DATA PROTECTION: ALL YOU NEED TO KNOW ABOUT DATA PROTECTION AND PRIVACY COMPLIANCE

Data Protection compliance is the universally accepted practice of ensuring that sensitive data gathered by organizations and businesses is organized and managed in such a way as to enable organizations to meet enterprise business rules along with lawful and constitutional regulations. Data protection compliance entails establishing policies that outline how data protection is achieved in your organization in line with existing laws and regulations.

In order to be compliant, an organization (also referred to as a data processor) who processes the personal data of data subjects (the individual or natural person whose data is to be protected) shall ensure that they exercise the highest level of care in collecting, storing and managing the personal/sensitive data of the data subject. 'The Personal Data' herein referenced means any information relating to an identified or identifiable natural person ('Data Subject'). Such a person is one who can be identified, directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier or by factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

LEGAL REQUIREMENTS FOR DATA PROTECTION COMPLIANCE

In the past decade, approximately 90 countries worldwide have adopted data protection regulations, with the European legislation known as the GDPR which came into effect on May 25 2018, being recognized as one of the most comprehensive pieces of legislation till date. In Nigeria, on the 25th of January 2019, a data protection regulation was released by National Information Technology Development Agency ("the NITDA") which is the primary body responsible for the administration and monitoring of the use of electronic data and other forms of electronic communication transactions.

On close scrutiny, it is evident that the material scope and content of the NITDA Data Protection Regulation 2019 ("the Regulation") which replaced the NITDA Guidelines 2017 ("the Guidelines") is heavily influenced by its European counterpart, The GDPR. Though the NDPR has been criticized as being a poorly knitted together version of the GDPR it is important to note that both legislation essentially agree that:

1) Data privacy is a fundamental right of the data owner (or data subject) which should be protected through regulatory oversight even though the data has been submitted to a company for the provision of services;
2) Both legislations provide similar definitions with respect to key areas such as 'processing,' 'personal data' 'sensitive personal data, 'data controller and data processor.

REQUIREMENT FOR DATA PROTECTION COMPLIANCE FOR BUSINESS OPERATIONS AND ORGANISATIONAL CULTURE

The presence of data protection regulation is globally recognized as an indication for trust in a country's digitally driven business space. Data protection practices amongst other concerns, have quickly become a topic for organizational risk management and now forms part of negotiation talks between companies in different geographical locations and jurisdictions looking to do business with one another. This has therefore

made it imperative that organizations seeking to do business online, consider incorporating privacy protection practices in their marketing and operational strategy.

As a marketing strategy, digitally driven businesses are utilizing the World Wide Web as a business development tool, which helps them easily connect with potential and existing consumers to better understand their needs. Companies with consumer focus at the core of their business strategy are continually applying ingenuous practices to accumulate data on consumers and/or their activities, the aim being to gather customer data to create competitive market advantage. Data protection compliance therefore requires that all such consumer data must have been collected with the lawful consent of the consumers and stored securely to ensure the integrity of the data/information is not undermined or exposed to risk.

Data protection should also form part of a company's internal HRM (Human Resource Management) strategy, as an organization is tasked with the responsibility of ensuring complete privacy of employee records which are stored as electronic data. As an employer, transparency and discretion is required in dealing with employees' personal data, within and outside the organisation. Employers must be accountable for data processing activities while also complying with data protection principles. The NDPR regulations advises businesses who gather such data to invest in the training and sensitization of employees on their rights under the regulation as well as their duties and obligations towards such information they may have access to in the course of carrying out their responsibilities.

In view of the covid-19 pandemic, certain cadre of public officials in the public sector work remotely resulting in the utilization of varying means of technology to facilitate the work process and transmit data from one remote personnel to another. In response to this, the National Information Technology Development Agency (NITDA) on the 18th of May, 2020 issued Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 ("the Guidelines"). The Guidelines govern the roles and responsibility of public officers and public institutions with regard to the processing and management of personal data in compliance with the Nigeria Data Protection Regulation 2019 (NDPR). It is then imperative that the government implements a data security strategy to ensure

that all government data and especially personal data is handled with care and in tandem with the provisions of the NDPR and the referenced Guidelines.

