April 8, 2020

Being Privacy Compliant During COVID-19

In March 2020, the World Health Organisation declared COVID-19 a pandemic. This has caused employers around the world to take measures to protect and screen their employees and business contacts. These measures include checking employees' temperatures, obtaining their health and travel data, collecting medical certificates, etc.

While these measures are important, organisations must also remember that they continue to protect the privacy of their employees and other contacts.

Under current Indian law, the collection, receipt, possession, storage, handling and transfer of personal information ("**PI**") and sensitive personal data or information ("**SPDI**") of natural persons through electronic means is regulated by the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Privacy Rules**" and along with the IT Act, "**Indian Privacy Laws**"). SPDI is defined to include physical, physiological and mental health condition and *medical records and history*. An organisation processing PI and/or SPDI must comply with Indian Privacy Laws. This includes taking data subject consent prior to collecting SPDI, collecting this only for lawful purposes, not retaining it for longer than required, issuing a privacy policy, implementing reasonable security practices, etc.

Indian Privacy Laws do not provide an exemption on privacy practises during emergencies. So far, no special dispensation or exemption has been issued by the government either. As such, even during this time, compliance with Indian Privacy Laws remains mandatory.

Medical data is quite clearly SPDI. If an employee/ consultant/ other business contact informs you that they are unwell, and provides you any data, be mindful to not publish their identity and health records. Disclosures of SPDI may be unlawful if you don't have specific consent. In the past, Indian courts have also recognised that persons with diseases, victims of sexual assault, etc. have the right to keep their identity confidential. There is a possibility that Indian courts/ regulators will act to punish the wrongful or negligent disclosure of an unwell person's identity and health records.

Be mindful, also, if and where you store the health data of such persons. If you, or your IT services provider, do not follow reasonable security procedures, or are negligent, liability may again latch on to you for any breaches. Do not transfer employee medical data to a third party without prior data subject consent, and track how the third party uses such data.

You will recollect that an updated draft of the Personal Data Protection Bill, 2019 ("**Draft Bill**") was introduced before the parliament in December 2019 and, subsequently, referred to a parliamentary select committee. This committee was expected to submit its report on the Bill before the end of the budget session in March 2020. However, due to the COVID-19 outbreak and consequent pre-mature adjournment of parliament, the committee sought an extension to submit its report in the second week of the monsoon session (usually commences by July, but dates are yet to be announced). This Draft Bill has many more stringent, binding requirements around protecting critical data. You should make sure liability for privacy breaches does not spill-over when this new, more draconian, law comes into force.

If you have any queries on how to handle PI and/ or SPDI during these uncertain times, feel free to reach out to us at practicemanager@btg-legal.com.