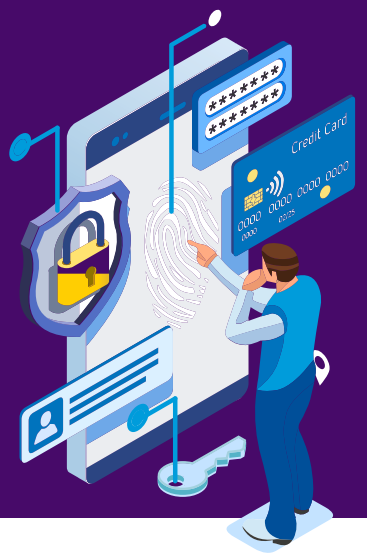
KPMG

Protecting privacy amidst COVID-19

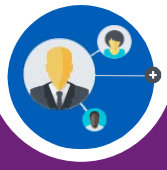


Developments across the globe

Coronavirus disease, 2019 (COVID-19) was recognised as a pandemic by the World Health Organisation (WHO) on 11 March 2020. As it stands, more than two and a half million people across 213 countries and territories[1] are confirmed as COVID-19 cases with a 6.8 percent mortality rate as on 21 April 2020. Countries across the world are focused on developing novel ways such as locking down international and domestic borders, analysing travel history of travelers, leveraging technology to trace and isolate infected people, establishing isolation centres to test and treat the virus, etc.

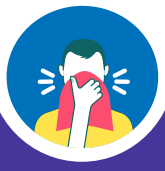
While the government authorities, medical institutions and organisations are involved in addressing the current situation by exchanging a lot of data, there is an inherent focus to protect the security and privacy interests of individuals, whose personal and sensitive personal data are widely being used.

Data protection authorities across the world such as the European Data Protection Board (EDPB), Information Commissioner's Office (ICO), Personal Data Protection Commission (PDPC) Singapore, Office of the Australian Information Commissioner (OAIC) are quickly responding to such challenges by facilitating clarifications and issuing guidelines on how to process personal and sensitive personal data under these circumstances. Certain authorities have provided clarifications to organisations on the following: -



Collection of visitor information for contact tracing

Usage of personal and sensitive personal information as part of response measures



Informing employees about the a potential COVID-19 patient identified in organisation.

1. Coronavirus disease (COVID-19) Pandemic, World Health Organization, accessed on 21 April 2020

Largely, the authorities across different countries have expressed their support and have requested public and private bodies to take a balanced approach while processing personal data. The authorities have also been liberal in informing them to prioritise in fighting the pandemic.

Some Asian countries, which have had significant impact due to COVID-19, are leveraging on various technologies to identify and contain the spread of the virus[2] for tracing, tracking the impacted individuals and enforcing quarantine. Governments are also relying on location information to generate alerts to the local authorities when the quarantined individuals leave their designated quarantine zones/locations. Similarly, Italian Civil Authority has approved the use of drones to enforce social distancing[3]. Data from wearable devices is also being used to monitor physical wellbeing based on critical parameters such as heartbeat, pulse, body temperature, etc. This data is again shared with health authorities to better understand and deal with the pandemic.

Most of the countries have also come up with their own platforms including mobile applications through which the location data is collected and used for some of the purposes mentioned above. European countries, who are generally reluctant to use these intrusive technologies on their residents have now adopted this approach to effectively manage the current situation.

What is the current situation in India?

As the world's second-most populous country with 1.3 billion people, India's challenges are deeper as the data privacy regime (Personal Data Protection Bill 2019) is yet to come into effect and the Data Protection Authority of India (DPAI) has not been established. Thus, there is a lack of guidelines regarding processing of personal and sensitive personal data in the current situation. While the government and private organisations are taking necessary steps to contain the spread of COVID-19, they also have responsibilities for ensuring that the privacy of the individuals is protected.

Indian constitution recognises privacy as a fundamental right of the citizens, as of now India does not have any comprehensive enforced regulation to cater to the privacy needs of an individual. However, the India IT Act 2008 43 A, defines that information shall be shared (including sensitive personal data), with government agencies without obtaining prior consent from information provider for the purpose of verification of identity, or for prevention, detection, investigation. The draft Personal Data Protection Bill (PDPB) 2019 provides the below grounds of processing personal data without obtaining consent:

In order to respond to any medical emergency involving a threat to the life or health of an individual, or

In order to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health.

