

AELEX



AN OVERVIEW OF
BIG DATA &
DATA PROTECTION
IN NIGERIA

April '19

www.aelex.com

INTRODUCTION

Cambridge Dictionary defines data as “information, especially facts or numbers, collected to be examined and considered and used to help decision-making or information in an electronic form that can be stored and used by a computer[1]”.

That definition helps us understand that data can cover a lot, ranging from employment records, criminal records, personal emails, bank records, health records, trade secrets and other vital information concerning individuals and corporations.

The world contains an unimaginably vast amount of digital information which is getting even vaster more rapidly. According to Forbes, we now produce 2.5 quintillion bytes of data every day. Indeed, 90% of all the data in the world has been created over the last two years. This huge availability of data is what the term ‘Big Data’ refers to.

For a working definition, Big data is a term that describes “a large volume of structured, semi-structured and unstructured data that has the potential to be mined for information[2].”

The European Data Protection Board has defined big data as the, “gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms”.

The Economist Newspaper has even described data as the oil of the digital era[3]. Indeed, this is arguable when one considers that five of the most valuable listed corporations in the world deal with data. These companies are Microsoft, Facebook, Apple, Amazon and Alphabet Inc. (the parent company of Google). The Business Insider reported in 2017 that 53% of online sales in America were made through Amazon. To put that in context, 53 cents of every dollar spent online was given to Amazon[4].

Forbes also recently reported that Google and Facebook have created a duopoly when it comes to digital advertising in America[5]. In 2017, \$83 billion was spent on digital advertising, surpassing the value spent on TV advertisements. Over 60% of the revenue generated went to

[1] Cambridge Advanced Learner's Dictionary, 'Data' (Cambridge University Press) Available at <<https://dictionary.cambridge.org/dictionary/english/data>> . Accessed 1 April 2019.

[2]TechTarget. 'Big data'. Available at <<https://searchdatamanagement.techtarget.com/definition/big-data>> Accessed 1 April 2019.

[3]The Economist. 'The world's most valuable resource is no longer oil, but data' (The Economist , 6 May 2017) Available at <<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>> Accessed 1 April 2019.

[4]Eugene Kim, 'More than half of online sales growth in the US came from Amazon last year Business Insider February 2 2017' (Business Insider, 2 February 2017) Available at <<https://www.businessinsider.com/amazon-drives-more-than-half-us-ecommerce-growth-2016-2017-2?IR=T>>. Accessed 1 April 2019.

[5] Avi Dan, 'The State Of Digital Advertising: The Google, Facebook Duopoly Tightens Its Grip March 19 2017 Forbes' Available from <<https://www.forbes.com/sites/avidan/2017/03/19/the-state-of-digital-advertising-the-google-facebook-duopoly-increases-its-grip/#7fddaab47eae>> Accessed 1 April 2019.

Facebook and Google. So it is clear that these data handlers may be dealing with the new oil or the new gold as the case may be.

The huge value of data has made it attractive to governments, companies, and even hackers.

Data is now subject to cyber threats. Companies, including Uber and Facebook have been victims of cyber-attacks. In September 2018, there were reports that a cyber-attack exposed Uber's data from 57 million customers and drivers. Facebook also had its share of cyber-attack in September 2018 as 90 million Facebook user accounts were exposed by a security breach in the UK.[6]

General Legal Framework for Data Protection in Nigeria

Most of the data that the world has produced are either personal data (or data that can be traced back to specific individuals). "Traditionally, organisations used various methods of de-identification (anonymisation, pseudonymisation, encryption, key-coding, data sharing) to distance data from real identities and allow analysis to proceed while at the same time containing privacy concerns.

Over the past few years, however, computer scientists have repeatedly shown that even anonymised data can often be re-identified and attributed to specific individuals."[7]

With the importance ascribed to data, it is pertinent that laws be established to protect the data so the persons who own the data, as well as the recipient of the data, are not put at risk.

Data protection and privacy is an extension of the fundamental right of citizens to privacy. Section 37 of the 1999 Constitution (as Amended) protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication.

