DATA PROTECTION & PRIVACY DURING COVID-19 PANDEMIC

Client Alert

TRIPLEOKLAW ADVOCATES

MAY 2020

THE KENYAN GOVERNMENT, SURVEILLANCE, RESIDENTS AND CHALLENGES FOR THE NEW WORKPLACE

Key Contacts

Catherine Kariuki
Email: ckariuki@tripleoklaw.com

Janet Othero
Email: jothero@tripleoklaw.com

Assisting Authors

Sherry Bor

Joyanne Njau

Amrit Singh

Introduction

The Constitution under Article 31 guarantees every Kenyan citizen of the right to Privacy.
This includes the right not to have:
a) their person, home or property searched;
b) their possessions seized;
c) information relating to their family or private affairs unnecessarily required or revealed; or
d) the privacy of their communications infringed

Article 24 of the Constitution allows for limitation of some of the guaranteed rights and freedoms in certain instances provided it is carried out by way of law and some considerations are made.

In 2019, Kenya joined the wave of many African governments passing national data protection laws to protect its resident's personal information. Anyone processing personal information in Kenya is expected to adhere to the provisions of the Data Protection Act, 2019. Our analysis of the Data protection Act can be read here.

Initially, there were challenges relating to interpretation of some provisions in respect of the extent of its applicability to public bodies. For instance, clarity was sought regarding processing of personal information by public bodies such as the civil registries. While the data commissioner's office has not been set up to issue regular interpretations and guidelines, the draft Data Protection (civil registration) regulations 2020 have been released by the Ministry of ICT to the public for comments and is expected to address the grey areas relating to public bodies that regularly process personal information like the immigration office, the registrar of persons, the registrar of births and deaths and registrar of marriages. Our submitted comments on the bill can be found here.

The global outlook in use of technology to combat the spread of COVID-19

The highly infectious nature of the COVID-19 pandemic has resulted in various governments adopting innovative technological solutions focused on Big Data and Bluetooth tracing to effectively track and contain the spread of the disease.

China, from the onset of the pandemic, had adapted their highly integrated nationwide CC-TV surveillance system to ensure social distancing and lockdown measures are adhered to. Apple and Google have collaborated to design an interoperable application platform that will allow various tracking applications to operate on both iOS and Android devices. E.U member states such as Germany and Switzerland have adopted contact tracing applications developed around Decentralized Privacy-Preserving Proximity Tracing (DP-3T), which is an open-source protocol developed in response to the COVID-19 pandemic to facilitate digital contact tracing of infected participants.

The Indian government has adopted a controversial contact tracing application named 'Aarogya Setu' or 'Bridge to Health', which collects the users' travel history, COVID-19 symptoms and location data, in order to calculate the likelihood of the user contracting the virus. Major concerns about gross violations to the right to privacy of Indian citizens have been raised, due to the fact that the application has been made mandatory across India's entire working population, including all employees whether in the private or public sector. Failure to download the application results in fines of a 1,000 Rupees or six months imprisonment. Further disdain for the application is due to considerable vulnerabilities to users data privacy, as malicious actors can use the application to access data files on the user's device and poor anonymization of the data collected can lead to re-identification of data subjects.

The European Data Privacy Board (EDPB) in April 2020 released guidelines for the development of 'location data' and 'contact tracing' applications in light of the COVID-19 pandemic, which

conforms to the E.U General Data Protection Regulation (GDPR), and as such guarantees the user's right to privacy. The guidelines emphasize the need for the data collected to be anonymized and not to be a data set that has been subjected to simple pseudonymization. Prudent data anonymization will ensure that the application developed can effectively balance between containing the pandemic and safeguarding the right to privacy of users through data minimization.

Kenya's privacy law in the midst of the COVID-19 pandemic

The Kenya Data Protection Act (DPA) has been developed around and contains numerous identical provisions with the European General Data Protection Regulations (GDPR). While it is clear that, in its efforts applied towards combating the spread of COVID-19, the government has been processing personal information like names, telephone numbers, ID. Numbers, physical addresses, health data etc, it has not disclosed the nature of the methods of surveillance and tracing that are currently deployed and the data protection measures in place. The lack of information pertaining to the modus operandi of the surveillance program in Kenya carries with it the potential gross and disproportionate violations of the right to privacy of Kenyan citizens and residents. Section 51 of the DPA exempts processors of personal data from the obligations imposed by the Act where it is necessary for national security or public interest. Notably, it does not exempt the requirements relating to compliance with data protection principles relating to lawful processing, minimization of collection, data quality and adopting security safeguards to protect personal data. Section 54 of the DPA permits the Data Commissioner to prescribe other instances where compliance with certain provisions of the Act may be exempted. The data protection regulatory body has not released guidelines to provide its interpretation and guidelines in relation to processing of personal information during the pandemic.

