Introduction

The outbreak of the COVID-19 pandemic has had (and continues to have) varying impacts on sectors of the global economy and the practice of law falls squarely within this space. Various fields of law pertaining to contractual relationships,[1] employment,[2] trade,[3] data protection, etc. have been expressly impacted by the COVID-19 pandemic. This article focuses on the impact of the COVID-19 pandemic from a data protection perspective. Personal data processing is a very powerful tool in the prevention and control of the COVID-19 pandemic. This is because activities such as the collection of travel data,[4] measurement of body temperatures,[5] identification and tracking of infected persons, etc. which are necessary for the control of the pandemic all amount to personal data processing activities. In fact, sensitive personal data[6] particularly health data is processed in a lot of cases.

The aim of the article is to examine the legal requirements which ought to be complied with in processing personal data for purposes relating to the COVID-19 pandemic across the African continent. To achieve this purpose, specific references will be made to the data protection laws of Nigeria, Kenya and the African Union (AU). The Nigerian Data Protection Regulation (NDPR) is the most comprehensive legal instrument regulating data protection law in Nigeria and will be the base Nigerian data protection legislation to be considered in this article.[7] In Kenya, the Kenyan data protection Act (KDPA)[8] came into force in 2019 and is the extant law on data protection in Kenya. The KDPA will also be referenced in this article as may be appropriate. The African Union Convention on Cybersecurity and Personal Data Protection (AUCCPDP)[9] will also be referenced as the relevant AU law for the purpose of this article. Using the NDPR, the KDPA and the AUCCPDP as legislative references, this article seeks to highlight the specific requirements of data protection law which ought to be complied with as well as instances of specific applicability in a COVID-19 personal data processing scenario.

IMPORTANT CONSIDERATIONS FOR PROCESSING PERSONAL DATA IN RELATION TO THE COVID-19 PANDEMIC

1. **Legal basis**

It is important that government agencies and health personnel collecting data during this pandemic are doing so with a ‘legal basis’ or a reason justified by law. This is otherwise known as the lawfulness principle. The use of a justifiable legal basis is a very fundamental principle in any processing activity including in the processing of personal data in relation

to the COVID-19 pandemic. Section 2.2 of the NDPR, sections 25(b) and 30 of the KDPA and Article 13 of the AUCCPDP provide variously for the lawfulness principle. Depending on whether the data controller[10] is in the public or private sector, different legal bases can be used for processing COVID-19 related personal data. Specific instances where various legal bases may be used are considered below:

Compliance with a legal obligation:[11] In this case, the processing of personal data during COVID-19 is justified where a specific law mandates such processing activity. For example, the Nigerian presidency issued the COVID-19 Regulations 2020 pursuant to Sections 2, 3 and 4 of the Quarantine Act.[12] The Regulations have been used as the legal justification for enforcing a stay-at-home order for members of the public in selected Nigerian states. According to the Regulations issued by the Nigerian presidency, this lockdown order is to "identify, trace and isolate individuals that have come in contact with confirmed cases". Such 'identification and tracing' of persons will inevitably involve the processing of personal data. This processing of personal data may be justifiable on the legal basis of complying with the legal obligations imposed under the Regulations.

Public interest:[13] Personal data may also be processed as part of efforts to curb the spread of the coronavirus when it is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the data controller.[14] This legal basis is typically reserved for use by public authorities acting pursuant to an existing law or by private entities authorized to act under such laws. The definition of what may amount to public interest may vary from country to country. For example, the Kenyan authorities have been tracking the mobile phones of persons suspected of being infected with coronavirus as part of their efforts to enforce a mandatory 14-day isolation period.[15] This tracking involves the collection and processing of various categories of personal data. In this case, public interest can be used as the legal basis for this processing activity because section 46 (2) (a) of the KDPA provides that personal data relating to health may be processed where it is necessary for reasons of public interest in the area of public health. This means that Kenyan authorities are authorized by law to process the personal data of Kenyan citizens on the basis of public interest so as to curb the spread of a pandemic.

