T0: Telecom Regulatory Authority of India
RE: Comments on TRAI Consultation Paper on Cloud Services

CONTEXT:

Our comments are based on our experience as a leading global cloud service provider ("**CSP**"). AWS currently operates in 190 countries, and provides services to millions of private and public sector customers. AWS holds a host of industry-recognized certifications and audits, such as PCI DSS Level 1, ISO 27001, FedRAMP, HIPAA, and SOC 1 and SOC 2 audit reports. AWS had also submitted its comments to TRAI's earlier consultation paper on cloud computing, released in 2016.

RESPONSE TO QUESTIONS:

1. **Question 1: Whether there should be single industry body or multiple industry bodies of cloud service providers which may be registered with DoT? If multiple industry bodies, whether there should be any cap on their number? Should the industry bodies be registered based on the category or type of CSPs? Can a CSP be a member of multiple industry bodies? Please suggest with justification.**

   We submit that cloud service providers ("**CSPs**") in India should not be subject to regulation by the Department of Telecommunications ("**DoT**") or the Telecom Regulatory Authority of India ("**TRAI**"), directly or indirectly. CSPs are already subject to various existing Indian laws and should not be governed by the TRAI or the DoT, for the reasons described below:

[A] TRAI and DoT do not have the remit to formulate and implement a regulatory framework for CSPs:

a. The Ministry of Electronics and Information Technology ("**MeitY**") is tasked with developing policies for information technology and the Internet under the Allocation of Business Rules[1]. While cloud computing is provided using the infrastructure of the telecom licensees as an information technology service, it is an IT related service, and consequently, governance of CSPs in any form falls squarely within the jurisdiction of MeitY. It is in fact regulated under the Information Technology Act, 2000 ("**IT Act**"), and will be regulated under the proposed Personal Data Protection Bill, 2018.

b. On the other hand, the scope of work of the DoT and the TRAI specifically covers only telecommunication related matters. Under the Allocation of Business rules[2], the DoT deals with "policy, licensing and coordination matters relating to telegraphs, telephones, wireless, data, facsimile and telematics services and other like forms of communication". TRAI's functions relate to telecommunication services, telecom service providers licensed under the Indian Telegraph

[1] Pg. 51, Government of India (Allocation of Business Rules) 1961 (as amended up to 04 April 2019), *available at* https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_1829.pdf ("Allocation of Business Rules") [MeitY- Policy matters relating to information technology; Electronics; and Internet (all matters other than licensing of Internet Service Provider); Promotion of internet, IT and IT enabled services].
[2] Pg. 34, Allocation of Business Rules.

Act, 1885, and the telecom sector[3]. As a result, cloud services do not fall within the scope of telecommunication services. This approach mirrors global regimes in free societies where telecom regulators do not prescribe regulatory requirements for CSPs.

[B] The telecom infrastructure used for providing cloud services is already regulated:

Cloud services are accessed by customers through network infrastructure, which is a communication service regulated by the DoT. CSPs also use telecom infrastructure for connecting their data centres. Such infrastructure, and telecom service providers providing such infrastructure, are extensively regulated by the DoT and TRAI. The pricing, interconnection, network architecture, legal intercept, and monitoring, etc. at the telecom layer is sufficiently regulated by the DoT and the TRAI. These regulations adequately serve the purposes of protecting customers, maintaining public network security and integrity, and enabling the Government to monitor and obtain information on transmission of data (e.g., for national security purposes). Thus, CSPs need not be licensed/regulated separately through additional measures imposed by TRAI/DoT.

[C] CSPs are sufficiently regulated under existing laws:

CSPs are already subject to several existing laws and as a result, there is no compelling reason to have an additional regulatory framework applicable to only CSPs. We note in the table below the manner in which CSPs are already adequately regulated under important regulatory regimes, such as data protection, consumer protection, telecom, and privacy. As a result, there is no harm which is left unregulated or uncontrolled, whose mitigation is desirable trough regulation of CSPs. Even during the consultation stage, the need for regulating CSPs did not specifically come out as there is no harm that is proposed to be addressed for such regulation. Moreover, outside of a regulatory perspective, competition among CSPs in creating value for customers, the existing best practices of the industry, consumer protection laws ensure that the customers are able to receive adequate protection in the CSP's services provided to them. As there is no specific need for introducing a new regulatory framework, such a framework will amount to overregulation and will merely increase the costs and efforts of CSPs, ultimately resulting in higher costs for all Indian customers.