Notably, it does not exempt the requirements relating to compliance with data protection principles relating to lawful processing, minimization of collection, data quality and adopting security safeguards to protect personal data.

It is important to have the data protection regulator issues guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak to be adopted in Kenya in order to effectively combat the pandemic and uphold the right to privacy. The EDPB proposed that the following standards, amongst others, be adopted in the design of the tracing applications:

a) Clear specification of purpose and explicit limitation concerning the further use of personal data collected;

b) Identification of categories of personal data and entities mandated to collect the data, and purposes for which the personal data is collected;
c) Additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing of the personal data;
d) Identify criteria to determine when the application shall be dismantled, and which entity shall be responsible and accountable for making that determination.

Data Subjects' rights during pandemics under Kenyan law

As mentioned earlier, the Constitution guarantees and protects the right to privacy of the citizens of Kenya, further enumerated by the DPA, though the right is not absolute and can be reasonably limited provided that there are justifiable circumstances. The envisioned limitation should be justifiable and acceptable in an open and democratic society based on human dignity, equality, and freedom.

If the COVID-19 pandemic is adjudged as a circumstance during which citizens' right to privacy can be infringed on reasonably by the Government of Kenya through its various ministries and departments, in their attempts to track and quarantine COVID-19 positive individuals, it can be said that permissible infringement to this right is limited to accessing and collecting information that is deemed necessary for controlling the spread and infection rate of COVID-19.

The DPA defines personal data as any information relating to an identified or identifiable natural person and includes the health data, which in this context is that data of individuals collected and tested during the COVID-19 pandemic. Furthermore, the health status of individuals is classified as 'sensitive' personal data and is subject to higher statutory protections compared to personal data. Personal data relating to the health of a data subject may only be processed if the processing is necessary for reasons of public interest in the area of public health. The DPA achieves the above objectives by ensuring that data controllers and processors are abiding by the universally recognized data protection principles, which includes:

a) Lawful, fair and transparent processing;
b) Health data to be collected for an explicit, specified and legitimate purpose;
c) Storage limitation; and
d) Data minimization and data anonymization.

What law takes precedence in the face of the pandemic?

There remains a lacuna as to the applicable law governing data protection and privacy during pandemics. In April 2020, the Pandemic Response and Management Bill (PRM Bill) was tabled before Senate and drafted to be the applicable law upon declaration of a pandemic and proposes temporary measures to address various matters during a pandemic. The proposed law empowers the Health Cabinet Secretary to propose regulations for the collection and publishing of data related to the pandemic. Following the potential promulgation of the PMR Bill, the Government of Kenya, through various data controllers and processors, would be legally entitled to collect health data of individuals and to publish such data. The collection and processing of the health data should ideally be streamlined to reflect the same standard established under the DPA. Data minimization would be a central tenet to the processing of the health data, so as to preserve the anonymity of the data subject.

The collection and processing of the health data should ideally be streamlined to reflect the same standard established under the DPA

During the pandemic, data protection and privacy considerations are important during collection and use of the health data, collaborative efforts with private bodies e.g development of apps, websites and services used as a response to COVID-19 and tracking of individuals using measures such as geo location tracking. Data protection measures such as relying on anonymized data, limiting unnecessary access to data and using data for a limited purpose of the crisis response. Consider storing the data in a separate database which can easily be deleted once the crisis is over. Governments must think beyond the crisis so as to protect their citizens rights and freedoms even post crisis.

Can employers legally impose health data collection and testing at the workplace?

Since the 13th of March 2020, when the first case of the COVID -19 was reported in Kenya, various directives, policies, and legislation have been developed to cushion against the social, economic, and health impact of the pandemic. The work dynamics as we knew them have been disrupted to new norms as highlighted in our article here. However, the Government has been slow to disseminate directives pertaining to the testing and collection of health data by employers from their employees.