Vital interest: Personal data may also be processed when it is necessary for the protection of the vital interests of the data subject[16] or of another natural person. The use of this legal basis is usually tied to the public interest legal basis particularly in relation to pandemics and their development and when there is a humanitarian emergency.[17] NITDA has suggested that the processing of personal data by the Nigerian government to contain the COVID-19 pandemic is compliant with the NDPR as it is being done to protect the vital interests of data subjects.[18] According to NITDA, this position is further reinforced by

section 45 of the Nigerian constitution which limits the right to privacy provided for in section 37 of the constitution.[19].

Legitimate interest:[20] Beyond the processing activities pursued by government operatives, various private sector participants and businesses have also been involved in the processing of personal data in relation to the COVID-19 pandemic. The legitimate interest of the controller may be a justifiable legal basis for processing personal data in such instances. While the parameters of what constitutes a legitimate interest is flexible depending on the facts of any relevant case, data controllers seeking to process personal data under this basis may be required to fulfil the three elements necessary for a lawful application of this basis: identifying a legitimate interest which they or a third party may pursue, demonstrating that the intended processing of the data subject's personal data is necessary to achieve the legitimate interest, and balancing the legitimate interest against the data subject's interests, rights and freedoms.[21] For instance, it is expected that employers will exercise their legitimate interest to prevent the spread of the pandemic among its workforce. The exercise of this legitimate interest may involve the collection and processing of employee personal data including their health and travel data. In exercising this legitimate interest, one of the most important considerations, as noted above, is conducting a balancing test aimed at weighing the interests of the data controller (in this case, the employer) against the rights and natural freedoms of the data subjects (i.e. the employees). This legal basis will not be applicable where the rights and freedoms of the data subjects outweighs the legitimate interest of the controller.[22]

Consent: The consent of the data subject is another legal basis that may be used for the processing of personal data in connection with the covid-19 pandemic. A data subject's consent to the collection and processing of his or her personal data ought to be freely given,[23] specific,[24] and informed.[25] Data subjects should also be able to withdraw their consent as easily as it was for them to provide it.[26] If these conditions are met, data controllers, particularly those in the private sector, can, subject to their compliance with other aspects of the applicable data protection law, process the personal data of data subjects in connection with the COVID-19 pandemic. For example, tying consent to collect and process employee personal data with restrictions that affect an employee's ability to work or otherwise be part of a company will not be determined as freely given. Where clear reasons for data collection are not given to the data subject, any consent granted may not qualify as being as informed. Data controllers must ensure that in collecting consent from data subjects, they comply with the requirements of the relevant laws in order to make such consent lawful.

Fairness and Transparency:[27] The fairness principle requires that data subjects be

made aware of the potential risks that may arise from the nature of the processing activity.[28] The fairness principle also requires that the data subject should be able to anticipate in what circumstances he would retain or part with his/her privacy in a processing operation.[29] The transparency principle on the other hand requires that personal data is transparently processed with data subjects being provided with all necessary information pertaining to the relevant processing operation.[30] To be compliant, adequate information about the processing activity (particularly through privacy policies) should be provided to data subjects and in appropriate cases, the said privacy policies should be updated.

Purpose limitation: The principle of purpose limitation requires that the processing of personal data be done for a specific, well defined purpose and only for additional purposes that are compatible with the original purpose.[31] Personal data collected for COVID-19 related processing activities should be used only for the purpose for which they have been collected.[32] The only derogation(s) to this requirement should be in accordance with clearly defined provisions of existing data protection laws.[33] One of the major concerns with the collection of large volumes of big data[34] for COVID-19 related purposes is the use of such data for purposes totally unrelated to the prevention of the pandemic. For instance, some intrusive applications have been introduced to help curb the COVID-19 pandemic.[35] Some of these applications collect personal data obtained which may be retained even after the COVID-19 crisis has abated, and could possibly be used for surveillance purposes against the initial intention and expectation of the data subject. Any such use will violate the principle of purpose limitation principle provided for under the data protection laws, where such surveillance neither qualifies nor is connected with the COVID-19 public health pandemic. In specific relation to the isolation period in force in Kenya, data controllers (i.e. the Kenyan authorities) are bound under the KDPA to collect, store and use personal data for a purpose which is lawful, specific and explicitly defined.[36]

Data Minimization: This principle requires that only the minimum amount of personal data needed to process personal data for a particular purpose should be collected. The data protection laws provide that data collection be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed.[37] With regard to COVID-19, the purpose of any data collection must be clearly outlined and only the categories of personal data necessary for executing such purpose must be collected.