2. How countries are using technology to fight coronavirus, The Economic Times, accessed on 21 April 2020
3. Coronavirus: Italy approves use of drones to monitor social distancing, Euro News, accessed on 21 April 2020

The Central government is in the process of building a common repository for medical records to enable governance of health data in order to provide medical facilities to all the residents of the country. This medical record repository will also help doctors and medical researchers in discovering efficient methods of curing patients. In line with this, 'Digital Information Security in Healthcare Act-2018' (DISHA) has been drafted to safeguard and enforce significant limitations on the use of health data.

Some common requirements from the draft PDPB and DISHA are as follows:

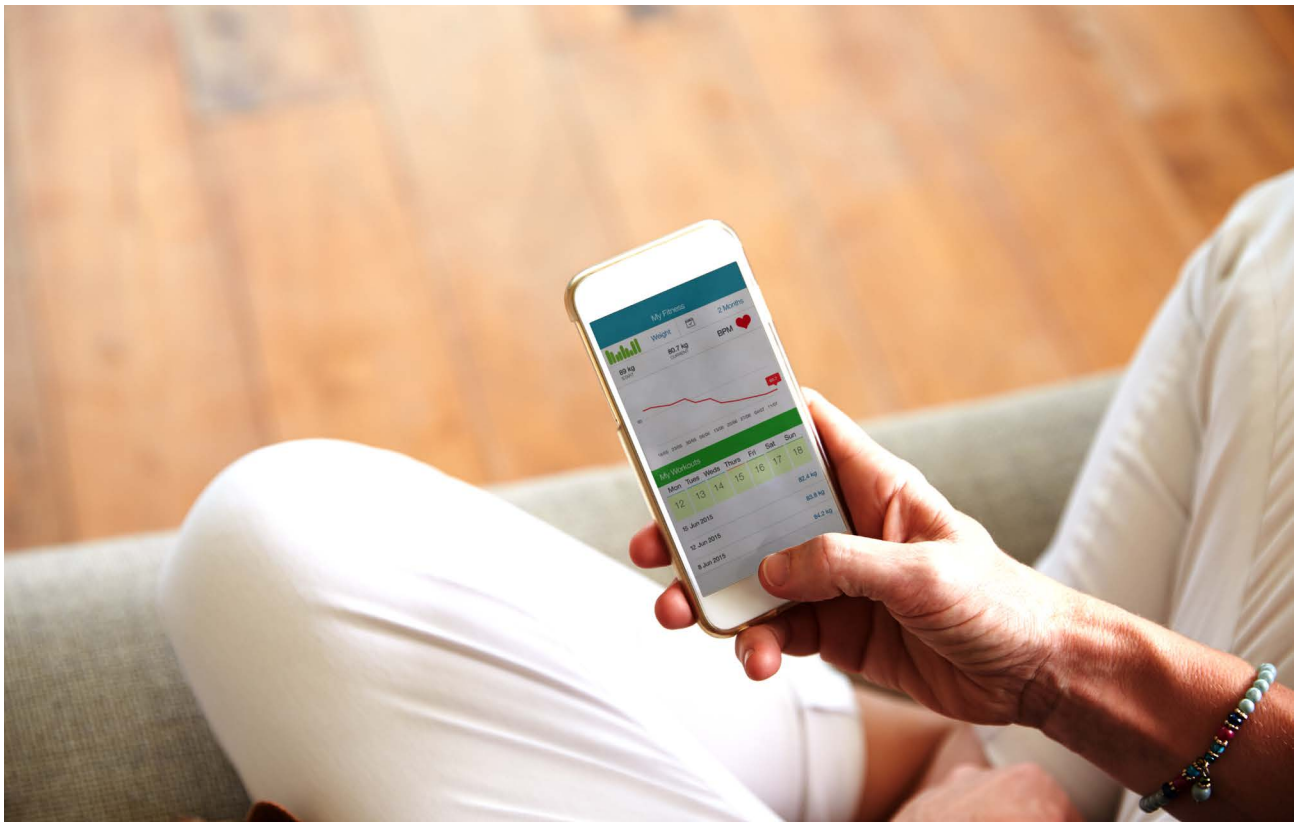
- Consent and its related rights
- Governmental access of the data for public health threats, clinical research, management of chronic diseases, etc.
- Processing of data by 'entities' other than clinical establishment
- Processing of health data by smartphones, wearable devices
- Sharing/receiving of anonymised data.