Aside from the Constitution, there are several other legislation that contains provisions that touch on the protection of data and privacy.

Some of them include the Freedom of Information Act No. 4 of 2011 which enables public access to public records and information, prevents a public institution from disclosing personal information to the public unless the individual involved consents to the disclosure.

[6] Techworld Staff, 'The most infamous data breaches' Available from <<https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/>> Accessed 28 February 2018.

[7] Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010); Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, 2008 Proc. of IEEE Symp. on Security & Privacy 111; Latanya Sweeney, Simple Demographics Often Identify People Uniquely 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000).



The Cybercrimes Act 2011 prevents the interception of electronic communications and imposes data retention requirements on financial institutions.

The Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission requires telecommunication operators to take reasonable steps to protect against “improper or accidental disclosure” and must ensure that such information is securely stored.

It also provides that customer information must “not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations”.

The Consumer Protection Framework issued by the Central Bank of Nigeria in 2016 contains provisions that restrain financial institutions from disclosing the personal information of their customers.

It has however been evident that though these preceding pieces of legislation exist, there had been no comprehensive data protection and data privacy legislation in Nigeria.

The Data Protection Regulation 2019

The National Information Technology Development Agency (“NITDA/the Agency”) was set up by the National Information Technology Development Agency Act 2007 (NITDA Act) as the statutory agency with the responsibility for planning, developing and promoting the use of information technology in Nigeria.

The NITDA Act also empowers the Agency to do the following[8]:

“Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information”.

It was further to the foregoing powers that on 28th January 2019, NITDA published its Data Protection Regulation (“the Regulation”) which aims at protecting personal data of all Nigerians and non-Nigerian residents in Nigeria.

[8] Section 6 (c) of the NITDA Act.

This Regulation is undoubtedly a game changer in the protection of data in Nigeria as it is contemporary and is a replica, in some respects, of the European Union (EU) General Data Protection Regulation (GDPR).

The Regulation wastes no time in describing data which is defined to include a name, a photo, an email address, bank details, medical information, computer internet protocol (IP) address and any other information specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[9]

'Personal data' is also defined as the information relating to an identified or identifiable natural person.[10] In other words, the kind of data that the Regulation seeks to protect does not include corporate information except where such information relates to natural persons. The Regulation applies to all transactions that involve the processing of personal data.[11]

In other words, the Regulation would apply to all natural persons, companies, law firms, hospitals, schools, etc and other persons that process personal information.

Some key persons are identified in the Regulation; they include Data Subjects, Data Controllers and Data Protection Officers.

The roles of the identified persons are envisaged to be very important in driving the objectives of the Regulation.

A Data Subject is the identifiable person who is identified directly or indirectly with reference to an identification number or other factors specific to his/her physical, physiological, mental, economic, cultural or social identity.[12]

The Data Protection Officer is a person designated by the Data Controller to implement the Regulation.[13] The person's responsibility is to ensure compliance of the Data Controller with the Regulation.

[9] Section 1.3 of the NITDA Data Protection Regulation.

[10] Section 1.3 of the NITDA Data Protection Regulation.

[11] Section 1.2 of the NITDA Data Protection Regulation.

[12] Section 1.3 of the NITDA Data Protection Regulation.

[13] Section 3.1.2 of the NITDA Data Protection Regulation.

A **Data Controller** is/are the person or persons who determine how personal data is processed or will be processed.[14]

Processing means any action carried out on personal information. It includes collection, recording, organisation, storage, adaptation, alteration, retrieval, use, disclosure or dissemination.[15]

In other words, a person who determines what happens to personal information must do so in accordance with the legal basis provided by the Regulation. The legal basis for processing includes any of the following:

The processing has been consented to by the Data Subject;

The processing is for the performance of a contract;

The processing is required for compliance with a legal obligation;

The processing is required for protection of the vital interest of a data subject or another natural person; or

The processing is necessary for the performance of a task carried out in the public interest.[16]

Subsequently, the Data Controller may proceed to obtain the information from the Data Subject. In doing so, the Data Controller must supply the Data Subject with certain information such as:

The identity and contact details of the Data Controller;

The contact details of the Data Protection Officer;

The purpose for which the data will be processed as well as the legal basis;

Recipient(s) of the data;

The period for storing personal information;

Rights of the Data Subject;

Possible transfer of the information to 3rd parties, foreign countries or international organisation.