WHO DOES IT APPLY TO?

As stated above the NDPR regulates both public and private sector business entities. The NDPR mandates that all organizations that process the personal data of more than 1000 data subjects in a period of 6 months and 2000 Data Subjects in a period of 12 months are to submit themselves to a Data Protection assessment to assess the impact of technology on privacy and security of stored data. An audited report is thereafter submitted to NITDA not later than15th March every year. It is pertinent to note that due to the continued effect of the covid-19 pandemic, NITDA has extended the timeline for filing the 2021 data audit report from 15 March 2021 till 30 June 2021.

In practice, this therefore makes it necessary for **ALL** forms of businesses in Nigeria irrespective of size or structure who meet the above criteria to audit their data collation, privacy and protection practices. Multinational companies operating in Nigeria are not exempt, and are deemed to be processing data in Nigeria where the following criteria are met:

1) Where the multinational company has a branch or subsidiary intended to promote its activities which is oriented towards Nigerians;
2) Where the parent company of the multinational designates an entity in Nigeria as its subsidiary for the purpose of contracting on its behalf for advertising or other legal or commercial purposes.
3) Where the branch or subsidiary in Nigeria forwards to the parent or other members of the group located outside Nigeria requests or requirements relating to data subjects.

HOW CAN AN ORGANISATION ACHIEVE DATA PROTECTION COMPLIANCE?

The Nigerian Data Protection Regulation clearly stipulates the responsibilities of data controllers and processors with respect to how they may lawfully obtain and process data. For a data controller or processor to successfully comply with the provisions of the NDPR, they must take into consideration the following:

Data Protection Compliance Officers (DPCOs) – the NDPR states that an organization seeking to comply with the regulatory requirement must enlist the services of a DPCO. Under the NDPR, DPCOs are licensed professionals who have been certified by NITDA to provide auditing and compliance services for data controllers. DPCOs execute Data protection audits and privacy trainings, provide legal and technical advisory services; draft regulation contracts and privacy notices, Data Protection Impact Assessment, and file audit reports on behalf of organizations to NITDA.

Consent: Section 7 of the Regulation requires that an organization must ensure that consent is obtained before data of any person qualifying as data subject is stored or processed. The consent must not be obtained by coercion or fraud, and the data subject must not be in doubt as to the reason why such information is being requested and for what purpose it will be utilized. Therefore, for an organization seeking to align with the NDPR requirements should take a closer look at its internal and external database to ensure that the data collation mechanisms employed in mining such data are in accordance with the NDPR guidelines.

Data Protection Audit: On the journey to compliance, the regulation requires that the organization must make its data privacy policies available to the general public in conformity with the law. The NDPR requires organizations who process personal data (data processors) to submit a Data protection audit report to NITDA not later than 15th March annually. The Data Protection audit should state:

1) The type and extent of data the organization collects on its employees and members of the public;

2) The purpose for which such data is collected;
3) Notice given to individuals regarding the collection and use of their personal information;
4) The access given to individuals to review, amend, correct, supplement, or delete such data;
5) Whether or not the consent of these individuals was obtained before collecting, using, transferring or disclosing these data; and the methods employed to obtain consent;
6) The policies and practices of the organization for the proper use and security of these data;
7) Organizational policies and procedures for privacy and data protection;
8) The policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.

Data Controllers should also audit third party processor contracts which require the transfer of personal data to such third parties.

CONCLUSION

Data is one of the most important assets in any organisation and as such data protection compliance should be a top priority for all businesses. In addition to several high profile leak of organisations' data, the need for data protection compliance has become increasingly important for all businesses.

In light of the above, local and international organizations doing business in Nigeria are advised to understand the importance of data privacy compliance and take all necessary steps to achieve the required level of compliance as required by the Regulations.

For more information please contact:

Blackwood & Stone LP

info@blackwoodstone.com

+234 903 3501 613