International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 14-07-2022, Accepted: 02-08-2022, Published: 17-08-2022
Volume 8, Issue 4, 2022, Page No. 177-183

Legal protections for health data processed using artificial intelligence wearable and the adequacy of the Nigeria data protection regulation

Musa Omayi Sandra
Data Protection and Tech Policy Analyst and Head of Research, University of Ibadan, Lagos State, Nigeria

Abstract
Artificial intelligence wearable technologies offer endless possibilities to the healthcare sector. They offer a proactive approach to healthcare and can detect health challenges early before they develop into more significant issues. While it offers certain benefits and usefulness, there are privacy and security risks. The sensitive nature of personal data – health data that these technologies collect requires that data protection and privacy legislations specifically respond to their use for processing health data. This paper seeks to analyze the provisions of the Nigerian Data Protection Regulation, 2019 (the Regulation) to ascertain whether its provisions are adequate in protecting the health data collected through artificial intelligence (AI) wearable and whether specific protection in the context of artificial intelligence (AI) wearable is provided for health data. To this end, the Regulation is juxtaposed with the Data Protection Bill, 2020 and the European Union General Data Protection Regulation 2016 to highlight and compare the differences in protection.

Keywords: health data, artificial intelligence wearable, Nigerian data protection regulation

Introduction

Artificial intelligence has been deployed in various sectors of the Nigerian economy [1]. It is used in e-commerce, by financial institutions, educational tools for children, and mobile health applications [2]. Specifically, artificial intelligence has been infused into most people's wearable technologies, including Nigerians. The market for wearable gadgets witnessed a boom as the pandemic bolstered interest in health monitoring and working from home. A record of 527 million wearable was sold in 2020 alone - the first time global wearable sales topped half a billion, with analysts forecasting the devices will overtake smartphone sales by the decade's end [3]. In the same year, the wearable technology market was valued at $27.91 billion and is expected to reach $74.03 billion by 2026. Nigeria has come under the radar as a growth market for wearable technology as it expands into the consumer technology space [4]. Using artificial intelligence (AI) for business, banking, and educational purposes lays a general background into how artificial intelligence (AI) has permeated our daily activities and the risks its use brings [5]. However, this study focuses on the health sector, the use of artificial intelligence (AI) to collect and process health data, and the data protection implications.

Artificial intelligence (AI) is being used to harness the value of health data for medical, research, and diagnosis purposes in the health sector. Specifically, during the Covid-19 pandemic, we witnessed the use of artificial intelligence (AI) for healthcare purposes [6]. For instance, Fraym, a startup, began using artificial intelligence (AI) and machine learning to help Nigeria's Center for Disease Control (CDC) to identify populations at risk of Covid-19 [7]. Also, Hadiel, an African Software as a Service (SaaS) Company, launched an artificial intelligence (AI) symptom checker that leverages health data to generate disease trends and map behavioural health patterns using data science & artificial intelligence (AI) across Nigeria and other African cities [8].

The real-life application of artificial intelligence in healthcare and its data privacy concerns is reflected in wearables such as the Apple watch series (especially series four and five) and the Fitbit. These devices collect health records, medical records and an individual's fitness activities. The way these companies handle this data raises privacy concerns. For instance, artificial intelligence (AI) analysis tool has been used to re-identify people through their wearable like fitness trackers by learning their daily footstep patterns. This links individuals to another person's location and private medical information and can bring cyber-stalkers to users' doorsteps [9]. In addition, these devices often collaborate with third-party applications, which are often not buffed with adequate privacy and data security protection or sometimes misappropriate personal data. Also, personal and sensitive health data processing is often carried out without an individual's informed consent, meaning that individuals may not know the extent of data collected, the purpose of use and the period within which the system will retain the data.

Thus, although artificial intelligence (AI) has, without doubt, facilitated the ease of carrying out a lot of our day-to-day activities, it gathers health data in ways that fall between the cracks of a weak data protection framework and may potentially violate data protection laws in Nigeria. Given this, this study examines the adequacy of the Regulation and health data collected through artificial intelligence wearable.

Methodology

This paper utilizes a qualitative research methodology to achieve its objectives. It largely relies on primary and secondary resources such as legislations, internet articles, and journal publications. The analysis of these resources was used to compile this research paper.

