SPICE ROUTE
LEGAL

CLOUD GOVERNANCE 101: PUBLIC PROCUREMENT OF CLOUD SERVICES

INTRODUCTION

The cloud service industry in India has generally been an unregulated space, despite multiple attempts by the government over the past decade to introduce legal and policy frameworks. The National Telecom Policy, issued by the Department of Telecommunications in 2012, was one of the first policy attempts that addressed the need to adopt cloud computing. In 2018, the Digital Communications Policy replaced the 2012 policy with an aim to establish India as a global hub for cloud computing and create a light touch regulatory framework for the industry. Simultaneously, the Telecom Regulatory Authority of India – the nodal telecom regulator – released two consultation papers between 2017 and 2019, with recommendations on cloud services, a proposal for a regulatory framework, and suggestions on the establishment of an industry body to govern and regulate cloud service providers in India. The recommendations were met with significant opposition from leading market players and were put on hold.

Today, there is no single regulation or legal framework that governs cloud services. Nevertheless, cloud services designed for government agencies are not a free-for-all, and certain government initiatives impose obligations on providers that offer cloud solutions to such agencies. This note provides an overview of the regulatory requirements for organisations that seek to provide cloud services to public sector players in India.

THE MEGHRAJ CLOUD INITIATIVE

In 2014, the Ministry of Electronics and Information Technology ("**MeitY**") introduced a national government cloud initiative called "MeghRaj". MeghRaj was intended to utilise and harness the benefits of cloud computing and ensure the proliferation of cloud services among government departments and public sector undertakings in a manner that enhanced their e-governance frameworks.

As part of this initiative and specifically to facilitate government procurement and adoption of cloud computing services, MeitY introduced a series of guidelines ("**MeitY Guidelines**") to highlight key considerations – particularly, data protection and security compliance requirements – for public procurement of cloud services.

APPLICABILITY OF THE MEITY GUIDELINES

The MeitY Guidelines apply to cloud service providers ("**CSPs**"), managed service providers, and system integrators that provide cloud services to government organisations, departments, agencies, ministries, autonomous institutions, statutory bodies, offices under the Government of India, states, and union territories, local governments, public sector undertakings, and nationalised banks within India (collectively, "**Government Departments**").

Government Departments are permitted to procure cloud services directly (a) from CSPs that are "empaneled" with MeitY, (b) through managed service providers ("**MSPs**"), or (c) through systems integrators ("**SIs**"). The General Financial Rules, 2017 clarify that Government Departments may only procure cloud services from empaneled CSPs registered on the Government e-Marketplace platform. In contrast, MSPs and SIs control and manage cloud services provided by empaneled CSPs but are not required to be empaneled themselves. The burden of ensuring compliance with empanelment requirements, registration requirements, and the MeitY Guidelines falls on the service provider. Any violation of these requirements may result in the temporary or

permanent suspension of the service provider or de-empanelment of the CSP, in addition to other legal and contractual remedies available to the Government Department.

CSPs can apply to be empaneled for different service models (i.e., IaaS, PaaS, and SaaS) and deployment models (these include public clouds, virtual private clouds, and government community cloud models). Different deployment models are required to comply with different technical requirements. As a baseline requirement, CSPs are required to mandatorily offer a set of "basic cloud services" (for example, virtual machines, database services, storage services, network and security services, etc.) to be empaneled. However, the provision of "advanced cloud services" (for example, data warehousing services, analytics services, and managed services like disaster recovery) is optional, and may be offered by CSPs at additional costs.

Since 2016, MeitY has conducted four rounds of empanelment of CSPs, the most recent of which, ended on August 31, 2021. An approved empanelment application remains valid for three years.

The MeitY Guidelines do not regulate private sector procurement of cloud services.

EMPANELMENT PROCESS

MeitY's empanelment process involves a detailed audit and assessment of the applicant. Once empaneled, MeitY conducts a surveillance audit of the CSP annually.