Many businesses have resumed operations and as such many employees have resumed on premises work schedules. Testing of staff present and working from the business premises would be

considered an essential step in protecting the health and safety of all personnel and to contain the wider spread of the pandemic. Simple biometric tests that are capable of identifying the symptoms of COVID-19, including reading of body temperature before one is allowed to access the workplace would be considered essential.

Challenges arise when the employer would like to introduce measures that result to processing what the Data Protection Act regards as personal information, of the special kind, like health data. In this case, it would be expected to be in compliance thereof. Section 26 of the Data Protection Act grants a data subject the right to;

a) be informed of the use to which their personal data is to be put;
b) access their personal data in custody of data controller or data processor;
c) object to the processing of all or part of their personal data;
d) correction of false or misleading data; and
e) deletion of false or misleading data about them.

What does this impose upon employers?

A strict interpretation of the Act would require the employer to acquire the consent of their employees before compelling them to undergo, say, various intrusive medical examinations for the symptoms or presence of COVID-19. For instance, Diagnostic test - molecular testing (Government approved testing procedure) and Anti-body blood tests, which reveal if an employee has a potential immunity to the virus. Notably, such tests can only be carried out by licenced institutions/ practitioners who are also subjected to certain data protection and privacy requirements.

It is therefore essential to limit the scope of health data processed by the employer and ensure that collection is limited to the minimum necessary data and directly linked to any typical symptoms of the COVID-19. This information should not be retained for longer than necessary. Employers should also consider updating their safety and health policy to provide for systematic testing of COVID-19 symptoms for employees that will be working frequently from the business premises. The Occupational Safety and Health Act (OSHA) establishes that it is the duty of an employer to provide and maintain a working environment for every person employed that is, safe, without risks

Employers should also consider updating their safety and health policy to provide for systematic testing of COVID-19 symptoms for employees that will be working frequently from the business premises.

to health, and adequate as regards facilities and arrangements for the employee's welfare, and justifies the need for systematic testing of staff. Furthermore, OSHA provides for the duties of employees at the workplace, and are not limited to:

a) comply with the safety and health procedures, requirements and instructions given by a person having authority over him for his own or any other person's safety;
b) co-operate with his employer in the discharge of any duty or requirement imposed on the employer;
c) at all times wear or use any protective equipment or clothing, including PPEs provided by the employer for the purpose of preventing risks to his safety and health; and
d) with regard to any duty or requirement imposed on his employer or any other person by or under any other relevant statutory provision, co-operate with the employer or other person to enable that duty or requirement to be performed or complied with.

Considerations to be made by the employer

It is therefore important for the employer to consider all relevant applicable laws including the Data protection Act and labour laws and generate internal procedures and policies to guide anticipated scenarios such as;

a) How much information can an employer ask about an employee's health data and what are the information obligations relating to collection?
b) with whom can the sensitive data be shared with including fellow employees who have come into contact?
c) Can an employer direct their staff to report covid-19 symptoms?
d) What steps can an employer take if an employee is tested as covid-19 positive?
e) What steps can be taken to ensure limited access to the collected and processed health data of infected employees (on a need to know basis) while observing data minimization and data protection measures?
f) Should the health information be filed in an employee's file?
g) Is the database held by the employer now subject to the company's Privacy Impact Assessment procedures?
h) What administrative and technical measures are in place to protect the data collected?
i) What are the actions to be taken once processing is no longer necessary?