The Nigeria Data Protection Regulation (Regulation)

On 25 January 2019, Nigeria's National Information Technology Development Agency (NITDA) issued the Regulation to address Nigeria's data privacy and protection issues [10]. The Regulation was made to raise the standard of data protection in Nigeria to meet the European General Data Protection Regulation 2016. Before this, Nigeria had fragmented and industry-specific regulations. The Regulation boasts of being Nigeria's most comprehensive legislation protecting personal data. As subsidiary legislation, it has the force of law. It governs the control and processing of the personal data of natural persons residing in or outside Nigeria but of Nigerian descent [11]. This means that the Regulation covers all data processing transactions involving Nigerian data subjects anywhere in the world.

The introduction of the Regulation increased awareness of the importance of data protection and privacy. As a result, the Federal High Court, on 28 June 2019, in a case instituted by the *Incorporated Trustees of Paradigm Initiative for Information Technology & Anor., v National Identity Management Commission & Anor.,* [12] affirmed the data privacy rights of Nigerians and directed the National Identity Management Commission (NIMC) to improve its data privacy and security systems to avoid a breach of citizens' rights to privacy. According to the court, it is not enough to have lofty data security policies but they must be implemented.

Alongside the Regulation, the NITDA also issued the Data Protection Implementation Framework in the same year [13]. In addition, in 2020, the Guideline for the Management of Personal Data by Public Institutions in Nigeria was issued [14]. Currently pending before the National Assembly is the Data Protection Bill, 2020. The Nigeria Data Protection Regulation applies to all transactions intended to process personal data, notwithstanding how the data is being conducted or intended to be conducted regarding natural persons in Nigeria. It also applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria [15].

Legal Protection

Protection of health data and Automated Decision making

The Regulation defines personal data as any information relating to an identifiable or identified natural person, otherwise known as a data subject. It defines an identifiable natural person as a person who can be identified, directly or indirectly, by a name, an identification number, location data, and an online identifier or through their physical, genetic, mental, economic, physiological, cultural, or social identity. Although this definition of personal data does not explicitly mention health data, the Regulation mentions an individual's health data as sensitive personal data [16].

The Regulation provides that health data can be processed when the data subject gives consent, where processing is necessary for the performance of a contract to which the data subject is party or to take steps before entering into a contract; where processing is necessary for compliance with a legal obligation to which the data controller is subject; where processing is necessary to protect the vital interests of the data subject or another natural person, and when processing is necessary for the performance of a task carried out in the public interest or exercise of official public mandate vested in the controller [17]. However, unlike the Regulation, its Implementation Framework states that consent is required before sensitive data like health data can be collected or processed [18].

Similarly, the Guidelines for the Management of Personal Data by Public Institutions make consent the sole and mandatory criteria for sensitive data like health data can be collected or processed even where another legal basis for processing applies [19]. The Regulation provides that consent must be freely given, specific, informed, and an unequivocal indication of the data subject's wishes through a statement or a clear affirmative action to have their data processed [20]. The Guidelines for the Management of Personal Data by Public Institutions provide that consent be direct, unambiguous, and a distinct communication of request for consent by any electronic means or in writing, based on the circumstances of each case [21]. The Implementation Framework provides that a higher consent standard is required for processing health data, which is the data subject's explicit consent [22]. It defines explicit consent as when a data subject gives clear, documentable consent by ticking a box, signing a form or paper or sending an email [23]. Unlike the Regulation and the Implementation Framework, which are silent on exceptions, the Guidelines provide the data subject's consent as the only circumstances where health data can be processed and recognizes national security and crime prevention [24].

Under the Regulation, the processing of health data through automated means specifically relates to where AI processes data. The Regulation requires that data subjects be informed of the existence of that automated decision-making, including profiling, meaningful information about the logic involved, and the significance and foreseeable consequences of such processing must be made known to the data subject. In addition, information regarding such processing must be made available to the data subject in a structured, commonly used, and machine-readable format [25]. In processing data through any automated means, consent must be obtained before the data controller makes a decision based solely on automated processing that produces legal effects concerning or significantly affecting the data subject [26].

However, a notable shortcoming with the provisions of the Regulation on automated decision-making is that they are merely general. For example, they do not expressly make provisions where automated decision-making involves collecting and processing health data and the applicable rules.

Legal Basis and Principles Guiding Data Processing

The Regulation provides the legal basis under which personal data may be processed. Thus, where data is processed using an AI system, it must comply with one of the legal bases for processing. Consent is recognized as a legal basis for data processing. Section 2.2(a) stipulates that processing will be lawful where consent of the data subject is given. Other lawful bases for processing may be where processing is for the performance of a contract to which the data subject is a party or to take steps at the data subject's request before entering into a contract. It may also fulfil a legal obligation by the data controller to protect the data subject's vital interests and for public interest purposes.

