Data collection in the health and education sectors: An African perspective

AFRICA CONNECTED

27 April 2021

By: Adewumi Salami, DLA Piper Africa, Nigeria (Olajide Oyewole LLP)

Many African countries are still grappling with the impact of the lockdown initiatives caused by COVID-19.[1] Adapting to the health and safety protocols across Africa has meant a significant increase in the sheer volume of data being processed, particularly in the health and education sectors.

Impact of COVID-19 on service offerings and data processing across health and education sectors in Africa

In Uganda, the Ministry of Education and Sports took measures to encourage and implement learning from home.[2] Some educational programs were broadcast on television and radio stations, and academic materials were printed and circulated. The phased reopening of schools started in October 2020 and is expected to continue in March 2021. In the health sector, the Ugandan government approved more laboratories to conduct COVID-19 testing at border entry points. Digital platforms for testing, tracking and reporting on COVID-19 were adopted by deploying an integrated Electronic Integrated Disease Surveillance Response (eIDSR) tracking system[3] at the border districts to control the spread of the virus.

In Senegal, the government closed schools in March 2020 and educational institutions were advised to set up distance education systems. Some television stations also broadcast classes for students every day. Only private schools were able to set up online classes. The Senegalese health sector also witnessed an upsurge in gathering of data as a result of the pandemic.

In South Africa, online classes were primarily available in private schools (as opposed to public schools). In the health sector, there has been a significant increase in data gathering due to the pandemic.

In Ghana, a few private pre-tertiary and public tertiary institutions with the requisite facilities organized online classes for students. These schools were, however, in the minority as public schools outnumber private schools. The Ghana Education Service rolled out Ghana Learning TV which is a 24-hour televised classroom channel with content covering kindergarten, primary school, junior high school and senior high school lessons. The health sector also witnessed an increase in personal data collection, particularly COVID-19 related data.

In Nigeria, the lockdown and social distancing regulations issued by the federal government meant that schools had to be closed and physical classes could not be held; however, some private schools were able to adopt online classes to continue teaching students. Different education management and online platforms were adopted and a wide range of personal data was collected and processed to actualize this. Public schools, on the other hand, were to some extent reliant on radio, television and tablets loaded with educational material. In the health sector, institutions like laboratories

and hospitals have had to adopt the use of different testing and monitoring applications in their service delivery to patients. The deployment of technology has involved gathering a significant amount of personal/health data of the patients/data subjects.

Data security

There is no doubt that the pandemic has adversely affected education and health services in Africa and elsewhere. The accelerated digitization has led to increased collection of data in all its ramifications. All of these have raised privacy and data protection concerns due to the sheer volume of personal data being collected. This can be challenging for organizations, as it requires successful data integration, efficient analysis as well as ensuring and prioritizing privacy. Digital transformation and COVID-19-inspired innovation have created new security risks with respect to sensitive personal data that organizations in these sectors mostly deal with. Some of the major risks and concerns include human error, malware, phishing, loss of data, cyber-attacks, hacks and data breaches.

In today's world, data security is a vital issue and a major challenge for every organization, underlined by stricter regulations and severe consequences in the case of data loss. In fact, data protection is moving from being an IT task to a strategic business imperative. More than ever, organizations in the identified sectors need to consider the security of the data they collect, store and share as a whole, and must have a strategy that ensures their data and the data subjects' data are safe.

The security strategy should include regular training for employees on digital technologies and cybersecurity, conducting regular infrastructure testing that help uncover potential vulnerabilities, using applications and devices that have built-in security, integrating security systems and choosing the right security software. Knowledge of the applicable laws and regulations and compliance are also critical. Besides external threats like phishing attacks, organizations should also guard their sensitive data against insider threats.[4]

Another aspect of digital transformation that must align with data protection is the need to monitor and track data usage within an organization. It is essential to know where each piece of data sits, and who can access it, as well as to tag and track its lineage to understand its usage. This is vital for fulfilling data protection legislation requirements such as subject access requests, but also to locate and move data in accordance with the law.[5]

Lawful data processing

To minimize risks and exposure to cyberattacks, it is imperative that organizations in the health and education sectors adhere strictly to the key principles of lawful data processing. These are:

- Lawfulness, fairness and transparency: ie processing data lawfully and in a transparent manner in relation to the data subject.
- Purpose limitation: data is to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimization: data to be collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accuracy: data is to be accurate and kept up to date.
- Storage limitation: data is to be stored in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Integrity and confidentiality: data is to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.
- Accountability: data controllers should be responsible and able to demonstrate compliance with all relevant data protection laws.

Organizations that process personal data should comply with the security strategy outlined above and ensure personal data is automatically protected in any IT system or business model (privacy by design).

Key regulations and enforcement of data protection laws in Africa

African countries like Morocco and Ghana have had data protection laws since 2009 and 2012 respectively. Other African countries have followed this trend and introduced laws to protect personal data of citizens and regulate how organizations

collect, process and store data. Of the 54 countries in Africa, 27 currently have data protection legislation, 9 have draft data protection legislation and 13 have no legislation.[6] The African Union in 2014 released the African Union Convention on Cyber Security and Personal Data Protection.[7] The convention set a strong intention for the protection of personal data and online security on the continent. However, only five countries have ratified the convention. There are efforts to revive this convention and have more countries ratify it.

It is important to note that harmonizing the data protection statutory and regulatory framework in Africa is still on the agenda of regional organizations and some African states. In addition to protecting citizens' privacy, having a uniform framework is seen as an opportunity to promote the continent's development by allowing free flow of data within Africa, encouraging data transfer from other continents to Africa, thus boosting the use of African-based datacenters, outsourcing services, e-government and other essential tech services. This is even more necessary now that the Africa Continental Free Trade Area (AfCFTA) is effective as its primary objective is to create a single market for goods and services, establish a liberalized market for goods and services and aid the movement of capital and people in Africa.

Recommendations

The sheer volume of data processed in education and health sectors across Africa means that organizations in these sectors must practice good data governance. This refers to the establishment of detailed processes and procedures to manage, use, and protect the data processed by organizations. It helps to make compliance standards easier to maintain, protects against cyberattacks and security breaches, allows for better communication and decision-making, lightens the IT team's data management duties and spreads responsibility throughout the organization. Thus, it is critical for organizations in these sectors to be proactive in compliance with the laws and practice of good data governance.

DLA Piper Africa is a Swiss verein whose members are comprised of independent law firms in Africa working with DLA Piper.

---

[1] A recent Mckinsey report points to emerging evidence that the stress and isolation of online learning is contributing to mental health issues among young people.
[2] COVID-19 Education Sector Response Guidelines, Continuity of learning during COVID-19 lockdown.
[3] This system tracks and captures real-time data and monitoring using an application that is downloaded to drivers' mobile phones (DHIS2 Community).
[4] Data Protection In The Age Of Digital Transformation.
[5] Factoring data protection into a digital transformation strategy.
[6] Please visit DLA Piper data protection website for more information on data protection laws in Africa.
[7] Popularly referred to as the Malabo Convention of 2014.