Data Privacy and Work from Home Arrangements

The Philippine Government has placed the island of Luzon, where the National Capital Region is located, on Enhanced Community Quarantine. This requires residents to observe strict home quarantine. Exempted from the lockdown are essential enterprises such as those related to food and medicine production. Perhaps due to the significant contribution of the local BPO industry to the Philippine economy, outsourcing enterprises have also been given some leeway on maintaining staff at their work site, but by and large these enterprises have had to resort to WFH arrangements to continue providing services to customers. WFH arrangements trigger a number of legal and contractual issues, including, for PEZA registered BPOs, the removal from the PEZA Zone of equipment that had been imported duty free by reason of registration incentives.

Another key question is the impact on a BPO's compliance with data privacy undertakings. One question that has sometimes been posed is whether the quarantine and current extraordinary circumstances have "suspended" compliance with the local laws on data privacy, principally the Data Privacy Act of 2012 (DPA). The simple answer is: no. While, the Philippine National Privacy Commission (NPC) has not (as of the time of this bulletin's writing) released any statement or guidelines specifically addressing this point, Government has not declared any general suspension of the law's application. Instead, the NPC, since the start of the quarantine, has consistently cautioned institutions and persons to comply with the law .

In this regard, it may help to note that the DPA does not require the implementation of very specific security measures (except for certain organizational security measures such as the appointment of a Data Protection Officer, which should not be affected by work from home arrangements). The DPA and the relevant issuances of the NPC require the implementation of "appropriate" organizational, technical and physical security measures and provide general parameters. While the commission recommends covered entities to obtain certain certifications or accreditations, such as those that relate to ISO standards, these are not specifically mandated.

The challenge for BPOs would be to:

(i) formalize or adjust any existing work-from-home policies to ensure continued enforcement of physical, technical, and organizational security measures.

(ii) take steps to replicate the level of privacy and protection for data in a WFH setting so that measures continue to be appropriate. Some suggested best practices include:

- Regularly and consistently reminding employees of the need to ensure the security of personal information and other confidential data;
- Advising employees on how to avoid and handle phishing and similar attacks;
- Reviewing data breach and security incident response plans and to update if necessary; and
- Mandating regular password and login information changes

For more information, please contact:

Rose Marie M. King-Dominguez
rmmking@syciplaw.com

Franco Aristotle G. Larcina
fglarcina@syciplaw.com

(iii) review contracts with customers, and insofar as these provide for data handling that cannot be replicated under a WFH scenario, discuss and agree on this issue with the customer.

(iv) continue to monitor and audit the situation so that gaps are immediately identified and addressed.

[FIN]

Disclaimer

The foregoing does not constitute legal advice and provides only an overview of the matters discussed therein. In making any decisions, readers are advised not to rely on this material alone and should seek specific legal advice when necessary.

For more information, please contact:

Rose Marie M. King-Dominguez
rmmking@syciplaw.com

Franco Aristotle G. Larcina
fglarcina@syciplaw.com