Accuracy: This principle requires that a data controller holding personal information ensure that the information is accurate and up to date before it is used.[38] In relation to the COVID-19 pandemic, data controllers must always ensure the accuracy of personal data being processed. Changing states in health data collected during the pendency of the

COVID-19 pandemic must be updated and may only be used when controllers have confirmed the accuracy of such information.

Data retention: This principle requires that personal data should only be retained in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.[39] In a COVID-19 scenario, the retention period for relevant personal data may be dependent on the strategies being deployed for the prevention and control of the virus such as collection for information for vaccine manufacture, monitoring of patients who have recovered etc. Where possible, the personal data of relevant data subjects can be anonymized[40] where it is still useful in an aggregated format. Where deployed, such anonymization must not lead back to the identification of data subjects.

Security of data: It is necessary to maintain the security of personal data so as to preserve its integrity and confidentiality.[41] This principle requires that appropriate measures are implemented when processing personal data to protect against accidental, unauthorized, or unlawful use, modification, disclosure, loss destruction or damage.[42] Various technical and organizational measures such as encryption,[43] pseudonymization[44] etc. are usually used to achieve this purpose. In some African countries, personal data in relation to the COVID-19 pandemic is collected through self-reporting forms[45] which could pose a data protection risk as such paper forms can be easily lost or stolen leading to its misuse by persons ordinarily without a legal access. In such cases, a framework for the transfer of the personal data from the sheets of paper to more secure databases must be designed and put in place.

Accountability: This requires that controllers demonstrate compliance with relevant data protection principles. Controllers should be able to prove that they have complied with applicable data protection principles. This principle is very germane to the lawful processing of personal data in relation to the COVID-19 pandemic. The processing of personal data to curb the COVID-19 pandemic may involve the use of various out-of-the-box and in most cases, intrusive solutions.[46] Complying with the accountability principle will therefore require controllers to document how they have complied with the applicable data protection laws. Data protection supervisory authorities will also be able to review processing activities with the aim of protecting the privacy rights of data subjects under the data protection laws. This principle serves as a silent watchdog which is capable of preventing controllers from processing personal data unlawfully.

In processing personal data in relation to the COVID-19 pandemic, adhering to the above principles (in accordance with the respective data protection laws across the continent) will

help in achieving compliance with data protection law.

THE USE OF TECHNOLOGY, (BIG) DATA COLLECTION AND DATA PROTECTION ACROSS THE CONTINENT

In Africa, various measures are being adopted by various national governments with the aim of preventing the spread of the COVID-19 pandemic. One such measure that is being adopted in Africa (and also globally)[47] is the adoption of technology for the purpose of tracing and tracking persons who are suspected of having come in contact with the pandemic. In Kenya, an app has been developed which identifies covid-19 hotspots, informs users about whether they have been in contact with infected persons, helps the authorities in tracking infected persons etc.[48] To provide these services, this app collects the data of its users while also using GPS tracking[49] for locating persons at risk.