No.	Relevant authority/legislation	Key provisions
a.	The Information Technology Act, 2000 ("**IT Act**"), including the various rules under the IT Act	(i) CSPs need to implement reasonable security practices and procedures, which govern collection, disclosure, retention, transfer, security and use of personal and sensitive personal information or data (Section 43A). (ii) CSPs can be directed to co-operate with authorised government agencies to facilitate electronic surveillance and access to information on their computer resources (Section 69) (iii) CSPs qualify as 'intermediaries' under the IT Act, and are subject to a wide range of due diligence requirements. Failure to comply with these

[3] Section 11, The Telecom Regulatory Authority of India Act, 1997, https://main.trai.gov.in/sites/default/files/The_TRAI_Act_1997.pdf.

No.	Relevant authority/legislation	Key provisions
		requirements will result in CSPs losing safe harbour protection under the IT Act (Section 79).
b.	MeitY	MeitY already governs empanelment of CSPs as government-approved service providers under its 'MeghRaj' cloud computing initiative [4]. To be empaneled, CSPs must demonstrate compliance with standards on security, interoperability, data portability, service level agreements, and contractual terms and conditions[5]. Compliance by CSPs is verified through a rigorous audit conducted by the MeitY's Standardisation Testing and Quality Certification Directorate[6]. Any entity choosing to obtain benefits of being empanelled by MeitY must therefore meet these high standards.
c.	Indian Contract Act, 1872	The e-contracts entered into by CSPs with their users are subject to the provisions of the Indian Contract Act, 1872. As a result, CSPs are bound by such contractual obligations (as per section 37 of the Indian Contract Act, 1872) with respect to their provision of cloud services in India.
d.	Consumer Protection Act, 2019 ("**CPA**")	(i) CSPs would fall under the definition of an 'electronic service provider' under the CPA [Section 2(17)] (ii) Buying or selling of cloud-based services would qualify as e-commerce under the CPA [Section 2(16)] (iii) The central government is empowered to take measures for the purposes of preventing unfair trade practices in e-commerce. Such measures may relate to the trade practices of CSPs (Section 94)
e.	Personal Data Protection Bill, 2018 ("**PDP Bill**")	CSPs will be subject to a number of obligations as 'data processors' under the PDP Bill. These include: (i) Processing data only as per instructions of data fiduciaries by whom the CSP has been engaged (Clause 37)

[4] GI Cloud (Meghraj) - A cloud computing initiative of MeitY, *available at* http://meity.gov.in/content/gi-cloud-meghraj. ("MeitY cloud computing initiative")

[5] Invitation for application/proposal for empanelment of cloud service offerings of CSPs, Ministry of Electronics and Information Technology, Government of India, *available at* http://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf.

[6] MeitY cloud computing initiative.

No.	Relevant authority/legislation	Key provisions
		(ii) Implementing appropriate security safeguards through use of methods such as encryption and de-identification of data (Clause 31) (iii) Possibly complying with 'codes of practice' issued by the Data Protection Authority under the PDP Bill (Clause 60)
f.	Device regulations	Devices used by CSPs are subject to licensing and registration regimes in India. For instance, Bureau of Indian Standards requires compulsory registration of certain electronic and information technology goods. Additionally, the Wireless Planning and Commission Wing of the DoT issues licenses for possession, import and dealing of wireless devices in India. The Mandatory Testing and Certification of Telecom Equipment, administered by the Telecommunications Engineering Center requires notified telecom equipment to undergo prior mandatory testing and certification for their use in India. Any devices falling within the scope of such frameworks being used by CSPs must meet the applicable criteria.

(Please see Annexure I for detailed information about the existing Indian laws applicable to CSPs)

The government has also taken pro-active efforts to ensure that these laws are updated with time. For instance, in August 2019, the government completely overhauled the old legislation on consumer protection and notified the CPA[7]. Similarly, the government is currently in the process of finalising[8] amendments to the Information Technology (Intermediaries Guidelines) Rules, 2011 under Section 69 of the IT Act.

Apart from this, there are several sectoral regulations which indirectly govern the cloud such as the Reserve Bank of India ("**RBI**") and the Insurance and Regulatory Development Authority of India ("**IRDAI**"). Each of the sectoral regulators already deal with cloud computing as part of their outsourcing guidelines and IT policies to ensure that sector specific requirements and needs are met in an appropriate manner. Given existing protections afforded to Indian customers, sufficient regulation exists currently and a co-regulation model is unwarranted.

[D] Cloud services form a part of a growing market segment and must not be subjected to extensive regulation that could hamper availability of cost-effective cloud services to Indian customers

As noted in section 2 of this document, CSPs are already subject to and required to comply with a number of laws in India. There is no clear reason why CSPs and the cloud industry in general must be

[7] Consumer Protection Act, 2019, http://egazette.nic.in/WriteReadData/2019/210422.pdf.

