ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

APRIL 2, 2020

What Does the Coronavirus Mean for Companies and Their Critical Offshore Services?

***by* Karen Sanzaro *and* Jim Harvey**

All industries and businesses have been impacted by the coronavirus pandemic. Most businesses in the U.S. have implemented at least some business continuity measures and have moved largely to a remote workforce for all but a skeleton crew in the face of lockdown orders and voluntary shelter-at-home measures. Given that many U.S.-based companies have sourced large parts of their operations to India and other jurisdictions, the impact of similar lockdowns and orders outside the United States adds yet more complexity to daily corporate life. In addition, these situations invoke the often deemphasized aspects of these agreements and relationships, including business continuity planning, force majeure provisions, and information security, as well as performance and service levels.

In India, the prime minister announced a near complete lockdown on March 24, 2020, including closing state borders and requiring residents and all nonessential workforce members to stay home for 21 days. There are exemptions designed to ensure the continued supply of essential goods, though these exemptions do not likely extend to the provision of services for customers or to supply chains outside India. Press reports indicate that local police are actively enforcing the lockdown.

What does this mean for India's considerable outsourcing industry and the foreign companies for whom they provide IT infrastructure, HR, payroll, accounting, call center support, and other critical services?

Various state governments have listed IT and IT-enabled services (ITeS) as essential services, allowing these establishments to continue to operate. In addition, India's Ministry of Electronics and Information Technology issued an advisory, also dated March 24, encouraging other state governments to permit critical staff working in IT and ITeS establishments supporting essential services, such as health care and banking, to continue working. These commercial entities are permitted to have only the bare minimum ("mission critical") staff necessary to supply essential goods. However, even with such a designation, these service providers will experience significant disruption – in their ability to operate their own businesses as well as their ability to continue to provide services to their customer base. The National Association of Software and Services Companies (NASSCOM), the trade association for India's IT and BPO outsourcing industries, is advising its members to assume that only a handful of staff will be allowed on site to operate data centers and support other mission-critical functions, and to "prepare for a complete lockdown and move all your assets immediately … to enable employees to Work from Home." While business continuity plans typically

contemplate the loss of a physical facility or location, in many cases – for Indian vendors at least – the backup or alternate location is located in another state in India.

While the recent lockdown order in India is front and center in news reports, similar concerns have arisen (or are likely to arise) in other offshore locations. With greatly reduced resources, vendors will be forced to triage support among their customers and the services provided to such customers. Companies that rely on offshore service providers (or offshore subsidiaries) should be prepared for significant service disruptions, at least in the short term. In addition, our clients report that vendors are requesting:

- Adjustments in, or relief from, implementation of business continuity / disaster recovery plans.
- Relief from restrictions on utilization of a remote workforce.[1]
- Relaxation of other contractually required security measures, including protections pertaining to personal information.
- Relief from service-level performance.
- Near complete waivers of liability arising out of the foregoing.

Companies facing these concerns need to assess risk and make decisions quickly. Understanding what rights and remedies are available in the relevant agreements will be important in making these determinations. Relevant provisions will likely include:

Governance

- Does the agreement establish a formal account governance structure?
  - Are the parties effectively leveraging this structure?
  - Is there a specific communication protocol that must be followed in a disaster or other crisis?
- Does the contract provide an expedited escalation method that allows for prompt resolution of issues?

Force majeure clauses

- Is there a force majeure or act of God provision?
- If so, does the provision excuse the vendor's delays in performance, or all vendor performance, caused by the pandemic? To the extent that aspects of the agreement or performance are governed under the laws of India, note that the government of India (via an office memorandum dated February 19, 2020) has categorized the coronavirus pandemic as a force majeure event for public procurement and other government contracts.
- To what extent does the provision excuse the company's performance? For example, would the provision permit the company to suspend or delay payment for services? Note that, pursuant to a supplemental (March 29) order, vendors in India must continue to pay employees during the lockdown, which may impact the vendor's willingness and ability to engage in these discussions.
- Is compliance with a business continuity or equivalent plan required to gain any protections afforded by the force majeure provision?

---

[1] Note that India has already softened "work from home" regulatory requirements applicable to telecom providers (referred to as Other Service Providers or OSPs), making it easier to utilize a "work from home" model – these accommodations remain in place through the end of April as stated here. Contractual restrictions will still apply, of course, but vendors will likely expect them to be waived to be in line with the easing of regulatory protections.

