BANWO & IGHODALO

LEGAL AND REGULATORY IMPLICATIONS OF THE GDPR ON BUSINESS ORGANIZATIONS: BASIC COMPLIANCE STRATEGIES FOR NON-EU ENTITIES

The European Union (**"EU"**)'s General Data Protection Regulations ("**GDPR**" or the "**Regulations**"), adopted by the European Parliament and the Council of the EU in April 2016, finally came into force on the earlier agreed date of May 25, 2018. The GDPR is a landmark in the global history of regulatory regimes. The Regulations apply extraterritorially to all business entities that target EU citizens and residents, anywhere in the world. It also prescribes heavy penalty for non-compliance. Whilst enforcement of the GDPR on affected entities has commenced with full and instant compliance within the EU territory, efforts at compliance among many organizations outside the EU remain an ongoing process.

This article highlights the core provisions of the GDPR, analyses the legal and regulatory implications of the Regulations on affected entities, and provides hints on compliance strategies for non-EU organizations, particularly Nigerian business entities.

SCOPE AND OBJECTIVES OF THE REGULATIONS

At its core, the GDPR is a set of rules made to give EU citizens and residents more control over their personal data. Prior to the adoption of the GDPR, the applicable data protection regulation in all EU Member States was the *EU Directive 95/46/EC*. Whilst the EU Directive has similar objectives and provisions to the GDPR, it was implemented in fragments across EU Member States. The GDPR is therefore developed to apply uniformly across the EU territory in protecting sensitive personal data of EU data subjects.

Essentially, the Regulations

(i) repealed and replaced the EU Directive 95/46/EC as the new rules applicable uniformly to the collection and processing of the data of all natural persons across the European Single Market ("Eurozone"); and

(ii) apply extra-territorially to all persons and entities offering goods and services to EU citizens and residents, and in the process collect, process, and store data of the citizens/residents.

As provided in Article 3 of the GDPR and paragraph 23 of the recitals, the Regulations are binding on:

(i) All EU organizations, with presence/offices either within the EU or outside of the Eurozone, that collect, process and store data of natural persons within the EU;

(ii) All non-EU organizations, situate anywhere in the world, that collect, process, store and control the data of natural persons who are citizens or residents in the EU, for the purposes of offering goods and/or services. It does not matter whether such goods or services are paid for by, or offered free of charge to, the data subjects.

Also, in accordance with Article 3(2) & (3) of the GDPR, the territorial scope of the Regulations is activated where personal data;

(i) are processed in anticipation of the offering of goods or services to data subjects in the EU, irrespective of whether a payment by the data subject is required;

(ii) are processed for the monitoring of the behavior of data subjects, as far as their behavior takes place within the EU;

(iii) are processed by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

For the purpose of the GDPR, mere accessibility to a data processor/controller's website or that of its intermediary by EU data subjects, does not amount to sufficient intention to offer goods and/or services. Same goes for accessibility of data processor/controller's email address or other contact details. In the same vein, the use of a language generally used in the foreign country where a data processor/controller is established, is insufficient to ascertain an intention to offer goods and/or services.

However, pursuant to Article 3 of the GDPR and paragraph 24 of the recitals, where a data processor/controller uses a language or a currency generally used in one or more EU Member States, with the possibility of ordering goods and services in that other language, it becomes apparent that the data processor/controller envisages offering of goods or services to data subjects in the EU. In this case, the provisions of the GDPR will apply. Same goes for situations where a data processor/controller mentions customers or users who are in the EU.

Similarly, the Regulations will be applicable where a data processor/controller who, not being established in the EU, processes personal data of EU data subjects for the purpose of monitoring how such data subjects behave within EU territory. A processing activity is considered as monitoring the behavior of

data subjects, if it is ascertained that it is done to track natural persons on the internet, including potential subsequent use of data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning the data subject for analyzing or predicting his or her personal preferences, behaviors and attitudes.

From the foregoing, the provisions of the GDPR are binding on all non-EU (including Nigerian) entities offering goods and services to persons within the EU territory, irrespective of whether or not they have offices within the EU. Such entities are bound by the Regulations in so far as they collect, process, store and control "personal data" or "sensitive personal data" of EU citizens and residents. Compliance is therefore required from Nigerian entities, such as banks, law firms, accounting firms, and consulting organizations among others, offering services to foreign clients who are European citizens or residents.

