UPDATES

COVID-19 – Key Issues Faced in the Technology Sector

10 April 2020

This update covers:

> The spread of COVID-19 and the consequent nationwide lockdown in India is having a far-reaching effect for companies across various sectors. In this update, we address some of the common issues that 'tech' companies amongst others are facing while managing business continuity and employees.

Ever since the World Health Organization declared novel coronavirus (COVID-19) as a pandemic on 11 March 2020, various countries, including India are on high alert to contain the spread of COVID-19 cases. The Indian Central and State governments have issued multiple advisories, notifications and regulations on work from home, travel and healthcare, in addition to declaring a 21-day nationwide lockdown till 14 April 2020. In this update, we address some of the common issues that tech companies are facing in the backdrop of COVID-19 lockdown.

a. Frequently Asked Questions

▪ Privacy and Data Protection

As COVID-19 continues to rapidly spread across countries, companies are looking at making important decisions to ensure the health of their employees and safety of the workplace. Data plays a crucial role in these decisions; however, it is also important to balance it with an individual's right to privacy while finding solutions amidst this pandemic. For example, we have seen companies requesting their employees, consultants, visitors, etc. to provide information about their health including medical reports, travel history, exposure to potential COVID-19 cases. In this backdrop, we address some of the common queries below.

– **Do Indian data protection laws provide any guidance on either permitting or restricting the collection of personal data to identify COVID-19 cases?**

Yes. Section 43A of the Information Technology Act, 2000 read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Data Protection Rules) governs the collection and processing of personal information of any individual in India. Certain categories of information such as information relating to an individual's physical, physiological and mental health condition, medical history, etc., are considered as sensitive personal information (SPI). This would include any medical/health data of an employee or his/her family members (including medical certificates), their symptoms and information about exposure to potential or confirmed COVID-19 cases. Other information such as one's travel history is considered as personally identifiable information (PI).

While PI can be collected without explicit consent, the Data Protection Rules impose several obligations on companies for the *collection and disclosure* of SPI. They mandate obtaining the consent of the information provider before the collection of any SPI. Further, SPI is only to be collected under a lawful purpose and when its collection is necessary for that purpose. Therefore, employers collecting any sort of medical or exposure information from their employees must obtain prior consent. Such consent must also state the purpose for which the SPI is being collected, the intended recipients (if any), and the individual must have knowledge of the fact that his/her SPI is being collected. This would be applicable for the collection of medical information regarding the individual's family members and/or requiring the employee to produce medical certificates. Typically, most privacy policies cover such collection and processing of SPI by the employees and if such SPI is collected as provided in the privacy policies, that will be sufficient.

– **How can I obtain consent from such an employee, consultant or visitor for collection of their medical information?**

Consent is often procured by employers for general health monitoring and health check purposes through existing terms of employment read with HR policies or employee handbooks. The first step would be for companies to assess their existing employment contracts, HR policies (including data or privacy policies) or handbooks to see if the consent they have already obtained is sufficient for the purpose of obtaining the SPI. If it is, the company does not need to seek consent afresh.

If not, employers can consider taking explicit consent when they conduct health checks, screen temperatures or collect medical data. Employers may also rely on various government advisories requiring them to undertake preventive measures such as asking employees to undergo health checks at the workplace. This has been covered in further detail along with other issues in our employment update on COVID-19 available here and here. However, if an existing consent framework is not in place, employers can consider obtaining it as a part of their action plan steps.

Several establishments are also monitoring the temperature of their employees, visitors, guests by way of thermal screenings. If the temperature is not being collected or processed in any form - for instance, thermal scanners at entrances that simply alert security staff about persons with high temperature without in any way identifying them or associating the identified person with any other personal information in the company's possession, this would not amount to collection of SPI and there would be no requirement to seek prior consent.

– **Am I permitted to disclose the identity of any employee or individual who is confirmed to be COVID-19 positive to the government or other co-workers? Am I mandated to report to the government agencies once I have information of any employee's confirmed COVID-19 status?**

The Data Protection Rules allow a body corporate to disclose an individual's SPI to a third party only if prior consent for such disclosure has been obtained from such individual; unless such disclosure has been agreed upon in the contract between the individual and the body corporate; or is mandated to be disclosed by law at the time.

