

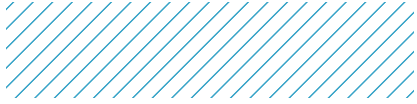


## DATA PROTECTION AND ADJUSTING TO THE “NEW NORMAL”

The government will use big data for the prevention and control of diseases

Written by Anubhav Kapoor, Group Vice President, Cummins India

The novel Coronavirus (COVID-19) has affected almost every country in the world and on March 11, 2020, the World Health Organization declared COVID-19 a pandemic. With nations in lockdown to protect their people from the virus, businesses and commerce were put on hold. The wheels of economic growth were severely impacted and, in few cases, damaged beyond repair as nations continue to grapple with the pandemic. The human and economic toll of the outbreak has already eclipsed other major crises in recent times and may permanently impact the world. As if overnight and rightly so, the focus shifted to health, environment and social responsibility.



We now slowly brace ourselves to co-exist with COVID-19 (at least until the cure/vaccinations are found). On one hand businesses are faced with unforeseen risks of financial, manpower, demand, supply, and regulatory uncertainty, but on the other the need to stop the spread of COVID-19 and cure those who are affected. This continues to be the single most important goal for the government and public health authorities globally. Reopening does not seem to be an easy process and perhaps we may never be the same as we were in “pre-COVID” times, something that we now refer to as the “New Normal”. For example, our work environments may be most affected as many employees may continue to work from home for extended periods of time. Enterprises have adopted technology, developed alternate processes, and some have also taken aggressive measures to manage cost and sustain their business. Social distancing norms, quarantine, virtual meetings, PPE kits etc. have become the order of the day in every space and subject of common parlance and everyday existence. Enterprises, governments, and public authorities across the globe are now engaged in the challenging and important work of identifying a path towards the “New Normal” and to get society back on track.

### Data protection principles support information sharing on COVID-19

Employers are taking a wide range of actions to operate in the new normal. Today, it is of utmost importance that employers be mindful of protecting the data privacy of their employees and business contacts. The principles enshrined in several international and national instruments including Convention 108+ can only be derogated or restricted in a lawful manner. The good news is that data protection principles have the flexibility and allow the balancing of interests in different situations particularly in unprecedented situations like COVID-19. These principles are consistent and very much compatible and reconcilable with other fundamental rights and relevant public interests.

### Data protection principles while reporting to public and government authorities

Data protection principles generally allow some exceptions and restrictions for safeguarding public interest and individuals’ vital interests. The right to data protection does not prevent public and government authorities to share the list of health professionals, public health workers and officials (names and contact details) tasked with testing, health moni-

*Enterprises have adopted technology, developed alternate processes, and some have also taken aggressive measures to manage cost and sustain their business.*

toring, distribution of relief materials etc. As anonymised data is not covered by data protection requirements, the use of aggregate location information or apps to signal, track, trace, or to indicate movements of persons traveling away from a severely infected area or in terms of number of COVID-19 positive persons would also not be prevented by data protection requirements. Neither can the right to data protection suggest that it is incompatible with epidemiologic monitoring and reporting requirements. However, personal data collected for preventing or treating epidemic diseases cannot be used for any other purpose. No personal information that has been collected for such use can be made public without the consent of the data subjects, unless this is necessary for the prevention of an epidemic and the information is redacted or anonymized.

If businesses are required by law to disclose certain data to government or public authorities for public health reasons, they are invited to do so under strict compliance with the law and with a clear understanding to return to "normal" processing (including permanent deletion) once the state of emergency regime is no longer applicable. We expect the government and public authorities to continue with the monitoring to safeguard our society. It is extremely important therefore that businesses take compliance seriously when disclosing such information to government and public authorities. When health and governmental authorities are communicating with the public, they should avoid the publication of publication of personal data related to specific individuals.

#### **Privacy concerns for employers for Covid-19 preventive practices**

In the new normal, employers may be required to follow and implement several measures or comply with standard operating procedures (SOP) for the public and their staff while maintaining their

business activity. Employers may now have to process personal or sensitive data that they traditionally did not collect—such as health-related data. While doing so, employers should respect the principles of necessity, proportionality, and accountability and should also be guided by principles designed to minimise any risks that such processing might pose to employees' rights and fundamental freedom. Employers must be compliant with the data protection principles when organising their work places and working conditions. Any personal information which is collected while providing services under lawful contract or in context of employment is not permitted to be disclosed except as agreed under such contract or unless consent for the same has been obtained. Employers should not process personal data beyond what is necessary or publish or share information that exposes the identification of individual employees. Privacy by design should be ensured and appropriate measures adopted to protect the security of data. Employers who collect and control personal data or data related to COVID-19 or health related data must have strict technical and management measures in place to prevent data breaches and an impact assessment should be carried out before the processing is started.

#### **Commonplace Practices in the New Normal**

Some of the common practices that enterprises and establishments are implementing include temperature recording, physical screening, self-declaration of medical condition, collecting travel history and related information from employees, visitors and business contacts or their families, downloading tracing or tracking apps, etc. What is important to acknowledge here is that any information pertaining to the physical condition of an employee such as body temperature, health

*The good news is that data protection principles have the flexibility and allow the balancing of interests in different situations particularly in unprecedented situations like COVID-19.*

data, travel data either through non-intrusive methods or through self-declaration forms or otherwise is personal data.

An individual's data or health status can be shared only after securing the individual's meaningful consent. Meaningful consent can be obtained by being transparent about the reason for collecting data, what data is being collected, for what purposes the data will be used, and how long it will be kept. No personal data or health status can be shared without consent and individual's being made aware of the processing of personal data related to them. Individual data subjects are entitled to exercise their rights under the law. If such sharing is pursuant to legal requirements, then the sharing should be strictly limited by the scope of the law. Processing of personal data can be carried out only if necessary and proportionate to the extent specified and legitimate purpose pursued. For example, when notifying the individuals that they may have been in physical contact with an infected person, only share the minimum amount of data necessary to avoid divulging the identity of an infected person.

#### **Conclusion**

Companies with big data expertise and capabilities are increasingly working with the government and authorities to use big data for the prevention and control of diseases. Addressing global problems of this magnitude understandably creates an urgent need for innovative uses of data to fight the pandemic, but the same needs to be done within the four corners of the data privacy and ethical principles. It's unfortunate to hear about several data breach incidents which have given rise to concerns over data protection, privacy, fraud, and potential discrimination against people. Like everything else, this too shall pass but we must make sure we keep intact the privacy and ethical principles as we move forward to use data responsibly to defeat the COVID-19 pandemic and get ready for the "New Normal".

**Disclaimer:** The article states my personal view and not the views of my organization or state of compliance in any organization.

#### **Author Biography**



**Anubhav Kapoor** is Group Vice President, Cummins India. He has more than 25 years of experience as Company Secretary & Corporate Lawyer which spans across various industries including IT, automotive, aerospace, pharmaceuticals, food, banking, and insurance software's and engineering.