Principles that should be observed while processing personal information

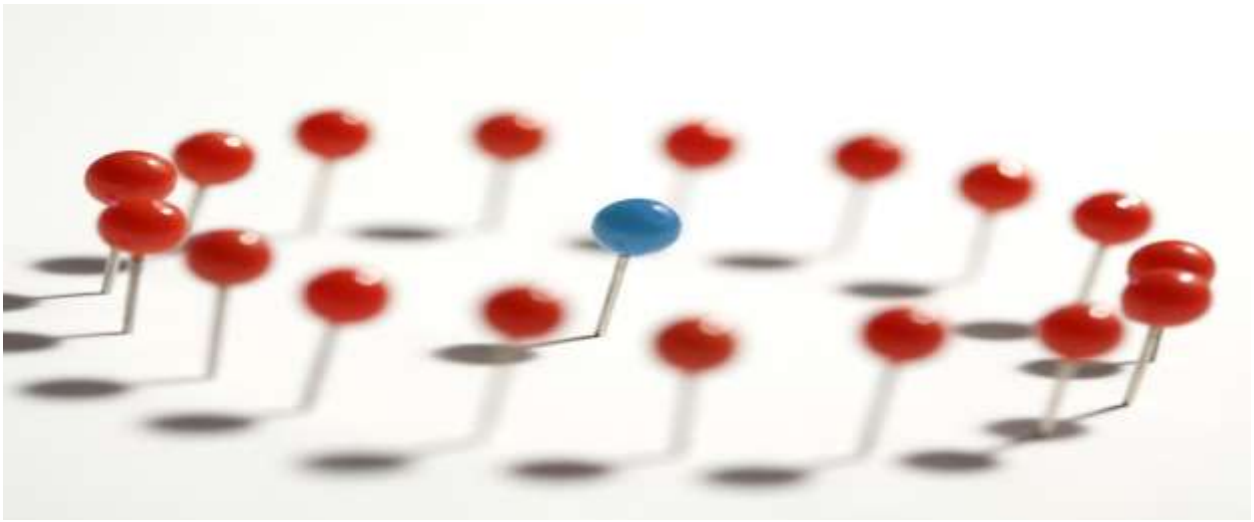
---

All processors of personal information during the COVID-19 crisis must be guided by the 6 principles of personal data protection provided in section 25 of the Data Protection Act which requires all personal information to be;

a) processed in accordance with the right to privacy of the data subject;
b) processed lawfully, fairly and in a transparent manner in relation to any data subject;
c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Data Protection Act compliance during the COVID-19 pandemic

The public health and interest element of personal information collected by the government and private entities is the classic scenario of giving up some personal rights for better services. While it makes sense that the country adopts a flexible and pragmatic approach to data protection compliance during the pandemic, public trust that the data subject's rights will be processed in compliance with the data protection laws must be maintained.



Data protection by design

The consent parameters being procured at every stage need to be precise and specific. The principles of data processing, and especially of health data, highlighted above cannot be overlooked despite the circumstances. There should be policies to enshrine the exceptional circumstances when the government and its third-party partners can limit the data subject's right to privacy. Guidelines for use in case of adoption of contact tracing mechanisms such as use of location data technology need to be issued by the data protection regulator in the absence of a Data Commissioner. The technology designed should focus on data protection by design as envisaged in section 41 of the Data Protection Act.

Issues to be addressed while designing systems

a) once the pandemic is effectively managed, what are the policies in place for retrieval of this data for research or dissemination and the data subject's rights over this?
b) How much data needs to be gathered and processed centrally?
c) Can the controller demonstrate how privacy is built into the technology used to process this data?'

Post COVID-19 pandemic

The ultimate scenario is that many governments will share this data with international governing bodies to aid a global strategy on how to put in place mechanisms to deal with it in the future. Data protection measures need to be adopted in relation to shared personal information especially cross

border transfers and in some instance the data subject may need to be informed and their consent procured especially if the initial reason for collecting the data differs from its end use. The other issues arising are those of retention, retrieval, and eventual destruction. This can be done by set out policies or upon request by the data subject.

Ultimately, the world finds itself in a very precarious position where a perceived "for the general good and welfare of the public" scenario outweighs certain aspects individuals' rights to personal information. The pandemic should neither be used as a general waiver of these rights nor as a reason to flout the general principals of data processing.

All in all, the guidelines issued during the COVID-19 pandemic period will be relevant for future public health situations that involve processing of personal information.

For further information, contact tmt@tripleoklaw.com

About Telecommunications, Media and Technology Practice:

TripleOKLaw LLP Advocates is alive to the emerging transactional issues as well as the ever changing legal and regulatory landscape. Our team works in tandem with the changing landscape to facilitate a myriad of transactions within the telecommunications, fin-tech, payments and technology industries. Our clients comprise of Innovators, start-up firms, P.E funds, VC firms, among others. The team is ranked as leading FinTech legal experts in the Chambers and Partners FinTech Legal Guide 2020 available here.