Therefore, the identity of a person along with his/her health information can be disclosed to the government or any third party only if doing so is mandated by law. If there are orders issued by the government to that effect, then this information can be disclosed to the government.

For disclosure of the identity to any co-workers, a company must take prior consent of the individual. The company can however, without disclosing the identity of the person, provide information about other details of the individual's potential exposure and the nature of such exposure, to implement appropriate precautions. However, employers should analyse the information already available with the co-workers before sharing additional information about potential exposure, to avoid any inadvertent disclosure of SPI without the individual's consent.

– **Does the government have a right to access the health data of people suspected of COVID-19?**

The government has invoked the Disaster Management Act, 2005, giving wide powers to the Ministry of Health and Welfare to take emergency response measures and to enhance preparedness and for the containment of the COVID-19. Various state governments have also classified COVID-19 as an 'epidemic disease' under the Epidemic Disease Act, 1897, giving local administration authority to impose various containment measures, such as quarantine, closure and surveillance. For example, the Delhi government has issued the Delhi Epidemic

Diseases, COVID-19 Regulations, 2020, which mandate all government and private hospitals to record travel and exposure history of all persons coming in for screening of suspected COVID-19 cases. It also notifies certain government officials as Authorised Person(s), including the Secretary (Health and Family Welfare), Director of General Health Services, District Surveillance Officers, etc. Such Authorised Persons are empowered to implement measures for the containment of the disease - including initiating active and passive surveillance of COVID-19 cases. It is also mandatory for all government and private medical practitioners to notify people having a travel history to any of the COVID-19 affected countries to the District Surveillance Unit, irrespective of whether such people are symptomatic or not. Given this, SPI of individuals can be disclosed to the government as long as it takes place further to a lawful order.

▪ Corporate Affairs

The Ministry of Corporate Affairs has announced several relaxations for companies and LLPs to enable businesses to cope with the disruptions caused due to the outbreak of COVID-19. The relaxations provided by the MCA are discussed below.

– What are the various relaxations for companies from compliance requirements under the Companies Act, 2013?

The Union Finance and Corporate Affairs Minister have announced the following relaxations with respect to compliances under the Companies Act, 2013:

- MCA filings: No additional fees will be charged for late filings from 1 April 2020 to 30 September 2020.
- Board meetings: The mandatory requirement of holding board meetings within the prescribed 120 days interval has been relaxed by an additional 60 days till the next two quarters up to 30 September 2020.
- Audit related: The Companies (Auditor's Report) Order, 2020 will be made applicable with effect from FY 2020-21 instead of FY 2019-20 (as previously notified).
- Independent director meetings: Non-compliance with the requirement of holding at least one meeting with only independent directors, as required currently, will not be treated as a violation.
- Newly incorporated companies: An extension of six months has been provided to newly incorporated companies to file their declaration of commencement of business.
- Resident Indian director: If a director in a company cannot reside in India for more than 182 days, this will not be considered a violation of the requirement of having at least one resident director in India.
- Deposit reserve: The deadline to create a deposit reserve of 20% of deposits maturing during the FY 2020-21 by 30 April 2020 has been moved to 30 June 2020.
- Debentures: The requirement to invest 15% of debentures maturing during a particular year in specified methods or instruments before 30 April 2020, has been extended to 30 June 2020.

Further, the Ministry of Corporate Affairs has issued a Companies Fresh Start Scheme, 2020 and revised the LLP Settlement Scheme, 2020 on 30 March 2020. The scheme provides a one-time opportunity to enable companies and LLPs to complete their pending compliances by filing necessary documents in the MCA-21 registry including annual filings. This scheme reiterates that no additional fees or penalties will be charged for delayed filings on the MCA-21 registry for both companies and LLPs during the period starting 1 April 2020 to 30 September 2020. The schemes elongate timelines as well as reduce the related financial burden on companies and LLPs. The schemes also provide additional time for filing appeals before the concerned

Regional Directors against the imposition of penalties, if already imposed. However, the immunity is only against delayed filings on the MCA-21 registry and not against any substantive violation of the law.