Furthermore, the Kenyan government has announced plans to launch a contact tracing app for public transportation with the intention of obtaining of critical contact data which could help trace the movements of confirmed or suspected covid-19 cases. In South Africa, telecommunication companies have agreed to give government the location data of their subscribers so as to help combat the covid-19 pandemic.[50] At the time of writing this article, Uganda is debating whether or not to use information from the immigration department and telecommunication companies to locate individuals suspected to have contracted the covid-19 virus.[51]

To perform the functions above, apps will collect both personal and special categories of data which falls within the scope of data protection law. These big data and apps being used to curb the spread of the COVID-19 pandemic, also require compliance with the principles of data protection law above, particularly the use of a justifiable legal basis, provision of adequate information to data subjects, using the minimum amount of data necessary for the purposes of the apps, limiting the use of the data for the purpose for which they were initially collected etc. It is important to note that the necessity of curbing the spread of the COVID-19 pandemic is not a justifiable reason to violate the principles of data protection law. In the use of apps and big data to curb the pandemic, it is necessary to incorporate the principle of privacy by design[52] so as to ensure that potential risks are identified with appropriate security measures put in place at the design phase of the apps. More specifically, features such as contact tracing should be based on the explicit consent of the users while strict compliance with the transparency principle must always be adhered to.[53]

Conclusion

As stated by Amnesty International,[54] the COVID-19 pandemic does not justify the derogation from the right to data protection. As African countries work to manage this public health crisis, it will serve as a learning curve for most African countries particularly from a data protection standpoint. This occurrence will also help determine what amounts to a legally admissible activity and the extent of the government's authority during a pandemic such as this. Even though there are constitutional grounds for derogating from the right to data protection,[55] it is still necessary to comply with the principles of data protection listed earlier in this article.

---

* Emmanuel Salami (Privacy Manager, Here Technologies) and Nnanke Williams (Senior Consultant, Brooks & Knights Legal Consultants).

[1] Andrew White, Victoria Hobbs, Loiuse Lanzkron, Force majeure, and beyond: Other contractual and related issues on COVID-19 March 19, 2020. Available at: https://www.twobirds.com/en/news/articles/2020/global/force-majeure-and-beyond-other-contractual-and-related-issues-on-covid-19 accessed 13/04/2020.

[2] International Labor Organization, COVID-19 causes devastating losses in working hours and employment, April 7 2020. Available at: https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_740893/lang–en/index.htm

accessed 13/04/2020.

[3] World Trade Organization, Trade set to plunge as COVID-19 pandemic upends global economy Available at: https://www.wto.org/english/news_e/pres20_e/pr855_e.htm accessed 13/04/2020

[4] Travel data is being collected by both public and private sector actors to determine which individuals have visited countries designated as covid-19 high risk areas.

[5] To determine persons who are showing symptoms of the covid-19.

[6] Sensitive categories of data are those categories of personal data which, by their nature, may pose a risk to the data subjects when processed and need enhanced protection. European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2018, page 117. Also available at:

https:andandfra.europa.euandsitesanddefaultandfilesandfra_uploadsandfra-coe-edps-2018-handbook-data-protection_en.pdf Accessed 13/04/2020

[7] The National Information Technology Development Agency (NITDA), the body charged with the enforcement of the NDPR, has implied that the NDPR continues to apply even during the processing of personal data in relation to the COVID-19 pandemic. See – Na'ankwat Dariem, Collection of COVID-19 data aligns with NDPR guidelines – NITDA (Voice of Nigeria, March 29, 2020). Available at: https://www.von.gov.ng/collection-of-covid-19-data-aligns-with-ndpr-guidelines-nitda/ accessed 4/4/2020.

[8] Kenya Gazette Supplement No. 181 (Acts No. 24).

[9] The African Union Convention on Cybersecurity and Personal Data Protection 2020 embodies the commitment of African Union member states towards cybersecurity and data protection. There are currently 5 signatories to the convention. Please see: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection accessed 13/04/2020.

[10] A Data Controller is a natural or legal person who determines the purposes and the means of processing data. Data Controllers generally exercise control over and are responsible for the processing of data. See Handbook on European Data Protection Law, supra at note 6, p.101. See also sections 1.3(x) of the NDPR, 2 of the KDPA and Article 1 of the AUCCPDP.

[11] Processing of personal data is allowable when it is done in compliance with a legal obligation that the data controller is subject to. Handbook on European Data Protection Law, supra at note 6, p.151. See also sections 2.2(c) of the NDPR, 30(1)(b)(ii) of the KDPA and Article 30, Principle 1(a) of the AUCCPDP.

