GROUP A

ASSIGNMENT, WEEK 1

A REVIEW AND ANALYSIS OF THE NIGERIAN DATA PROTECTION ACT (NDPA) 2023, VIZ A VIZ THE GENERAL DATA PROTECTION REGULATION

The **General Data Protection Regulation** (**Regulation (EU) 2016/679** (**GDPR/the Regulation**) is a European Union regulation on information privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also governs the transfer of personal data outside the EU and EEA. The GDPR's goals are to enhance individuals' control and rights over their personal information and to simplify the regulations for international business. It supersedes the Data Protection Directive 95/46/EC and, among other things, simplifies the terminology.

SCOPE AND APPLICABILITY OF GDPR

The GDPR applies to all organizations that process the personal data of EU citizens. This includes every company that offers goods and services or employs people in the EU, even if an entity is based outside the EU. The GDPR applies to companies, associations, organizations, authorities and in some cases private individuals. The regulation applies if the Data Controller (DC), Data Processor (DP), or the Data Subject (DS) is based in the EU

Amongst other things, the GDPR provides that:

- The "Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

- The protection afforded by the regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

- The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system.

- The Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. However, the Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

- The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is

related to the monitoring of the behavior of such data subjects in so far as their behavior takes place within the Union.

RIGHTS OF DATA SUBJECTS UNDER THE GDPR INCLUDE BUT NOT LIMITED TO:

- Right to be informed about how and why their data is used
- Right to access personal data held about them
- Right to rectification of inaccurate or incomplete data
- Right to erasure or to be forgotten
- Right to restrict processing of their data.

The GDPR provides for the protection of natural persons in relation to the processing of personal data as a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

DATA PROCESSING REQUIREMENTS

The GDPR requirements for data processing include:

- **Lawfulness, fairness, and transparency**: Data processors must process personal data lawfully, which means they must have a legal basis for processing the data.
- **Purpose limitation and data minimization:** Data processors should only process personal data for the specific purposes for which it was collected.
- **Accuracy and storage limitation:** Personal data must be accurate and kept up to date, and should not be kept for longer than necessary.
- **Integrity and confidentiality (security):** Personal data must be processed in a manner that ensures appropriate security.
- **Accountability:** Data processors must be able to demonstrate compliance with GDPR.

In addition to the requirements above, the GDPR also covers lawful basis, special category data, criminal offence data, consent, contracts, legitimate interests, vital interests, public task, legal obligation, and biometrics.

CONSENT MECHANISMS UNDER THE GDPR

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis. In other words, consent is just one of the legal bases you can use to justify your collection, handling, and/or storage of people's personal data. Article 6 states five other justifications.

These are the other legal bases:

1. Processing is necessary to satisfy a contract to which the data subject is a party.

2. You need to process the data to comply with a legal obligation.

3. You need to process the data to save somebody's life.

4. Processing is necessary to perform a task in the public interest or to carry out some official function.

5. You have a legitimate interest to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data.

According to the Article 32 of the GDPR, "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided".

Also, Article 33 of the GDPR provides that "data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research."

You only need to choose one legal basis for data processing, but once you've chosen it you have to stick with it. You cannot change your legal basis later, though you can identify multiple bases. You should conduct a GDPR data protection impact assessment before processing personal data.

DATA BREACH NOTIFICATION REQUIREMENT OF GDPR

The GDPR requires organizations to report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. The notification is not required if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the affected individuals must also be informed without undue delay. A breach that requires notification under GDPR is an incident that causes accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

PENALTIES AND ENFORCEMENT MECHANISM

Violators of the provisions of the GDPR may be fined up to €20 million, or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater.

ENFORCEMENTS: THERE ARE TWO POTENTIAL AREAS OF LIABILITY UNDER THE GDPR:

- The Information Commissioner could take regulatory action. The most severe sanction would be the imposition of a fine (a penalty notice). That fine could, in theory, be for the greater of €10 million or 2% of annual worldwide turnover. ...
- Private claims by individuals for damage or distress caused by the breach. Such claims have historically been rare but are becoming more common.

SIMILARITIES WITH THE NIGERIA DATA PROTECTION ACT (NDPA) 2023

Scope and Applicability

The primary legislation governing data protection in Nigeria is the **NIGERIA DATA PROTECTION ACT 2023 (NDPA/the ACT)**, which applies to the processing of personal data by data controllers and processors in Nigeria, regardless of whether such processing occurs within Nigeria or not**.** The scope of the Act transcends across safeguarding the fundamental right of privacy and interest of data subjects guaranteed under the 1999 constitution of the Federal Republic of Nigeria. See Section 1 and 2 of the Act. The Act does not apply to processing of personal data carried out solely for personal or household purposes in as much as it does not violate the fundamental rights to privacy under Chapter IV of the constitution. See Section 3(1) of the Act. The Act does not also apply to processes carried out by competent authority in furtherance of public policy. See Section 3(2)(a)-(e) of the Act.

CONSENT MECHANISMS

The NDPA requires data controllers to obtain the consent of data subjects before processing their personal data. Consent must be freely given, specific, informed, and unambiguous. Section 25 of the Act provides for the lawful basis of personal data processing. The section dwells on the need for the data subject to give, and not withdraw consent for the specific purpose(s) for which the data is to be processed. To ensure consent is duly obtained, Section 26 of the Act places the burden of proof for establishing consent on the data controller. Notably, in establishing consent, the Act provides that consent must be in the affirmative and not based on a pre-selected confirmation. See Section 26(7)(a)-(b). It is also noted that silence or inactivity of the data subject shall not constitute consent under the Act. See Section 26(3). Sections 30, 31, 35, 37, 43, 65 of the Act also reinforces the concept of the unequivocal consent of the data subject in processing of data and the right of the data subject to withdraw consent as s/he deems necessary.