– **Does contribution to the PM CARES Fund qualify as a CSR activity?**

Yes, the contributions to the PM CARES Fund (an emergency relief fund set up for dealing with emergency or distress situation such as that posed by COVID-19 pandemic) will be an eligible CSR activity under item no. (viii) of the Schedule VII of Companies Act, 2013 which includes a contribution to any fund set up by the Central Government for socio-economic development and relief.

– **Are there any COVID-19 related filings that are required to be made by companies?**

The MCA released an update regarding the filing of a 'Companies Affirmation of Readiness towards COVID-19' form (CAR 2020 form) and later clarified that this filing is voluntary. The CAR 2020 form deployed on 23 March 2020 is a web-based form with minimum fields, which can be filed from anywhere. Digital signature certificate is not required to make the filing and the filing does not involve payment of statutory fees.

Force Majeure

The COVID-19 outbreak is disrupting businesses and global supply chains resulting in parties being unable to meet their contractual obligations. The questions below address how force majeure clauses in commercial contracts and the doctrine of frustration may be used in the context of the COVID-19 outbreak.

– **Has the spread of COVID-19 been declared as a force majeure event by the government?**

The Ministry of New and Renewable Energy (MNRE) has issued an Office Memorandum dated 20 March 2020 stating that:

- all Renewable Energy implementing agencies of MNRE are required to treat delay on account of disruption of the supply chain due to spread of COVID-19 in China or any other country, as a Force Majeure event;
- the Renewable Energy implementing agencies may grant a suitable extension of time for projects, due to COVID-19, based on evidence/documents produced by developers and submitted as a formal application to Solar Energy Corporation of India/NTPC Limited/other implementing agencies; and
- the State Renewable Energy Departments (including agencies under Power/Energy Departments of States, but dealing in renewable energy) have also been requested to treat delay on account of disruption of the supply chains due to spread of COVID-19 in China or any other country, as a force majeure event and issue their own instructions on the subject.

The Office Memorandum is of relevance to companies that are engaged with the MNRE and its implementing agencies as it enables such companies to invoke force majeure clauses under their contracts.

Further, the Department of Expenditure, Procurement Policy Division under the Ministry of Finance issued an Office Memorandum on 9 February 2020, in relation to the government’s ‘Manual for Procurement of Goods, 2017’, which effectively states that the COVID-19 outbreak could be covered by a force majeure clause on the basis that it is a natural calamity. However, due procedure should be followed by any government department seeking to invoke it.

– **What are the criteria for invoking force majeure under a contract governed by Indian law?**

In common law jurisdictions, force majeure events are agreed as contractual clauses. Generally, the occurrence of a force majeure event absolves parties from performing the contract without incurring any liability. The intention of a force majeure clause is to cover events that affect a party's ability to perform a contract, either in its entirety or in a timely manner and where such event is beyond the reasonable control of the non-performing party. Whether the outbreak of COVID-19 will qualify as a force majeure event under a particular contract is a factual analysis that will have to be undertaken on a case to case basis. In the event the force majeure clause includes acts of nature such as the spread of epidemics, natural calamities, it is possible to argue that the outbreak of COVID-19 would be a force majeure event. Further, for contracts with the Government of India, it may be possible to argue force majeure given the government notifications highlighted above.

In the absence of a contractual force majeure clause, to justify non-performance of a contract due to the outbreak of COVID-19, the non-performing party will have to show that the contract has been frustrated. Frustration of contract is covered under Section 56 of the Indian Contract Act, 1872. In order to claim that the contract is frustrated, it must be shown that the performance of the contract is entirely impossible and that it has become fundamentally different from the arrangement contemplated at the time of executing the contract. However, mere difficulty in the performance of any obligation under a contract is not sufficient reason to invoke frustration of contract. Moreover, this is also a factual analysis that will have to be undertaken on a case to case basis.

▪ Work From Home

At the initial stages of the COVID-19 outbreak, several notifications passed by the Central and State governments advised employers to allow their employees to work from home to the extent possible. However, ever since the Ministry of Home Affairs (MHA) ordered a 21-day nationwide lockdown from 25 March 2020 to 14 April 2020, all '*commercial and private establishments*' must be mandatorily closed during the lockdown, except for establishments deemed to be carrying on essential services or as notified by the governments. Given this, most companies are currently under an obligation to provide their employees with an option to work from home.