[12] Chapter Q2 Laws of the Federation of Nigeria (LFN) 2004.

[13] Sections 2.2(e) of the NDPR, 30(1)(b)(iv) of the KDPA and Article 30, Principle 1(b) of the AUCCPDP.

[14] Handbook on European Data Protection Law, page 153.

[15] Dickens Olewe, *Coronavirus in Africa: Emergency Laws v. Individual Rights*, (BBC News, 9 April 2020), available at https://www.bbc.com/news/world-africa-52214740, accessed on 14 April 2020.

[16] A data subject is any identified or identifiable natural person who is the subject of personal data. See sections 1.3(xiv) of the NDPR, 2 of the KDPA and Article 1 of the AUCCPDP.

[17] European Union Agency for Fundamental Rights and Council of Europe (2018), Page 152.

[18] ITEdge News, *COVID-19 Data Collection Complies with NDPR, Says NITDA*, (ITEdge News, 30 March 2020), available at http://itedgenews.ng/2020/03/30/covid-19-data-collection-complies-with-ndpr-says-nitda/, accessed on 14 April 2020.

[19] *Id*. It is also worth mentioning that Nigerian courts have interpreted the right to privacy to include the right to data protection. See: MTN Nigeria Communication Ltd v. Barr. Godfrey Nya Eneye, Appeal No: CA/A/689/2013 (Unreported)

[20] Section 30(1)(b)(vii) of the KDPA.

[21] Data Protection Commission, *Guidance Note: Legal Bases for Processing Personal Data*, (December 2018), p.21, available at https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance%20on%20Legal%20Bases_Dec19_1.pdf

[22] See also Opinion of the Article 29 Working Party: Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/and46/EC.

[23] Each of the NDPR, KDPA and AUCCPDP define consent as an assent to collection and processing of personal data by the data subject which is freely given, specific and informed. See sections 1.3(iii) of the NDPR, 2 of the KDPA and Article 1 of the AUCCPDP.

[24] *Id*.

[25] *Id*.

[26] Sections 2.3(2)(c) of the NDPR, and 32(2) of the KDPA.

[27] Please see Article 13, principles 2 and 5 of the AUCCPDP, and section 25(b) of the KDPA.

[28] *Id*.

[29] Peter Carey, Data Protection: A Practical Guide to UK and EU law, Oxford University Press, 2018. Page 44-46.

[30]Please see Article 13, principle 5 of the AUCCPDP, and section 25(b) of the KDPA.

[31] Article 29 Data Protection Working Party, Opinion 03and2013 on purpose limitation, (WP 203, April 2013).

[32] Sections 2.1(1)(a) of the NDPR, 25(c) of the KDPA and Article 13, Principle 3(a) of the AUCCPDP.

[33] For example, section 45 of the Nigerian constitution limits the right to privacy in favour of the provisions of any law enacted to protect the public defence, safety, order, morality or health. Any collection and processing of data under the Nigerian COVID-19 Regulations 2020 but used for defence purposes may still be allowed.

[34] Big data refers to the growing technological ability to collect, process and extract new and predictive knowledge from great volume, velocity, and variety of data.. See Handbook on European Data Protection Law, supra at note 6, p.350.

[35] Apps such as CoronApp, Home Quarantine and Track Virus have been developed for apps stores in countries such as Colombia, Poland and Israel, among others, to track location and assist in contact tracing efforts. Apple and Google are partnering to develop contact tracing technology for mobile phones operating their software. Apple Newsroom, *Apple and Google Partner on COVID-19 Contact Tracing Technology*, (Apple, 10 April 2020), available at https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/, accessed on 14 April 2020.

[36] Section 28(3) of the KDPA.

[37] Sections 2.1(1)(b) of the NDPR, 25(d) of the KDPA and Article 13, Principle 3(b) of the AUCCPDP.