CORE GDPR PRESCRIPTIONS

- **Consent & Data Security**

  The GDPR prescribes more control for EU data subjects over their personal data. In essence, data processors/controllers across the globe must show that data subjects not only consented to the collection, processing, storing, and transmission of their personal data but that the consent was freely, genuinely and absolutely given, without restrictions. Hence,

  (i) Article 7 of the GDPR requires that consent must be freely given, specific, informed and unambiguous. Request for consent by a data controller should be separate from other terms, and be in clear and plain language. In addition to this, a data subject's consent to processing of their personal data must be as easy to withdraw as it is to give;

(ii) consent must be explicit for sensitive data. A data controller is required to be able to demonstrate that consent was given;

(iii) where personal data is processed for direct marketing, the data subjects will have a right to object. This right must be explicitly brought to their attention by a data processor/controller; and

(iv) provision for parental consent is to be given when data of children is involved. This will not be necessary only in the context of processing the data of a child for preventative or counselling services offered directly to the child.

- **Right of Access to Personal Data**

The GDPR provides in Articles 15 and 16 that data subjects should be given the right and opportunity to access their data or update them at any time, in the data base of processors and controllers.

- **Right to Data Portability**

The GDPR provides in Article 20 for the **"right to data portability".** This is the right to receive personal data previously provided by a data subject to a processor/controller in a structured, commonly used and machine-readable format. This also includes the right to transmit those data to another processor/controller without hindrance from the existing processor/controller.

- **Right of Erasure of Personal Data**

In accordance with Article 17 of the GDPR, where a data subject withdraws prior given consent, at any stage of a collection process (whether at the beginning, middle or after the completion of a transaction), such data subject has the right to request that his/her personal data be completely erased from the data processor/controller's data base, storage or system. This is otherwise known as "right to be forgotten". This right is however limited by instances in which processors/controllers are required by law to keep the data.

- **Data Security Audit**

The GDPR requires that data processing be carried out in a manner as to ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. To this end, the use of appropriate technical or organizational measures (Integrity and Confidentiality) is prescribed in

Article 5(1) f) of the Regulations. Similarly, organizations are to establish a culture of monitoring, reviewing and assessing data processing procedures in order to forestall unnecessary retention of data in the system. In this connection, adoption of a compliant Binding Corporate Rules ("BCR"), as provided in Article 47 of the GDPR, is prescribed for affected entities. In line with the provisions of Article 32 of the GDPR, organizational BCR should emplace an IT architecture that supports "pseudonymisation" and encryption of personal data; ongoing confidentiality, integrity, availability and resilience (CIAR) of processing systems and services; as well as a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

- **Data Breach Notification**

The GDPR in Article 33 requires a data controller to report any case of a personal data breach to the appropriate supervisory authority at once, or if impracticable in phases, without undue delay and where feasible, not later than seventy-two (72) hours after having become aware of the breach. Where the notification to the supervisory authority is not made within the stipulated period, it shall be accompanied by reasons for the delay. The notification shall describe the nature of the breach, categories and approximate number of data subjects and personal data records concerned, likely consequences of the breach, and measures taken or proposed to be taken by the controller to address the breach, including possible measures to mitigate the likely adverse effects of the breach. In Article 34, the GDPR further mandates data processors/controllers to communicate to affected data subjects, without undue delay, any personal data breach likely to result in a high risk to the rights and freedoms of natural persons.

PENALTIES FOR INFRINGEMENT

The GDPR in Article 84(5) prescribes penalties of up to EUR 20 million for infringements of its provisions. Under the Regulations, a Data Protection Authority ("DPA") in any Member State is empowered to impose fines of up to EUR 20 million, or in the case of an undertaking, 4% of annual worldwide turnover of the preceding financial year (whichever is higher) for infringements relating to

(i) transfers of personal data to a recipient in a third country or to an international organization;

(ii) basic principles for processing, such as conditions for obtaining the consent of data subjects;

(iii) the rights of subject data; and

(iv) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to the Regulations.

For other infringements, such as relating to (i) the obligations of data processors and controllers, and (ii) data certification and data monitoring authorities; a fine of up to EUR 10 million shall be applicable, or in the case of an undertaking, 2% of annual worldwide turnover of the preceding financial year (whichever is higher). A DPA is required to consider the nature, gravity and duration of an infringement before arriving at appropriate sanctions to apply.

COMPLIANCE STRATEGIES

Given the severity of the prescribed penalties for non-compliance, non-EU entities whose activities fall under the regulatory purview of the GDPR have an obligation to speed up their compliance process in the aftermath of the May 25 deadline and be in the same position with their EU counterparts. In this regard, the following are recommended as quick wins for affected non-EU entities working to attain full compliance with the GDPR:

- **Privacy Policy & Hack-proof IT System:** Business entities should develop privacy policies for the use of their data processing systems/platforms in a plain and direct language easily understandable by data subjects. A compliant privacy policy should observe and respect the rights of data subjects as specified in the GDPR**.** For those who already have a privacy policy in place, existing consents may still work, but only provided they meet the new prescriptions in the Regulations. Entities must embrace privacy by design and default in accordance with Article 25 of the GDPR. In the same vein, organizations should invest in modern, hack-proof information technology ("IT") systems with IT departments devising a strategy for establishing certification mechanisms and data protection seals and marks, that allow data subjects to quickly assess the level of data protection on their websites.