There are certain specific regulatory restrictions applicable to companies with Other service providers registrations and companies working out of Special Economic Zones and Software Technology Parks of India (STPI) units. We have covered the same below. To refer to the general questions that employers may have regarding work from home facility, please refer to our previous update of 17 March 2020, here and of 29 March 2020, here.

– Other service providers (OSPs)

a. How can companies with registered OSP centres provide their employees/agents work from home facility?

Companies providing 'application services' are regulated by the 'Terms and Conditions – Other Service Provider Category' (OSP Terms), issued by the Department of Telecommunication (DoT) in 2008. Under the OSP Terms, the facility of Work From Home (WFH) can only be provided to employees on fulfilment of certain conditions and after seeking prior permission from the DoT. Once the permission has been granted, the OSP is required to enter into an agreement with the DoT, and furnish a security deposit of Rs. 1 crore in the form of a bank guarantee in favour of the DoT. Any employee who is working from a location outside the OSP centre is called an 'Extended Agent' under the OSP Terms, and such location is referred to as an 'Extended Agent Position'. To avail WFH, interconnection between the OSP centre and the Extended Agent Position must only be through a Provider Provisioned Virtual Private Network (PPVPN) provided by an authorized telecom service provider. The PPVPN must pre-define the location of the OSP centre and each of the Extended Agent Positions.

Given that employers have been mandated to allow their employees to WFH during the lockdown, the DoT has, through its notification dated 13 March 2020 (WFH Notification) provided certain relaxations in the OSP Terms to facilitate WFH for OSP employees. These relaxations are available till 30 April 2020 and are as follows:

- Security Deposit and Agreement: OSPs are exempted from the requirement to pay a security deposit of Rs. 1 crore and enter into an agreement with the DoT to enable WFH facility for its employees.
- PPVPN: OSPs are exempted from the requirement of obtaining a secured VPN from an authorised service provider. To avail the WFH facility, OSPs can now use a secured VPN configured using 'static IP' addresses by themselves to enable the interconnection between the Extended Agent/employee with the OSP centre, where the employee's home and the OSP centre must be pre-defined locations.
- No prior permission: There is no longer a requirement to obtain prior permission for WFH. OSPs can now simply notify/intimate their respective Licensed Service Area field unit/Term Cells of the DoT before starting the WFH facility. They must submit complete details for the Extended Agents such as their name, physical address, 'static IP' address assigned, etc., while furnishing such intimation.

Despite the above relaxations, OSPs must continue to comply with all other applicable conditions of the OSP Terms for this period, including maintaining tamper-proof Call detail records/system logs of the Extended Agents for one year. Violation of the WFH Notification or any other OSP Term(s) by any agent/employee or OSP can render the OSP liable for a monetary penalty of up to Rs. 5,00,000 per WFH location which is in violation. In addition to this, its OSP registration may also be cancelled by the DoT.

b. Can OSPs provide a secure VPN gateway from outside India for employees?

The WFH Notification is silent on this aspect. It only permits OSPs to use a secured VPN configured using static IP for any interconnection between the home agent position and the OSP centre. If read against the original conditions of availing the WFH facility under the OSP Terms, the DoT's intention under the WFH Notification seems to be to ensure that the employee is connected to the OSP centre's telecom resources only through a secure VPN provided by the OSP. Further, a plain reading of the conditions in the WFH Notification points to the interpretation that the secure VPN configured *by the OSP in India* should be used for any interconnection between the OSP centre and the pre-defined location of the employee. Several players in the industry whose VPNs are located outside of India have approached the DoT regarding clarification on using a VPN gateway from outside India.

c. Does this relaxation apply to all employees or only the employees who work at the OSP centre?

Any employee using the OSP centre's telecom resources to provide 'application services' to the customers will be considered an employee of the OSP and would have to be provided WFH subject to the conditions laid under the WFH Notification. A quick way to check this can be to look at the number of seats considered while filing the application for the OSP registration, and/ or ascertaining the number of employees providing 'application services' to the customers.