Service levels and service-level failure excused performance provisions outside of force majeure clauses

- What are the remedies for service-level failures (typically credits and termination rights)?
- Does the contract include a list of circumstances for which performance is excused (outside of or in addition to the force majeure clause)?
- If relief from service levels is requested, engage in a thoughtful review of the entire list of service levels and grant limited relief only where it makes sense for the customer. Any relief from service levels will, ideally, be limited to a date certain – rather than an amorphous statement of satisfaction of conditions on the ground or lifting of government restrictions. When that date approaches or has expired, the parties can engage in another conversation about the situation, results, and how to move forward.

Customer's step-in rights

- Does the contract provide the company with the ability to take over performance of services that the vendor is unable to provide?
- Is such a "step in" feasible operationally? Does the company have alternative resources that could actually perform the services to the extent necessary?
- What does the agreement say about expenses in the event of step in?
  - Do you continue to pay the vendor or just net out the expense of the alternative resources? Are there limitations or caps on what the vendor will reimburse for the alternative resources?

Disaster recovery and business continuity provisions

- These provisions are often seen as boilerplate, or overlooked, because the circumstances such provisions are designed to cover seem remote. This inattention often results in companies and their critical providers either failing to consider and develop the necessary contractual framework or failing to execute on the framework provided for in the agreement (development of plans, regular testing, etc.) and designed to address these circumstances.
- Does your agreement require the vendor to maintain a DR/BC plan specific to the services provided? If so, was such a plan prepared and approved?
- What are the vendor's obligations to notify and report in a disaster or business interruption? Is a post-mortem required once the dust has settled?
- Does the vendor have the ability to modify the plan without your approval, and if so, is there at least a requirement that any updates maintain a similar level of protection?
- We often try to negotiate provisions that prevent the vendor from prioritizing other customers during a disaster – does your agreement address the vendor's obligations to its other clients? Does the agreement (or the plan) address recovery based on criticality (e.g., of the application, service, or based on industry)?
- Does your force majeure provision excuse performance under the DR/BC plan? Is it a blanket excuse or only to the extent prevented by the disaster itself?
- Other considerations:
  - Does the DR/BC plan or the agreement address mobility issues of the vendor's workforce, such as travel restrictions and delays in visa renewal processing?
  - Does your agreement provide for regular (joint) testing of the DR/BC plans? And does it provide for adjustments to be made to address gaps identified during testing?

  - Have you actually engaged in regular testing? And does any such preparation appear to be assisting in current continuity efforts?
  - Are there express termination rights tied to disasters? Is a failure to implement the DR/BC plan designated as a material breach or otherwise subject to express termination rights? Does the agreement provide for a right to terminate in case of an extended disaster?
  - Does the DR/BC plan specify the trigger and process for returning operations to business as usual?

Information security requirements, including work from home and other workforce restrictions

- Consider whether and to what extent security measures can be relaxed and for how long.
- What data will be affected? Does the data include personal information or protected health information (PHI)?
- Which information security measures are mandatory (i.e., necessary to address compliance requirements (e.g., HIPAA, CCPA, or GDPR)) and which are discretionary?

Insurance coverage

- Are any of the company's losses or liabilities related to the vendor's nonperformance covered by the vendor's insurance?
- Are there specific restrictions in the insurance policy?

Liability / Indemnities

- Consider whether and to what extent invocation of force majeure measures will impact the parties' ability to invoke remedies and recover damages.
- Who bears the risk if a security incident occurs during a disaster?
  - Does the force majeure provide the vendor with absolution for incidents that occur during this time?
  - What if the parties agree to relaxed security measures, as discussed above? How is risk allocated? In considering a waiver of liability for any agreed-upon relaxation of security standards, be sure it is tightly crafted and time-bound.

Of course, this is not an exhaustive list. We recognize that each agreement and situation is unique, but hope that this helps frame some of the material issues as you navigate your way through this crisis.

Alston & Bird has formed a multidisciplinary task force to advise clients on the business and legal implications of the coronavirus (COVID-19). You can view all our work on the coronavirus across industries and subscribe to our future webinars and advisories.

You can subscribe to future ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333