ERGO

Analysing developments impacting business

DECODING THE NEW CERT-IN DIRECTIONS: GOVERNMENT RELEASES THE MUCH-AWAITED FAQS

20 May 2022

The Indian Computer Emergency Response Team (**CERT-In**) had issued directions on 28 April 2022 (**Directions**) on information security practices, procedure, prevention, response and reporting of cyber incidents for safe and trusted internet. On 18 May 2022, the Ministry of Electronics and Information Technology (**MEITY**) issued clarifications in the form of frequently asked questions (**FAQs**) in respect of the much talked about Directions. The FAQs have been released at a pivotal juncture, with just about 5 weeks left before the Directions come into effect.

Post the issuance of the Directions, various stakeholders have been in disarray with regard to its applicability and scope, and particularly relating to certain compliances like synchronisation of system clocks and enabling of logs. The FAQs have been released with an aim to explain the nuances of the Directions to the concerned stakeholders. However, it has been clarified that the FAQs have been released in response to general queries received by CERT-In and is not to be treated as a legal document which amends, alters or replaces the Information Technology Act 2000 (**IT Act**) and rules framed thereunder.

Key clarifications to the Directions

- *Covered Entities*: The FAQs clarify that the Directions are applicable to service providers, intermediaries, data centres, body corporate (which has the same definition as provided under the IT Act) (**Covered Entities**). There are certain additional obligations that are also applicable to virtual private server (**VPS**) providers, cloud service providers (**CSPs**), virtual private network (**VPN**) service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and government organisations. Importantly, individual citizens are not covered under the scope of these Directions.

- *Responsibility where multiple entities are involved*: If multiple parties (e.g., a consumer facing business and its backend/ outsourcing partner) are affected by a cyber security incident, any entity which notices the cyber security incident should report to CERT-In. Notably, this reporting obligation cannot be contractually transferred or dispensed with. Similarly, parties cannot seek indemnities in respect of non-compliance with the reporting obligation by their counterparties.

- *Reporting obligation overrides confidentiality restrictions*: The FAQs have stated that reporting of cyber security incidents to CERT-In is in the nature of a statutory obligation. Accordingly, it will not be subject to any confidentiality restrictions imposed by way of contractual obligations.

- *Extra-territorial applicability*: It has been clarified that the Directions are applicable to "*any entity whatsoever*", in the matter of cyber incidents and cyber security incidents, if the offence or contravention involves a computer, computer system or computer network located in India. Thus, it applies to foreign entities that serve Indian customers, including virtual asset service providers, virtual asset exchange providers and custodian wallet providers that are not located in India but catering to Indian users or may have infrastructure placed in India.

- *Synchronisation of system clocks*: The FAQs set out that there is no need to mandatorily set system clocks in Indian Standard Time (**IST**). Network Time Protocol (**NTP**) Server provides time stamp in coordinated universal time (**UTC**) and the conversion of UTC to local time is done at the host which receives the NTP sync from the NTP Server. National Physical Laboratory (**NPL**) or National Informatics Centre (**NIC**) also provides UTC time as per global norms. The Directions require uniform time synchronisation across all ICT systems irrespective of time zone. Customers in cloud environments, on the other hand, have an option to use the native time services offered by the cloud to synchronize their clock or they can also set up their own NTP server within their cloud environment. However, it has been reiterated that, a time source other than NIC / NPL, if used, must not deviate from NPL and NIC standards. The FAQs also stipulate the process through which system clocks can be synchronised with the NTP server of NIC and NPL.

- *Designation of a Point of Contact*: Covered Entities offering services to the users in India are required to designate a Point of Contact to liaise with CERT-In. Importantly, this obligation is not linked to whether an entity has a physical presence in India or not, as long as it provides services to users in India.

- *Reporting of cyber security incidents*: The FAQs clarify that entities may provide information to the extent available at the time of reporting and any additional information may be reported later within a reasonable time to CERT-In. Pertinently, the FAQs set out that any incident as stated in Annexure-I of the Directions and meeting certain specified criteria (such as incidents of severe nature, incidents impacting safety of human beings etc.) should be reported within the stipulated 6-hour time.

- *Compliance by data centres, VPS providers, VPN service providers and CSPs*: The FAQs provide some clarity in relation to the ambiguity on the obligation to register and maintain information about subscribers / customers. The FAQs indicate that such obligation does not apply to enterprise / corporate VPNs. For the purpose of the Directions, VPN service provider refers to an entity that provide "Internet proxy like services" through the use of VPN technologies, to general Internet subscribers/users. Further, with reference to the requirements of registering information by such entities, '*ownership pattern of the subscribers / customers hiring services*' has been clarified to mean basic information about customers/subscribers who use their services viz. individual, partnership, association, company etc. of whatsoever nature, with brief particulars of key management.

- *Storage of logs*: With respect to the requirement to store logs within the Indian jurisdiction, it has been clarified that the logs may also be stored outside India, as long as the obligation to produce logs to CERT-In is adhered to by the entities within a reasonable time. Hence, the logs need not be stored within India only. A copy of such logs is permitted to be stored in foreign jurisdictions as well.

- *Constituent of logs*: According to the FAQs, the constituents of logs that should be maintained depend on the sector that the organisation is in. The FAQs also prescribe an indicative list of logs to provide a flavour of the requirements. Additionally, it has been clarified that both successful as well as unsuccessful events shall be recorded.

Comment

While one cannot undermine the efforts taken by CERT-In to issue Directions in light of the increasing threat towards cyber-security and online safety, the Directions have been subject to a fair share of criticism for inter alia unrealistic timelines for breach reporting, excessive data retention and data localisation requirements, concerns relating to threat to privacy and mass surveillance etc.

As the effective date of the Directions inches closer, Covered Entities will be required to gear up and take appropriate measures to ensure compliance. Although the FAQs have been helpful to some extent in interpreting the Directions, the scope and impact of certain compliances continue to remain vague and unclear. In due course, it will be interesting to see how the implementation of the Directions in terms of the on-ground plays out.

- *Harsh Walia (Partner), Supratim Chakraborty (Partner), Shobhit Chandra (Counsel) and Sumantra Bose (Principal Associate)*

For any queries please contact: editors@khaitanco.com