However, for employees who do not work at the OSP centre, i.e., employees who are out of the scope of the OSP Terms and subsequently this relaxation, companies can provide WFH to such employees under their own policies.

d. Can OSPs implement their own authentication and authorisation protocols for the employees of the OSP centre working from home?

Yes, there is no restriction on implementing authentication or authorisation protocols of the OSP in addition to the conditions under the WFH Notification. Companies can require their employees to adhere to a certain device policy, use a two-factor authentication or any other security protocol while working from home. In fact, the OSP Terms specifically permit the OSP's own authentication and authorization protocols over and above the security provided by the PPVPN.

– Special Economic Zones (SEZs)

1 Can IT/ITeS companies in SEZs allow employees to work from home?

Yes, the Special Economic Zone Act, 2005 and Special Economic Zone Rules, 2006 (SEZ Rules) (and collectively SEZ Regulations) permit the following categories of employees of IT/ITeS units to work from home:

1.1 Employees of IT/ITeS SEZ units and IT/ITeS units registered as OSPs with DoT;

1.2 employees temporarily incapacitated; and

1.3 employees who are travelling and offsite employees.

For other employees, there is no specific provision prescribed in the SEZ Regulations. It is therefore recommended that the Development Commissioner of the SEZ unit may be approached for permitting all employees to work from home along with permission regarding the duration/extension of such a set up.

Such permission should be obtained before extending work from home facilities to the employees and after the unit has verified its compliance with all work from home requirements (discussed below).

2 What are the compliance requirements that IT/ITeS units in an SEZ should follow in case employees work from home?

The SEZ Rules stipulate the following compliance requirements:

2.1 the work to be performed by the employee permitted to work from home should be as per the services approved for the unit, along with an ID card and the work should be related to a project of the unit;

2.2 the unit is required to provide a laptop/desktop and secured connectivity (for e.g. Virtual Private network, Virtual Desktop Infrastructure) for the employee to work on the project;

2.3 the unit must account for export revenue for the resultant work product/service and such work done from home should not be treated as export of service from outside the unit;

2.4 once the employee ceases to be a part of the project, the employee should be untagged from the project and the ID card should be surrendered to the specified officer; and

2.5 a list of employees along with their ID card numbers, asset identification numbers (laptops etc.) should be submitted to the specified officer.

3 Has the government provided any relaxations for compliances that are required to be met by units/developers/co-developers of SEZs?

Yes, the Department of Commerce by its Press Release dated 30 March 2020 has relaxed the following compliances:

3.1 requirement to file Quarterly Progress Report (attested by Independent Chartered engineers) by developers/co-developers

3.2 SOFTEX form to be filed by IT/ITeS units

3.3 filing of Annual Performance Reports by SEZ units

3.4 extension of Letter of Approvals (LoA) which may expire, in the cases of:

3.4.1 developers/co-developers who are in the process of developing and operationalising the SEZ;

3.4.2 units which are likely to complete their 5-year block for net foreign exchange assessment;

3.4.3 units that are yet to commence operations.

Development Commissioners of SEZs have been directed to ensure that no hardship is caused to developers/co-developers/units and no punitive action is taken in cases where any compliance is not met during this period.

To the extent possible, all extensions of LoAs and other compliances are to be facilitated through electronic mode in a time-bound manner. In the cases where it is not possible to grant extension through electronic mode or in cases where a physical meeting is required, Development Commissioners have been asked to ensure that the developer/co-developer/units do not face any hardship due to expiry of validity during this period of disruption. Ad-hoc interim extension/deferment of the expiry date may be granted without prejudice till 30 June 2020 or till further instructions of the Department on the matter, whichever is earlier.

– Software Technology Parks of India (STPI)

1 Can IT/ITeS companies registered as STPI units allow employees to work from home?

Yes, the STPI units can authorize employees to work from home.

The permission to work from home should be provided before extending work from home facilities to the employees and after the unit has verified its compliance with all work from home requirements (discussed below).