As the COVID-19 outbreak continues to surge significantly in the country despite regular measures being announced and lockdown imposed countrywide, Ministry of Electronics and Information Technology (MeitY) has developed a mobile application, 'Aarogya Setu', which helps users to check whether they are/were in the proximity of an infected person and alerts the users to self-quarantine themselves. This application does not reveal the identity of the infected or quarantined person.

In addition to contact tracing via Aarogya Setu mobile application, the Indian government is also relying on airline and railway reservation data to trace or identify the suspected COVID-19 patients. Provisions of the Epidemic Diseases Act, 1897 and National Disaster Management Act, 2005 permit governments to adopt to such emergency response measures.

Overall the authorities shall establish adequate measures for secure deletion or disposal of personal data collected during the pandemic, after it has been used for the specified purpose of identifying potential patients and designing response strategies.

Private and public sector organisations have also become invaluable partners to government and medical agencies in their contact tracing efforts through collection of information of employees, occupants and visitors at their premises. This has spurred concerns around excessive data collection and its potential misuse. Forward-looking concern would be, how long this data will be stored and whether it will be purged/anonymised once this crisis ends. Oganisations may feel a need to rapidly develop processes to protect the data collected from their employees, occupants and visitors. While it is paramount to have a swift response to the crisis, it is also critical to ensure that all processing activities are in line with the privacy principles, and do not subsequently violate any regulatory requirements that may apply.



Guidance for organisations to handle information during current scenario

Organisations may encounter the following challenges while processing data in this circumstance:

Record keeping practices - While maintaining records about employees with regard to the COVID-19 pandemic, businesses should keep in mind that the health information of employees should not be kept as part of the standard personnel file and rather store the same in segregated confidential files to which the access is restricted.

Internal communications about employee health - Prior to issuing communications about employee health, organisations must ensure that the identity of the individuals is sufficiently protected. Furthermore, it must be kept in mind that e-mails can be misdirected or inadvertently forwarded to individuals outside the organisation.

Sharing employee records with authorities – Organisations should take extreme care prior to sharing confidential employee information to any authorised agency of the government who may request for the same. Data should not be shared without consulting relevant teams such as legal, regulatory, data privacy, HR. Additionally, all employees should be made wary of potential phishing and ransomware attacks that may be attempted to leverage the ongoing crisis to infiltrate the organisations critical systems.

Remote working practices - Organisations are forced to work remotely, and teams have to rely on workplace collaboration tools to ensure business continuity. It is crucial to assess the data privacy policy and guidelines of such tools against the organisation's privacy policy or best practices. Such collaboration of tools may reuse the data which they collect from users or organisation in exchange of their services, for alternative purposes such as marketing, data monetisation. Organisations may also choose to rely upon technologies such as productivity monitoring tools and attention tracking to ensure that productivity levels of their employees are maintained. Use of such technologies may constitute monitoring of employee behaviour which is prohibited under certain regulations.

The following considerations need to be made with respect to privacy during the ongoing crisis:

- **Establish clear accountability** - Organisations should assign an individual to oversee all data processing operations with regard to COVID-19 response, and it should be ensured that inputs are obtained from the data protection officer prior to commencing any such processing activities.
- **Secure data sharing** - Organisations must ensure that all communication channels offer adequate security for the protection of the data being shared. Furthermore, measures should be taken to ensure the traceability of the data shared by the organisations. It is ideal to store the data in a centralised repository and access the data through secure channels. This manner is likely to ensure only authorised people can access the data.

Storage limitation - All personal data collected for the purpose of responding to the COVID-19 crisis should be securely disposed or anonymised, and archived as per statutory/regulatory requirements.

Quick tips to be considered while processing of personal data: -

1. Organisations must include the privacy team / data protection officer as the part of the crisis management team during such situations
2. Collect and store personal and sensitive personal data in a structured digital format, which will increase the reusability of the data
3. Organisations must ensure a single of source truth is maintained, instead of maintaining multiple copies in different formats across various teams.

KPMG in India Contacts:

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-Leader Global Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner and Head
IT Advisory
India Cybersecurity Lead
E: atulgupta@kpmg.com

Mayuran Palanisamy
Director - IT Advisory
India Lead - Data privacy
E: mpalanisamy@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia