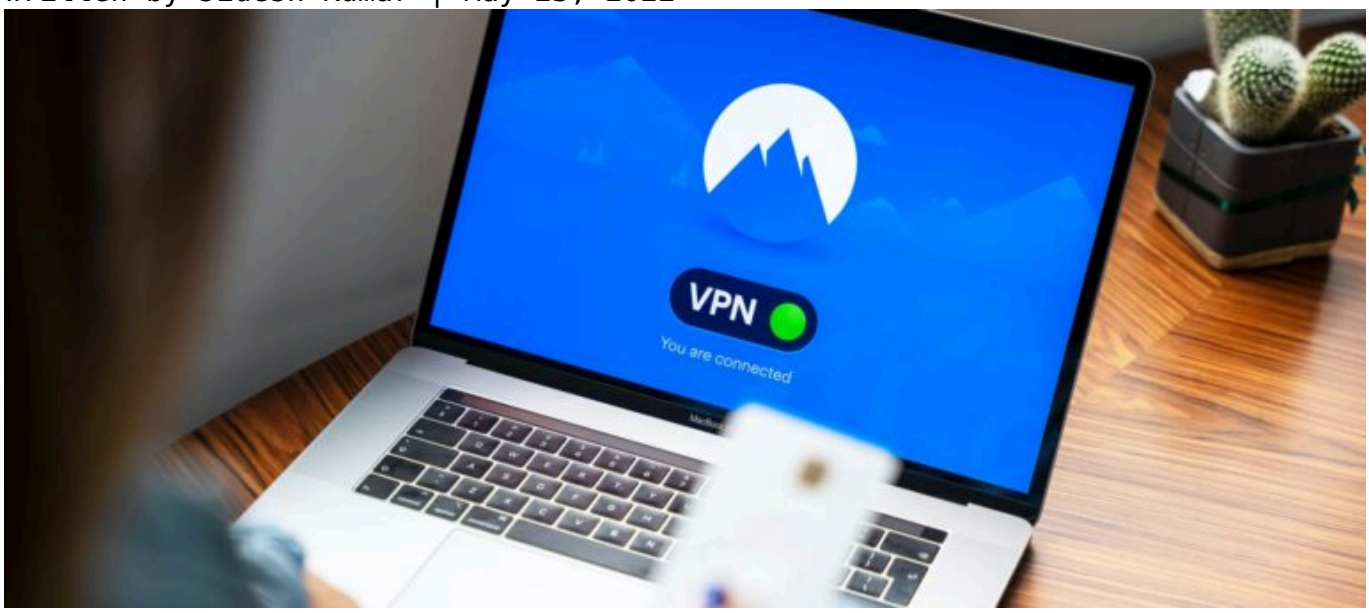
Impact Of New CERT Guidelines On VPN Service Providers & Users

written by Jidesh Kumar | May 23, 2022



CERT Guidelines on VPN

On 28 April 2022, the Indian Computer Emergency Response Team (CERT-In) issued certain directions under the powers granted to it under sub-section (6) of Section 70B of the Information Technology Act, 2000. These directions relate to information security practices, procedures, prevention, response, and reporting of cyber incidents.

CERT-In is the national nodal agency for performing the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incidents response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed.

These new directions require any service provider, intermediary, data centre, body corporate and government organisation to adhere to the following:

Mandatory Reporting Of Cyber Incidents

All the concerned stakeholders are required to report cyber incidents within six hours of noticing such incidents or being brought to notice about such incidents. But there is no clear definition of what action amounts to ‘noticing’ or ‘being brought to notice’. Additionally, these rules bring up quite a few questions that remain unanswered as of yet.

First is the uncertainty around who exactly the rules apply to. Are the rules directed only towards the VPN service providers who are catering to the general public? Or does it extend to enterprise and corporate VPN service providers as well? This would affect employees working from home connected to the corporate network through a VPN post the pandemic.

Mandatory Logging

This would require enabling the logs of all their ICT (Information Communications Technology) systems and maintaining them securely for a rolling period of 180 days.

The issue is that ICT is a very broad term. It behaves as an extensional term

for information technology, stressing the unification of communication and technology to allow users to access information.

The strict interpretation of this will mean maintaining all logs for a period of six months. It remains to be seen the liberal interpretation that will be termed permissible and considered as being in compliance by the Indian government.

Maintain All Logs Within Indian Jurisdiction

The government is justifying this move by stating that they are not interested in storing consumer data. Instead, they want the service providers to preserve the data, which then can be shared with the government only when legally required, under court orders or in criminal investigations.

Furthermore, there is the issue of jurisdiction. VPN service providers offer services to consumers within and outside India. Due to the government's push for data localisation, this might have a twofold effect. Not only will the Indian consumers be brought under the scope of this regulation but also those service providers with servers outside India will be exposed to the jurisdiction of Indian courts.

Additionally, companies will also be subject to Indian penal provisions. If any service provider, intermediary, data centre, body corporate or person fails to provide the information called for or comply with the guidelines, they shall be held punishable. This involves imprisonment for a term that may extend to one year or with a fine which may extend to INR 1 Lakh or with both.

Storage Of Data

VPN (Virtual Private Network) service providers, cloud service providers, data centres and VPS (Virtual Private Server) service providers shall be required to register and maintain the following information for a period of five years after any cancellation or withdrawal of the registration as the case may be:

- Validated names of subscribers or customers hiring the services
- Period of hire including dates
- IPs allotted to or being used by the members
- Email address, IP address and time stamp used at the time of registration or on-boarding
- The purpose for hiring the services
- Validated address and contact numbers
- Ownership pattern of the subscribers or the customers hiring the services

There is a lack of clarity on certain key issues. Ambiguity still exists around whether additional infrastructure has to be created to store the data. Or whether they are allowed to outsource the storage of data to third party data storage, retention and localisation service providers.

Further, the requirement for these service providers to register accurate information is also very vague. It remains unclear how they will ensure the accuracy of the data provided by the user. There might also be the requirement for additional costs to be incurred to ensure the accuracy of the information.

Lastly, the regulation makes it mandatory for the service providers to designate a POC (Point Of Contact) to interface with CERT-In. The directives remain, as of yet, vague when it comes to who can be a POC. Does the POC have to be an Indian resident or can they be an outstation personnel? Who can be a POC – an administrative contact of the company, a person with certain

authority or key management personnel? The regulations also □□keep mum on the issue of the POC being charged as an accused in the case of penal protection under the IT Act and Rules.

Challenges To Privacy Regime

While this regulation is for a number of service providers including cryptocurrency exchanges, VPN service providers look to be the most affected. The government's new directions listing down data localisation requirements and data retention guidelines have raised serious data privacy concerns

The bedrock principle of VPN networks is privacy and the current directives are clearly in conflict with those principles. The absence of formal privacy law has the authorities relying on various Supreme Court judgements, the IT Act, the IT Rules and Article 21 of the Indian constitution. This makes it challenging for industry players and service providers to comply with the guidelines.

Additionally, VPN service providers use various different technologies. In some of the existing networks, the storage of the logs remains non-existent. This means additional funding for the infrastructure and workforce to operate and maintain these services in India.

Strategise Your Way To Compliance

Since a lot remains unanswered, a need for a base legal strategy arises. This will help companies achieve compliance with the new regulation, in the event, there is no further clarification from the government. This base legal strategy contains the following steps:

- Change or amend the privacy policy of the VPN service providers and obtain additional consent of customers by a clickwrap, shrink-wrap or other acceptance and consent formats to avoid any liability.
- Create servers in India and add infrastructure, processes and even resources to comply with the rules.
- Modify KYC norms of the customers to comply with the additional data capture requirements.
- Create an internal policy to comply with the regulation.
- Change the values on which the VPN system is created. The push for data localisation and retention would require VPN service providers offering services within India to alter their values to suit Indian legal requirements.
- Designate a person in India to act as a POC to communicate with CERT-In.

Contributed by Jidesh Kumar, Managing Partner (jidesh@ksandk.com)

Disclaimer: This article was originally published on INC42