- DPOs are tasked with monitoring compliance with the NDPR and other data protection laws, organisation's data protection policy, audits of privacy and data protection practices.
- When performing their tasks, DPOs have due regard to the risk associated with processing personal information collected, and takes into account the nature, scope, context and purposes of processing

Reference: The Nigeria Data Protection Regulation 2019 is the regulation that safeguards the rights of natural persons to data privacy, it fosters safe conduct for transactions involving the exchange of personal data and prevent manipulation of personal data.

For further information on NNNGO's work on Guide on Data Protection for Nonprofits, contact:

Adeola Odunsi
Project Officer
Nigeria Network of NGOs
Tel: +2349069460107
E-mail: adeola.odunsi@nnngo.org

Oyindamola Aramide
Communication Officer
Nigeria Network of NGOs
Tel: +2349069460107
E-mail: oyindamola.aramide@nnngo.org

About NNNGO

The Nigeria Network of NGOs (NNNGO) is the first generic membership body for civil society organisations in Nigeria that facilitates effective advocacy on issues of poverty and other developmental issues. Established in 1992, NNNGO represents over 2800 organizations ranging from small groups working at the local level, to larger networks working at the national level.

Nigeria Network of NGOs
15, Ramat Crescent, Ogudu,
GRA,Lagos,Nigeria.
Tel: +2349069460107
Email: nnngo@nnngo.org
Website: https://nnngo.org/

Connect With Us

nnngo.org nnngo nnngo nnngo 2349030700208