[38] Sections 2.1(1)(b) of the NDPR, 25(f) of the KDPA and Article 13, Principle 4 of the AUCCPDP.

[39] Sections 2.1(1)(c) of the NDPR, 25(g) of the KDPA and Article 13, Principle 3(c), (d) of the AUCCPDP.

[40] Anonymized data is data that does not lead to the identification of natural persons and falls outside the purview of data protection law as a result. For further readings, see: Stalla-Bourdillon, Sophie and Knight, Alison, Anonymous Data v. Personal Data — A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data (March 6, 2017). Wisconsin International Law Journal, 2017. Available at SSRN: https://ssrn.com/abstract=2927945

[41] Sections 2.1(1)(d) of the NDPR, 29(f) of the KDPA and Article 13, Principle 6 of the AUCCPDP.

[42] See Handbook on European Data Protection Law, supra at note 6, p.131.

[43] Encryption involves the breakage of all links identifying a data subject. *Id*.

[44] Pseudonymization involves the replacing of attributes in personal data which make it possible to identify the data subject, with a pseudonym. *Id*.

[45] There is the proof of the use of self reporting forms at Nigerian airports. See – World Health Organization, Close Marking COVID-19 – WHO supports screening activities at Lagos International airport arrivals, March 11, 2020. Available at: https://www.afro.who.int/news/close-marking-covid19-who-supports-screening-activities-lagos-international-airport-arrivals accessed 15/04/2020.

[46] An example of this is the house to house search being carried out by the Lagos state government with the aim of identifying infected persons in their homes. See: Olasunkanmi, COVID-19: Lagos commences house to house check for infected persons, (LASG website, April 10, 2020). Available at: https://lagosstate.gov.ng/blog/2020/04/10/covid-19-lagos-commences-house-to-house-search-for-infected-persons/ accessed 15/04/2020

[47] Iran, Israel, Italy, Singapore, South Korea, Taiwan, are among the countries using geo-location technology reliant on data from tech platforms and telecom companies in order to contain the spread of the Covid-19. Please see Gabrielle Hermier, *The Most Privacy Invasive COVID-19 Apps*, (Surfshark, 1 April 2020), available at https://surfshark.com/blog/privacy-invasive-covid-19-apps. accessed on 14 April 2020.

[48] KTN News Kenya, Kenyan Mobile App to track COVID-19 infections, March 26, 2020. Available at: https://www.youtube.com/watch?v=yOpCAnWKCEQ accessed 11/04/2020.

[49] GPS tracking is used to identify the location of identified targets. For further reading,

see: Bellovin, Steven M. and Hutchins, Renee M. and Jebara, Tony and Zimmeck, Sebastian, When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning (2014). NYU Journal of Law & Liberty, Vol. 8; U of Maryland Legal Studies Research Paper No. 2013-51, page 563. Available at SSRN: https://ssrn.com/abstract=2320019 or http://dx.doi.org/10.2139/ssrn.2320019 accessed 15/04/2020.

[50] Collaboration on International ICT Policy for East and Southern Africa (CIPESA), COVID-19 in Africa: When is Surveillance Necessary and Proportionate?, (CIPESA website, March 27, 2020). Available at: https://cipesa.org/2020/03/covid-19-in-africa-when-is-surveillance-necessary-and-proportionate/ accessed 15/04/2020.

[51] Ibid.

[52] Ann Cavoukian, Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, (IAPP resource centre). Available at: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ accessed 15/04/2020.

[53] European Commission, Joint European Roadmap towards COVID-19 containment measures, (European Commission website, 15/04/2020. Available at: https://ec.europa.eu/info/files/european-roadmap-lifting-coronavirus-containment-measures_en accessed 15/04/2020.

[54] Amnesty International, *COVID-19, Surveillance and the Threat to Your Rights*, 3 April 2020, available at https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/, accessed on 14 April 2020.

[55] In Nigeria for example, section 45 of the Nigerian constitution limits the right to privacy in favour of the provisions of any law enacted to protect the public defence, safety, order, morality or health.