PRINCIPLES OF DATA PROTECTION:

The NDPA outlines principles similar to those in the GDPR, such as lawfulness, fairness, and transparency in data processing, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. The sections under Part V of the Act copiously made provisions for principles guiding data controllers and processors to foster data protection. For instance, Section 25, 26, 27, 28, 29, 30, 31, 32 and 33 provides guiding principles on lawful basis to process personal data, consent and its withdrawal, provision of information to the data subject on how his or data will be processed or used, as well as data impact assessment in cases where data may result in high risk of breach to fundamental rights of the data subject.

The Act further provides for obligations of the data controller and data processor, principles guiding processing of sensitive personal data, principles on how to process data of individuals that lacks legal capacity to give consent. The act also made it a requirement in data processing for a data controller to have a Data Protection Officer who is knowledgeable in data protection law and practice to advise and monitor compliance of the data processor or controller with the principles of data protection set out in the Act.

RIGHTS OF DATA SUBJECTS

The NDPA grants data subjects rights similar to those in the GDPR. These include right to make relevant enquiries on how the data obtained for processing are stored, the purpose of processing, category of personal data concerned, particulars of third-party users etc. Data subject also have rights to access their personal data, the right to rectification, erasure, restriction on processing, the right to data portability for easy access and transmission without any hinderance, withdrawal of consent, right not to be subjected to a decision based solely on automated processing of personal data (i.e., profiling) and the right to object to processing. See Section 34 to 38 of the Act.

DATA PROCESSING REQUIREMENTS

Section 39 of the NDPA requires data controllers and processors to implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control. The Act requires a level of security appropriate to the risk in processing such data. In fact, data controllers and data processors are required to conduct data protection impact assessments for high-risk data processing activities while taking into account

(a) The amount and sensitivity of the personal data

(b) The nature, degree, and likelihood of harm to a data subject that could result from the loss, disclosure or other misuse of the personal data

(c) The extent of the processing

(d) The period of data retention, and

(e) The availability and cost of any technology, tools or other measures to be implemented relative to the size of the data controller or data processor/

To aid compliance with the above requirement, the Act in its Section 39(2) made provisions for measures data processors and data controllers may adopt for security integrity and confidentiality such as encryption of personal data, periodic assessment of risks to processing systems and services to include cases where such processing involves the transmission of data via an electronic communication network as well as regular updating of the measures and introduction of new measures to address shortcomings in effectiveness and accommodate evolving risks ascribed to data processing

DATA BREACH NOTIFICATION REQUIREMENTS

Both regulations are subject to notification within 72hours of becoming aware of a data breach. The NDPA requires data controllers to notify the Nigerian Data Protection Regulation Commission (NDPAC) and affected data subjects of data breaches **within 72 hours** of becoming aware of a breach which is likely to result in risk to the rights and freedoms of individuals, and where feasible, the data processor or data controller is required to describe the nature of the data breach to include the categories and the approximate numbers of data subject and personal data records breached. See Section 40(2) of the Act. Also, where a personal data breach is likely to result in a high risk to the right and freedoms of a data subject, the data controller shall **IMMEDIATELY** communicate the incident to the affected data subject in plain and clear language and advise on measures the data subject may take to mitigate the effects of such breach. See Section 40(3) of the Act.

For GDPR, in the case of a data breach,

a. The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

b. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

c. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

PENALTIES AND ENFORCEMENT MECHANISMS:

The NDPA in its Section 4 established a commission, the Nigerian Data Protection Commission (NDPC), and under Section 6 of the Act, the commission is saddled with the duty of enforcing and implementing the provisions of the Act. In another sense, the Act empowers the NDPC to enforce compliance with the regulation and imposes fines and other penalties for non-compliance.

Section 48 of the Act provides that where the commission is satisfied that a data controller or data processor has violated any provision of the Act or any subsidiary legislation made under the Act, commission may order the data processor or data controller to remedy the violation, or ordered the data controller or data processor to pay compensation to the data subject who has suffered injury due to the violation of the provisions of the Act by the data processor or data subject, order the data processor or data controller to account for the profits made from such violations, pay a penalty fee or a remedial fees. Section 48(4) of the Act provides the remedial punishment. For instance, the higher maximum amount shall be greater of ₦10,000,000 and 2% of its annual gross revenue in the preceding financial year, while the standard minimum amount shall be the greater of ₦2,000,000 and 2% of its annual gross in revenue in the preceding years. The Act made it an offence to fail to comply with the order of the commission and upon conviction, the court may award fine against the data processor or data controller in line with the highest maximum amount and small minimum amount as provided or give a term of imprisonment not more than 1 year as the case must be body. See Section 46 – 53 of the Act.

CONCLUSION

The GDPR and the NDPA have similar goals of regulating the processing of personal data and safeguarding individuals' privacy rights, but they differ in terms of their precise rules, applicability, and extent. On the bright side, initiatives to bring Nigerian data protection laws into compliance with global norms like the GDPR show that the country is committed to guaranteeing the security of personal data of its citizens.

REFERENCES

1. https://nitda.gov.ng/wp-content/uploads/2021/01/NDPA-Implementation-Framework.pdf

2. https://gdpr-info.eu/