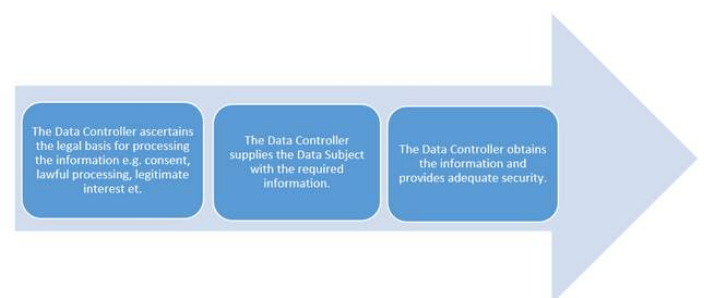


Figure 1: Process flow

[14] Section 1.3 of the NITDA Data Protection Regulation.

[15] Section 1.3 of the NITDA Data Protection Regulation.

[16] Section 2.2 of the NITDA Data Protection Regulation.

During the processing period, the Data Controller has the responsibility to secure the data and respect the right of the Data Subject.

The right of the Data Subject includes the right to rectify the information and to have it in a portable format, the right to erasure of the information, restriction in processing the information and the right to transfer the information to a third party.

Transfer of Data to third party countries

The Regulation provides for the transfer of data to third-party countries.¹⁴ It vests supervisory powers on the Attorney General of the Federation to determine third-party countries with adequate data protection laws for possible data transfer to such countries.

However, where the Attorney General has not decided on such countries, the Data Controller may process the information where:

The Data Subject has consented to the processing;

It is for the performance of a contract in favour of the data subject;

It is for the public interest;

It is for the establishment, exercise or defence of legal claims; or

It is to protect the vital interests of the Data Subject or other persons.

Penalty

The Penalty for failing to comply with the Regulation is dependent on the number of data subjects that a company processes: [17]

a) More than 10,000 Data Subjects - payment of the fine of 2% of Annual Gross Revenue or 10 million Naira whichever is greater;

b) Less than 10,000 Data Subjects - payment of the fine of 1% of the Annual Gross Revenue or 2 million Naira whichever is greater.

Contrast between the GDPR and the Data Regulation

Are the provisions of the Regulation sufficient in protecting personal information? This is yet to be tested. But we hope that like the GDPR, the Data Regulation would be an effective tool.

The GDPR is the data protection law among EU member states, which came into effect on 25th May 2018.

It was necessitated by the vast amount of data collected from EU member countries. The GDPR and the Regulation have similar provisions but differ on some points.

One of such points where they differ include the provisions guiding the different categories of data.

[17] Section 2.10 of the NITDA Data Protection Regulation

Both Laws identify a special category of personal data which the Regulation termed sensitive personal data.

The special categories of data as stated in the GDPR are those which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation. [18]

Unlike the Regulation, one of the legal basis for processing sensitive information in the GDPR, is where it is publicly available. It is reasonable that information already made public by the Data Subject can be processed. Unfortunately, this legal basis is not recognised by the Regulation.

In addition, the GDPR has excluded the processing of personal data in the course of a purely personal or household activity. [19] Unfortunately, this was not replicated in the Regulations.

However, it is doubtful that NITDA would fine Data Controllers found in this situation. Also, following the adoption of the GDPR in 2016, Companies were given a period of two (2) years to ensure compliance.

This gave companies an adequate opportunity to set up data protection mechanisms. On the other hand, the Regulation is effective from the date of its issuance by NITDA i.e. 28th January, 2019.

It is unlikely that at the effective date of the Regulation, relevant Data Controllers have made provisions for compliance.

Data Protection and Big Data

Essentially, big data is the process of collecting information (massive amounts of data) and the subsequent step of analysing it. Despite the benefits of big data and big data analytics, big data should not come at the cost of the privacy of persons.