Further, the STPI has released a circular on 12 March 2020, enabling work from home for employees of STPI registered units due to the outbreak of COVID-19. The duration of such a set up should be clarified from the Development Commissioner of the STPI unit.

2 What are the compliance requirements that IT/ITeS units registered as STPI units should follow in case employees work from home?

The compliance requirements for work from home include the following:

2.1 there must be an authorisation from the unit specifying the duration of such authorization;

2.2 responsibility for carrying out the work and supervision, if any, will be that of the unit, which will be liable for any misuse;

2.3 export of the resultant products/services would take place only from the premises of the unit;

2.4 laptops/computers can be taken out of premises temporarily by authorized employees; and

2.5 persons authorized by software units may access facility installed in the STPI unit through communication links.

Exports

– Are there any relaxations that have been provided by the Reserve Bank of India (RBI) for realisation of export proceeds?

The RBI in its 'Master Directions – Export of Goods and Services' requires the value of goods or software exports to be realized fully by exporters and repatriated to the country within 9 months from the date of such export. However, due to the disruptions in business caused by the COVID-19 pandemic, the RBI has extended this period to 15 months from the date of export, to ensure that exporters are not in violation of the regulations and can negotiate future export contracts with buyers abroad based on this extension.

Essential goods/services

Considering the outbreak of COVID-19 in India, the MHA has ordered establishments both private and public to implement work from home. The MHA has also issued exemptions to the requirement for work from home for certain essential goods/services and a Standard Operating Procedure (SOP) to ensure the supply of essential goods.

– Are e-commerce companies, IT/ITeS units and data centres classified as essential services?

The MHA has classified the following services, among others, as essential services, which are exempt from the lockdown:

- Telecommunications, internet services, broadcasting and cable services, IT and ITeS (for essential services);
- Delivery of all essential goods including food, pharmaceuticals, medical equipment through e-commerce;
- Data and call centers for Government activities only; and
- IT vendors for banking operations, banking correspondent and ATM operations and cash management agencies.

– What constituents of the supply chain for essential goods/services have been permitted to operate as per the SOP?

The supply of essential goods taking place through local retail shops, organised retail stores and e-commerce companies are permitted to operate during the lockdown. To ensure smooth functioning of these three types of operators, the following constituents of the supply chain are also permitted to operate:

- Suppliers of essential goods, including restaurants supplying cooked food through home delivery;
- Warehouses, godowns etc. for the storage of essential goods;
- Inter-city or intra-city transport/loading of essential goods from warehouses to wholesalers/retailers;
- Manufacturing units of essential goods including pharmaceuticals, medical devices, their raw materials and intermediaries.

– Is there a procedure specified for the supply of essentials goods/services?

The following SOP is suggested for ensuring smooth supply of essential goods:

- All facilities in the supply chain of essential goods, whether involved in manufacturing, wholesale or retail, through local stores, organised retail stores of e-commerce companies should be allowed to operate, while ensuring strict social distancing;

- All such facilities, registered under the applicable Shops and Establishments legislations, can be randomly checked to verify the veracity of the documents produced;
- If non-essential goods are also stored in warehouses where essential goods are stored, such warehouses should not be asked to close down;
- The retail end of the supply chain should operate only in essential goods. Such operators are required to provide an undertaking and permit an audit of their records to ensure compliance;
- Employees or persons engaged in the supply chain should be allowed to commute based on e-passes or any other certification issued by the concerned local authorities along with a valid identification card;
- For the unorganised sector, employees/persons engaged will be permitted based on an approval/authorisation issued by the local authorities;
- These commercial entities should ensure that they engage only a bare minimum of staff to supply essential goods only;
- These facilities are required to carry out regular health and sanitation check-up of persons engaged and should provide protective gear; and
- The state governments are required to publish 24x7 helplines to register complaints/grievances.

– **Are e-passes being issued?**

Yes, e-passes for persons engaged in the supply of essentials goods/services are being issued state wise. Each state prescribes its own procedure for obtaining e-passes. The governments of Maharashtra, Karnataka, Delhi and Uttar Pradesh have started issuing e-passes. Local authorities have been tasked with issuing e-passes. While some states have enabled online applications, others require local authorities to be contacted for procuring the passes.