The empanelment process consists broadly of the following steps:

(a) An applicant submits an application form and details of the proposed cloud services in accordance with the format prescribed in the application document.

(b) MeitY conducts an initial assessment and compliance check to confirm the submission of all requisite documents.

(c) Upon a successful completion of the initial assessment, the applicant is required to have its cloud service offerings and data centres audited by the Standardisation Testing and Quality Certification ("**STQC**") which is a MeitY office that determines compliance with MeitY-prescribed data protection and security requirements and standards.

(d) If the applicant successfully passes the STQC audit, MeitY issues a letter of award that certifies the empanelment and publishes details of the applicant on its website. A list of current providers empaneled with MeitY is available here.

THE GEM PLATFORM

In 2016, the Indian government established a Government to Business ("**G2B**") online platform called the Government e-Marketplace ("**GeM**") that aimed to make public procurement a transparent process. GeM functions as an online portal for the procurement of goods and services, where sellers can register and bid for government contracts and provide such goods and services. Empaneled CSPs, MSPs, and SIs are mandatorily required to register themselves on the GeM platform and comply with the standard GeM terms and conditions

to offer cloud services to Government Departments. These departments may, in turn, procure such services either through the GeM marketplace or through bid and reverse auction facilities available on the GeM platform.

Foreign entities are not permitted to directly sell their products or services on the GeM platform but must appoint and authorise distributors to sell and provide services on their behalf. Once authorised, distributors are required to comply with a detailed vendor assessment, and upon successful completion, may sell their products or services on the platform.

DATA PROTECTION, SECURITY, AND LOCALISATION REQUIREMENTS

In addition to general compliance with the legal requirements imposed under the Information Technology Act, 2000 and the rules issued under it, CSPs that seek to be empaneled under the MeghRaj initiative must fulfil detailed data protection, security, and other legal requirements prescribed by MeitY.

This includes compliance with security standards that include ISO 27001:2017 and 20000-1:2018 (for data center facilities), Cloud Security ISO Standard ISO 27017:2015, and Privacy Standard ISO 27018:2019. Additionally, CSPs must provide an intrusion detection system, deploy anti-malware tools, and implement service and operational management processes and procedures, incident management procedures, backup services, cloud storage requirements, and disaster recovery and business continuity plans. MeitY requires CSPs to contractually impose these obligations on their subcontractors and sub-processors as well.

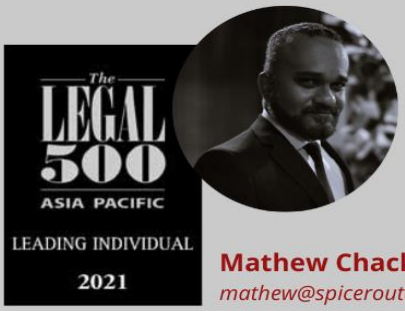
Perhaps the most crucial aspect of the MeitY Guidelines is the data localisation requirement, which is in line with the Indian government's overarching stance on data sovereignty and heightened security requirements for data held by Government Departments. All data functions and processing activities undertaken by CSPs must only be carried out within India, and the export of any type of data (including backups), is prohibited.

CONCLUSION

MeitY's empanelment process is detailed, fastidious, and imposes heightened obligations on cloud service providers that aim to contract with or otherwise offer solutions to players in the public sector. Accordingly, before seeking to tap into the public procurement processes, organisations that offer cloud services ought to undertake internal diligences to ensure that they are compliant with MeitY's requirements.

SPICE ROUTE
LEGAL

For any queries, please reach out to:



Mathew Chacko
mathew@spiceroutelegal.com

Aadya Misra
aadya.misra@spiceroutelegal.com

Samyukta Ramaswamy
samyukta.ramaswamy
@spiceroutelegal.com

Ada Shaharbanu
ada.shaharbanu
@spiceroutelegal.com

Shambhavi Mishra
shambhavi.mishra
@spiceroutelegal.com

Anubhav Das
anubhav.das
@spiceroutelegal.com