- **Appointment of a Data Protection Officer ("DPO"):** Non-EU entities required to comply with the Regulations should establish a framework for accountability by appointing a Data Protection Officer (DPO), as prescribed in Articles 37, 38 and 39 of the GDPR. The DPO is to ensure that the privacy policy in place is not opaque or restrictive and that data security architecture installed is at all times not susceptible to hacking or cyberattacks. It will also be the duty of the DPO to ensure that proper documentation is done along the data processing line and that data retention is in compliance with the provisions of the GDPR. The DPO will also ensure that proper notification of any personal data breach is made to the appropriate supervisory authority or the affected data subjects, as the case may be, to avoid contravention of the GDPR.

- **Lawful Processing of Data:** Another way by which affected non-EU entities can easily comply with the GDPR is by keeping their data processing activities within the areas classified under Article 6 as "Lawfulness of processing". Essentially, activities qualified as lawful processing constitute permissible derogations under Article 49 of the GDPR. Accordingly, data processing and transfer shall be lawful only if, and to the extent that at least, one of the following applies:

  - ✓ The data processing is by a natural person in the course of a purely personal or household activity;

  - ✓ the data subject has given consent to the processing of his or her personal data for one or more specific purposes, after having been informed of the possible risks of such processing/transfer;

  - ✓ 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;

  - ✓ processing is necessary for compliance with a legal obligation to which the controller is subject;

  - ✓ processing is necessary in order to protect the vital interests of the data subject or of another natural person;

  - ✓ processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

  - ✓ processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, particularly where the data subject is a child. Public authorities are however exempted from this provision where they process data in the performance of their official tasks;

  - ✓ transfer of data 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;

- ✓ transfer of data 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;
- ✓ transfer of data is necessary for important reasons of public interest;
- ✓ transfer of data is necessary for the establishment, exercise or defence of legal claims;
- ✓ transfer of data 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; and
- ✓ transfer of data is made from a register which, according to the EU or a Member State law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that laid down conditions in the law for such consultation are fulfilled in the particular case.

CONCLUSION

The GDPR is a first of its kind. Prescribing heavy penalties, enforced uniformly across the EU and applicable extraterritorially, it is no doubt a super regulation. Whilst it is incontrovertible that non-EU entities that process personal data of EU citizens/residents must comply with the provisions of the GDPR, it should be noted that application of the Regulations will have to be subject to extant local legislation across different jurisdictions.

In Nigeria, entities that serve EU citizens and residents, while taking the above recommended steps for compliance, will have to consider applicable statutory provisions relating to the processing of personal data. For instance, while the rights of data subjects to restrict the processing/transfer and disclosure of their personal data without consent may be in sync with extant regulatory and constitutional provisions in Nigeria, the right of erasure of personal data after withdrawal of consent by data subjects will not be absolute as certain entities are required to retain information, including personal data, collected in the ordinary course of business for specified number of years.

For instance, a financial institution in Nigeria is required under the *Money Laundering (Prohibition) Act,* to preserve the record of a customer's identification for a period of at least five (5) years after the closure of the account or the severance of relations with the customer. A bank is similarly required under the *Anti-Money Laundering and Combating the Financing of Terrorism (Administrative Sanctions) Regulations* of the Central Bank of Nigeria (CBN AML/CFT Regulations), to retain transaction information containing particulars of customers and, in some cases, forward same to certain regulatory agencies. Also, a Credit Bureau is required under the *Credit Reporting Act*, to first retain credit information of persons for a period of not less than six (6) years after which such information shall be archived for a further period of ten (10) years before it can be destroyed. Further, a service provider is required, under the *Cybercrimes (Prohibition, Prevention, etc.) Act,* to retain all traffic data and subscriber information, as may be prescribed by the relevant authority for communication services in Nigeria, for a period of two (2) years.

These obligations will necessarily limit the rights of EU data subjects, especially the right to withhold consent and the right of erasure. However, it is instructive to note that these statutory limitations are recognized under the "Restrictions" in Article 23 of the GDPR.

We note that while enforcement of the GDPR will be easy within the EU, the same cannot be said of other jurisdictions outside the EU. No doubt, it will be easier to sanction EU affiliates of Nigerian entities that contravene the GDPR. It is therefore imperative that multinationals ensure that their Nigerian subsidiaries/affiliates are in full compliance. Also, the issue of proportionality will obviously be taken into consideration in view of the challenges involved in extra territorial enforcement and big scale infringers may be targeted than small scale infringers.

The Grey Matter Concept is an initiative of the law firm, Banwo & Ighodalo

Contact Persons

OLUMIDE OSUNDOLIRE
osundolire@banwo-ighodalo.com

OLUWATOBA OGUNTUASE
ooguntuase@banwo-ighodalo.com