The Regulation provides guiding principles for the collection and processing of health data. First, data must be collected and processed following the specific, legitimate, and lawful purpose consented to by the data subject. However, further processing may be done for archiving, scientific research, historical research, or statistical purposes for the public interest. Second, data must be adequate, accurate, and without prejudice to the dignity of the human person; it must be stored only for the period within which it is reasonably needed and must be protected against all foreseeable hazards and breaches such as theft, cyber-attack, dissemination, damage by rain, fire or exposure to other natural elements. Finally, data processing must be transparent at all times. Therefore, the data controller must take appropriate measures to provide the data subject with information relating to processing in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

The purpose for which data is collected and the legal basis for processing must be communicated to the data subject before collecting personal data from a data subject. Furthermore, further data processing must also be communicated to the data subject. Also, the period for storing data must be communicated to the data subject and the criteria for arriving at such a time frame. Where anyone is entrusted with the personal data of a data subject, that person is accountable for their acts and omissions regarding data processing.

Rights of Data Subjects

Under Part 3 of the Regulation, data subjects have the following exercisable rights.

1. Right to be informed

A data controller is required to take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The information shall be provided in writing or by other means, including, where appropriate, by electronic means. Where a data subject's data will be processed for additional purposes, the data subject has the right to be informed of such further processing, the purpose of use, and any other relevant information. Where the data controller is a public institution that intends to change or expand the purpose for which the data was initially collected or used, it can only do so with an express instrument from statutory authority or the data subject's consent [27]. Data subjects must also be informed about transferring personal data to a foreign country or an international organization and the appropriate safeguards for data protection in that foreign country.

2. Right to access data

A data subject has the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format. In addition, the data subject has the right to transmit data to another controller without hindrance. A data subject has the right to access and obtain personal data free [28]. However, where the requests from a data subject are unfounded or excessive because of their repetitive nature, the controller may either: charge a reasonable fee; or write a letter to the data subject stating the refusal to act on the request.

3. Right to withdraw consent, erase and rectify data

Before giving consent or collecting personal data from a data subject, the data subject must be informed of his right and method to withdraw his consent at any given time. However, the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Therefore, the controller must inform the data subject of the right to withdraw consent at any time. Furthermore, data subjects have the right to be notified by the data controller of rectifying data. The data controller must respond to this right to rectify inaccurate personal data without undue delay. A data subject also has the right to request the erasure of their data.

4. Right to object/opt-out of data processing

Under the Regulation, data subjects have the right to withdraw their consent to processing their data at any time. In addition, a data subject may object to the processing of personal data relating to them, which the data controller intends to process for marketing. The data subject also has the right to be offered the mechanism for objection to any form of data processing free of charge.

5. Right to request the deletion of data

A data subject has the right to request the controller to delete their data without delay. The controller shall delete personal data where one of these grounds apply: where personal data are no longer necessary to the purposes for

which they were collected or processed; where the data subject withdraws consent on which the processing is based; objects to the processing and there are no overriding legitimate grounds for the processing; where personal data has been unlawfully processed; and where personal data must be erased for compliance with a legal obligation in Nigeria. Under Section 3.10, the data controller who has made the personal data public is obliged to delete it and take all reasonable steps to inform controllers processing the personal data of the data subject's request.

6. Right not to be subject to automated decision-making

Before collecting personal data from a data subject, the data controller has to provide the data subject with information regarding the existence of automated decision-making, including profiling, and the significance and consequences of such processing for the data subject. The data subject has a right not to be subject to such decision-making.

7. Other rights

A data subject has other rights, including the right to complain [29], send a request to the data controller, complain to the relevant authority regarding data processing activities and know the details of the data controller [30]. Also, data subjects have the right to transmit their data from one data controller to another without hindrance from a data controller [31].

Adequacy of the Nigeria Data Protection Regulation

Under the Regulation, the definition of personal data [32] does not explicitly mention health data, neither is health data expressly defined. This shortcoming is also evident in the Data Protection Bill [33]. Similarly, although the GDPR does not define personal data to include health data, it mentions genetic data. Even though health data is not mentioned under the definition of personal data, the GDPR in Article 4(15) defines health data as personal data regarding a natural person's physical or mental health, which reveal information about their health status. Furthermore, it defines health data as a part of genetic data. Genetic data is defined as personal data regarding the inherited or acquired genetic characteristics of a natural person, giving unique information about the physiology or health of that natural person [34].