At the same time, technology and innovation cannot be stopped, and the "principles of privacy and data protection must be balanced against additional societal values such as public health, national security and law enforcement, environmental protection, and economic efficiency"[20].

In other words, while the abundance and ubiquity of data creates huge social and economic value, it is important to draw the line between data collection, processing, and use, and then apply the appropriate data protection safeguard at the very centre of the value chain.



[18] This is similar to the definition of sensitive data.

[19] Article 1(2)(b) of the GDPR.

[20] Omer Tene & Jules Polonetsky, 'Privacy in the Age of Big Data' (2012) Available at: < <https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/> > Accessed on 1 March 2019.

WAY FORWARD

1. What is Big Data without Protection?

Personal data retain their value if they are perceived (and they are) a scarce and difficult-to-obtain resource by individuals and corporations at large. This is of utmost importance because, if personal data were so widely available, without little or no form of regulatory protection of their content, their informational value would be lower.

For example, people would be more reluctant in providing their data or they would provide false data.

The big data analytics industry will ultimately have to cope with data protection regulations, as the abundance of personal data should be a value to protect, which is also in the interest of the big data analytics service providers.

From a legal standpoint, big data analytics service providers should ensure that the data processed has been or is obtained in a legitimate fashion, i.e. in compliance with the Data Protection Regulation and without deceiving the data subjects.


2. Anonymisation & Pseudonymisation

Anonymisation is the process of removing personal identifiers (direct and indirect) that may lead to the identification of a particular person.

Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of the Regulation and it becomes easier to use.

Pseudonymisation is defined within the GDPR as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual”.

Anonymisation and Pseudonymisation should not only be seen merely as ways of reducing regulatory burden, but should also be considered means of mitigating the risk of inadvertent disclosure or loss of personal data.



Again, anonymisation and pseudonymisation are tools that assist in big data analytics and help government, companies, organisations, and individuals to carry on research or develop products and services.

These processes also give assurance to the people whose data are collected that their data would not be used or exploited unlawfully.

3. Consent

As stated earlier in this article, one of the legal basis for processing personal data under the Regulation is where the consent of the Data Subject has been obtained.

If an organisation is relying on people's consent as the condition for processing their personal data, then that consent must be specific, informed, and freely given.

This means that people must be able to understand what the organisation is going to do with their data and there must be a clear indication that they consented to it.

If an organisation has collected personal data for one purpose and then decides to start analysing it for completely different purposes (or to make it available for third parties to do so) then it needs to make its users aware of this, except where the data is further processed for archiving purposes (in the public interest, scientific or historical research or statistical purposes).

This is particularly important if the organisation is planning to use data for a purposes that are not apparent to the individual because it is not obviously connected with the individual's use of a service.

For example, if a social media company were selling on the wealth of personal data of its users to another company for other purposes, it may be possible to have a process of graduated consent, but until such consent is obtained, any person that falls under the umbrella of Data Controller must not deal or trade in personal data.

It may also be reasonable for organisations to use consent as a condition for processing in a big data context, but they must be sure that it is the appropriate condition.

Conclusion

The introduction of the Data Protection Regulation by NITDA is a welcome development, although there are speculations on the applicability of the Regulation on the premise that the Regulation is simply a subsidiary legislation.

However, we must note that similar to other subsidiary legislation, the Regulation has the force of law; therefore, all transactions on personal data must comply with the provisions of the Regulation.

AELEX



AUTHOR
DAVIDSON OTURU

Partner/IP/TMT
doturu@aelex.com

COPYRIGHT: All rights reserved. No part of the publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior permission in writing of AELEX or as expressly permitted by law.

DISCLAIMER: This publication is not intended to provide legal advice but to provide information on the matter covered in the publication. No reader should act on the matters covered in this publication without first seeking specific legal advice.

AELEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana.

Contact us at:

4th Floor, Marble House,
1 Kingsway Road, Falomo Ikoyi,
Lagos, Nigeria

Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,

E-mail: lagos@aelex.com

Click here www.aelex.com

to follow our social media handles click below

 @aelexpartners

 @aelexpartners

 @aelexpartners