Under each of the laws, health data is recognized and protected as sensitive personal data or a particular category of data as used under the GDPR. The Regulation mentions individual health data as sensitive personal data [35]. The Data Protection Bill also defines sensitive personal data as data concerning health and improves on the shortcomings in the Regulation by including genetic data. Furthermore, the Bill under Section 2(4) provides that health data includes personal medical and health records. The GDPR, on the other hand, also classifies health and genetic data as special categories of data. The Regulation does not prohibit processing health data, but Section 26(1) of the Bill prohibits disclosing personal data on health subject to the exceptions provided under the Act. Similarly, the GDPR expressly prohibits its processing, subject to derogations [36].

For health data to be processed, exceptions are highlighted under each of the laws. Under the Regulation, health data can only be processed when the data subject gives consent, where processing is necessary for the performance of a contract to which the data subject is party or to take steps before entering into a contract; where processing is necessary for compliance with a legal obligation to which the data controller is subject; where processing is necessary to protect the vital interests of the data subject or another natural person, and when processing is necessary for the performance of a task carried out in the public interest or the exercise of official public mandate vested in the controller [37].

By extension, unlike the Regulation, its Implementation Framework provides that consent is required before sensitive data like health data can be collected or processed [38]. Similarly, the Guidelines for the Management of Personal Data by Public Institutions makes consent mandatory before sensitive data like health data can be collected or processed, even where another legal basis for processing also apply [39]. The Regulation provides that consent must be freely given, specific, informed, and an unambiguous indication of the data subject's wishes through a statement or a clear affirmative action to have data processed.

Similarly, the Guidelines for the Management of Personal Data by Public Institutions provides that consent be direct, unambiguous, and a distinct communication of request for consent by any electronic means or in writing [40]. The Implementation Framework provides that a higher consent standard is required for processing health data, which is the data subject's explicit consent. It defines explicit consent as when a data subject gives clear, documentable consent by ticking a box, signing a form or paper and sending an email [41]. Unlike the Regulation and the Implementation Framework, which are silent on exceptions, the Guidelines provides the consent of the data subject as the only circumstances where health data can be processed and recognizes instances wherein consent must be derogated from such as in cases of a health emergency, national security, and crime prevention [42].

Specifically, the Data Protection Bill provides instances where the prohibition against processing health data will be lifted. This includes where it is required to obtain legal advice, defend a legal right, administer justice, or for medical purposes undertaken by a health professional under a duty of confidentiality between the patient and health professional [43]. Similarly, the GDPR provides for specifics which includes where [44]:

a. The processing relates to personal data, which are manifestly made public by the data subject.
b. Processing is necessary for public interest purposes.

c. Processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems under a contract with a health professional and subject to the conditions and safeguards.
d. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products or medical devices.
e. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

These laws also recognize the processing of health data by automated decision making or artificial intelligence (AI). The Regulation provides that where health data is to be processed by automated means, the existence of that automated decision-making, including profiling, meaningful information about the logic involved, the significance and foreseeable consequences of such processing must be made known to the data subject. Furthermore, information regarding such processing must be made available to the data subject in a structured, commonly used, and machine-readable format [45]. However, except for applying general exceptions under Paragraph 2.5 of the Guidelines, the Regulation does not provide or recognize where health data is sought to be processed by artificial intelligence (AI). Neither does it provide any special exceptions where AI systems process health data.

The Data Protection Bill also applies to the automated processing of data. It defines automated decision-making and profiling under Section 66 as a decision based solely on automated processing, including profiling. Thus, where an automated decision is to be carried out, including profiling, the data controller must inform the data subject of the significance, the envisaged consequence of such processing, and the data subject's right to object and challenge such processing [46]. This is because a data subject has the right not to subject him or herself to a decision significantly affecting him based solely on automated data processing without considering his view. Although this provision will not apply where the decision is authorized by law to which the data controller is bound, appropriate safeguards have been put in place to protect a data subject's legitimate interests, rights, and freedoms [47]. Like the Regulation, the Bill does not provide any special provision where health data is sought to be processed by artificial intelligence (AI).

However, unlike the Regulation, its Implementation Framework, the Guidelines, the Data Protection Bill, the GDPR expressly provides for when artificial intelligence (AI) or automated decision making involves the processing or a special category of data like health data [48]. The GDPR provides that where health data is to be processed by artificial intelligence (AI), the general exceptions under Section 9(2) and Section 22(2) will not apply [49]. Health data will only be subject to such automated processing where special exceptions apply. The applicable exceptions will be when the data subject gives explicit consent or when processing is for public interest purposes, and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place [50].

This comparison shows that while under the GDPR, consent and public interest are the only conditions for processing health data by artificial intelligence (AI), the provisions of the Regulation and the Bill are silent on the conditions for health data to be processed by artificial intelligence (AI) in Nigeria.

Recommendation

It is observed that the Draft Data Protection Bill 2020 has improved upon the provisions of the Regulation. It made substantial provisions for sensitive personal data that extend to health data. The provisions show an improvement from the inadequate and scanty provisions obtainable under the Regulation. Also, the Bill improved on the provisions regarding automated decision-making or artificial intelligence (AI), allowing data subjects to obtain information on how a decision was arrived at and challenge decisions made through automated means.

Despite these remarkable additions, the Bill does not provide special conditions for collecting and processing health data using artificial intelligence (AI). Thus, while the provisions of the Regulation are sorely inadequate, the improvements made by the Bill are not sufficient. As the Bill stands, health data as a category of sensitive personal data does not have any special status where it is to be processed by an artificial intelligence (AI) system. However, it is recommended that there is a need to revisit the legal instruments to make consent and public interest reasons the only conditions for such processing to occur.

Furthermore, because the use of new technologies like artificial intelligence (AI) in processing personal data makes the need for a unified data protection law much more imperative, this study recommends the quick and timely passage of the Bill to enable comprehensive personal data protection in Nigeria.

Conclusion

This paper highlights the need for legislation to move apace with innovation to cater to challenges such as privacy issues that may arise with artificial intelligence (AI) wearables. The Nigerian government must create specific privacy rules to manage health data. Its data policies may embrace data protection by design and default, and require each data controller to integrate privacy and security into every step of its initiatives. In addition, there must be strong enforcement mechanisms to ensure that consent requirement is met, and higher threshold

for balancing legitimate interests of data controllers against that of vulnerable people. Furthermore, these legislations should be guided by strict application of data protection principles such as transparency and data minimization.

References

1. Victor Obi. 'Economic Impacts of Artificial Intelligence (AI) in Nigeria and Africa'. https://www.researchgate.net/publication/347440084_Economic_Impacts_of_Artificial_Intelligence_Ai_in_Nigeria_And_Africa accessed 25 July, 2022.
2. University of Pretoria, Artificial Intelligence for Africa: An Opportunity for Growth, Development and Democratization., 2018.
3. Pandemic Lifts Sales of Wearable Gadgets' (The Guardian Nigeria News - Nigeria and World News, 30 June 2021) <https://editor.guardian.ng/technology/technology-technology/pandemic-lifts-sales-of-wearable-gadgets/> accessed 16 May 2022.
4. 'Wearable Technology Market | 2022 - 27 | Industry Share, Size, Growth - Mordor Intelligence' <https://www.mordorintelligence.com/industry-reports/wearable-technology-market> accessed 16 May 2022.
5. Philip Boucher, Artificial Intelligence: How does it work, why does it matter, and what can we do about it*?'*. Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf accessed 25 July, 2022.
6. Francesco Picciali, Vicenzo Schiano di Cola, Fabiano Giampaolo, Salvatore Cuomo. The Role of Artificial Intelligence in Fighting the COVID. 23 Information Systems Frontiers https://link.springer.com/article/10.1007/s10796-021-10131-x#citeas accessed 25 July, 2022., 2021.
7. The Data Governments are using AI to fight covid-19 in Africa and Asia. (InsideBIGDATA, 4 July 2022) Available at https://insidebigdata.com/2020/07/04/the-data-governments-are-using-ai-to-fight-covid-19-in-africa-and-asia/ accessed 25 July, 2022.
8. Hadiel launches powerful new AI symptom checker for COVID-19 personal clinical evaluation. (2020, 15 April). Businessday NG. Retrieved 15 April, 2021, from https://businessday.ng/coronavirus/article/hadiel-launches-powerful-new-ai-symptom-checker-for-covid-19-personal-clinical-evaluation/
9. Richie Koch. Fitness apps are a risk to your privacy, here's why. (*ProtonVPN Blog*, 31 October, 2019). ProtonVPN Blog. https://protonvpn.com/blog/fitness-apps-are-good-for-your-health-but-often-bad-for-your-privacy/ accessed 25 July, 2022.
10. National Information Technology Development Agency Act 2007, section 6.
11. Nigeria Data Protection Regulation 2019, section 1.2 (b).
12. Andersen Tax Legal Practice. 'Nigeria: Federal High Court Affirms the Data Privacy Rights of Nigerian Citizens' (*Mondaq*, 3 September 2019) www.mondaq.com/nigeria/privacy-protection/841960/federal-high-court-affirms-the-data-privacy-rights-of-nigerian-citizens accessed 26 July, 2022.
13. Nigeria Information Technology Development Agency (NITDA), Nigeria Data Protection Regulation 2019: Implementation Framework. July, 2020. https://taxtech.com.ng/download/ Nigeria%20Data% 20Protection%20Regulation%202019%20Implementation%20Framework.pdf accessed 26 July, 2022.
14. Hadiza Umar, 'Press Release- NITDA issues Guidelines for the Management of Personal Data by Public Institutions in Nigeria' (Abuja, 4 March 2020) https://nitda.gov.ng/press-release-nitda-issues-guidelines-for-the-management-of-personal-data-by-public-institutions-in-nigeria/
15. Nigeria Data Protection Regulation 2019, article 1(2) (a) & (b).
16. Nigeria Data Protection Regulation 2019, article 1.3 (iv) (xix) (xxv).
17. Nigeria Data Protection Regulation 2019, article 2.2.
18. Data Protection Implementation Framework 2019, paragraph 5.3.1(b)
19. Guidelines for the Management of Personal Data by Public Institutions 2020, article 2.3(b).
20. Nigeria Data Protection Regulation 2019, article 1.3(iii).
21. Guidelines for the Management of Personal Data by Public Institutions 2020, article 2.4.
22. Data Protection Implementation Framework 2019, article 5.3.2
23. Data Protection Implementation Framework 2019, paragraph 5.4 (a).
24. Guidelines for the Management of Personal Data by Public Institutions 2020, article 2.5.
25. Nigeria Data Protection Regulation 2019, article 3.1(7) (l) & 14) (c)
26. Data Protection Implementation Framework 2019; Article 2.3(f); Guidelines for the Management of Personal Data by Public Institutions 2020, paras. 5.3.1(f), 5.4(a).
27. Guidelines for the Management of Personal Data by Public Institutions 2020, article 2.2(h)
28. Nigeria Data Protection Regulation 2019, article 3.1(5).
29. Nigeria Data Protection Regulation 2019, article 2.2.
30. Nigeria Data Protection Regulation 2019, article 3.1(7) (j) (a).
31. Nigeria Data Protection Regulation 2019, article 3.1(7) (h).
32. Nigeria Data Protection Regulation 2019, article 1.3(xix).
33. Data Protection Bill 2020, section 66.
34. General Data Protection Regulation 2016, article 4(1), 4(4) & 4(13).
35. Nigeria Data Protection Regulation 2019, article 1.3(xxv).
36. General Data Protection Regulation 2016, article 9 (1) (2).

37. Nigeria Data Protection Regulation 2019, article 2.2.
38. Guidelines for the Management of Personal Data by Public Institutions 2020; Paragraph 5.3.1(b) Data Protection Implementation Framework 2019, article 2.3(b).
39. Guidelines for the Management of Personal Data by Public Institutions 2020; Paragraph 5.1(b) Data Protection Implementation Framework 2019, article 2.3(b).
40. Guidelines for the Management of Personal Data by Public Institutions 2020, article 2.4
41. Data Protection Implementation Framework 2019, paragraph 5.3.2. & 5.4(a).
42. Guidelines for the Management of Personal Data by Public Institutions 2020, article 2.5.
43. Data Protection Bill 2020, section 26(6).
44. General Data Protection Regulation 2016, article 9(2) (e) (g) (h) (i) (j).
45. Nigeria Data Protection Regulation 2019, article 3.1(7) (l). & 3.1(14) (c).
46. Data Protection Bill 2020, section 6(3) (h).
47. Data Protection Bill 2020, section 19 (1) (2).
48. General Data Protection Regulation 2016, article 9(1).
49. General Data Protection Regulation 2016, article 22(4). The exceptions are when processing is necessary for a contract or the performance of a contract between the controller and the data subject, where processing is authorized under the European Union or member state law and where the data subject explicitly consents to processing
50. General Data Protection Regulation 2016, article 9(1) (a) (g).