[8] https://economictimes.indiatimes.com/tech/internet/process-of-notifying-intermediary-rules-likely-to-be-completed-by-january-15-2020-meity-to-sc/articleshow/71689301.cms

subject to specialised regulations when they are already compliant with applicable laws, such as data privacy and information security, which apply to all other computer systems functioning in India. Cloud technology is constantly evolving and improving in efficiency and costs. This is possible due to the fact that CSPs need not spend time and money on extensive regulatory compliances at the time as they introduce new innovative changes to their services and technologies.

The government should consider CSPs as regular business entities, which are registered to conduct business in India under its existing laws. As per a NASSCOM report[9], highly efficient cloud spending in India is estimated to grow at 30% p.a. to reach USD 7.1-7.2 billion in 2022. In 2019 itself, India's public cloud services will record the third-highest growth rate globally[10]. In order to ensure unhindered growth and innovation in the cloud services market segment in India, CSPs should not be subject to any further regulation through an industry body or otherwise. Such regulation would raise costs for Indian customers and impede India's goal of becoming a global hub for cloud computing, content hosting and delivery[11].

[E] The TRAI consultation paper does not propose light-touch regulation:

a. **TRAI has previously recommended a 'light touch' approach for regulation of CSPs:** In 2017, the TRAI had expressly recommended adopting a 'light touch regulatory approach' for cloud services after a stakeholder consultation [12], on account of stakeholders' concerns that licensing/registration of CSPs could be counterproductive and restrict inventions. In TRAI's view, articulated in the recommendations, a light touch approach would allow the cloud services industry to grow while addressing any consumer concerns. Following a similar approach, the National Digital Communications Policy seeks to enable a "light touch regulation for the proliferation of cloud based systems"[13].

b. **TRAI's consultation paper departs from its own recommendations for a light-touch approach:** Some proposals in the present consultation paper indicate that instead of following TRAI's recommendation of a 'light touch' approach, the DoT would exercise regulatory control over CSPs indirectly. For example, both the registered industry body and its CSP members 'may' be required to comply with the orders/directions issued by the DoT. The industry body and CSP members may also be required to furnish such information as is sought by the DoT/TRAI[14]. The paper also prescribes mandatory provisions for the code of conduct of the industry body[15]. The code of conduct covers various aspects of the industry body, such as membership and working groups to be formed. It also covers various aspects of CSPs such as quality of service parameters, billing and dispute resolution framework. Instead of promoting a 'light touch regulatory approach', such

[9] Cloud- Next wave of growth in India 2019, NASSCOM, April 2019, https://www.nasscom.in/knowledge-center/publications/nasscom-cloud-next-wave-growth-india-2019

[10] Gartner Forecasts Public Cloud Services Revenue in India to Grow 24% in 2019, Gartner, 18 June 2019, https://www.gartner.com/en/newsroom/press-releases/2019-06-18-gartner-forecasts-public-cloud-services-revenue-in-in0

[11] Para 2.2, pg. 12, National Digital Communications Policy, 2018, Department of Telecommunications, Government of India, http://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf.

[12] Pg. 36, para 4.1(i), chapter 4, TRAI Recommendations on cloud services, 16 August 2017, https://main.trai.gov.in/sites/default/files/Recommendations_cloud_computing_16082017.pdf.

[13] Para 2.2(f)(ii), pg. 12, National Digital Communications Policy, 2018, Department of Telecommunications, Government of India, http://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf.

[14] Paragraphs (i) and (j), Annexure-I, TRAI consultation paper on cloud services, 23 October 2019, https://main.trai.gov.in/sites/default/files/CP_23102019.pdf.

[15] Annexure-I, TRAI Consultation Paper.

provisions would curb the freedom of CSPs. In fact, the current proposals are similar to an indirect licensing regime, which will hamper further growth of the sector.

We submit that the industry bodies discussed in the consultation paper are very different from the industry body proposed by TRAI. These industry bodies, such as the Cloud Industry Forum and Cloud Computing Innovation Council of India: (i) have completely voluntary membership models; and (ii) do not envisage any kind of government intervention in their functioning (Please see Annexure II for more details).

In any case, AWS suggests conducting a regulatory impact assessment study to understand the need, if any, for and impact of a regulatory framework on India's growing cloud services industry[16], especially in terms of business cost.

Since CSPs are already regulated by existing laws and form a part of a growing yet rapidly evolving field, we see no need, and consultation has so far not identified a need , for any regulatory intervention by DoT/ TRAI, through an industry body or otherwise. Any additional regulation will create overlapping or conflicting requirements and result in avoidable additional business costs for CSPs and ultimately Indian customers, thereby hampering their innovation and growth in India.

While the TRAI has referred to a number of international bodies of CSPs such as the Asia Cloud Computing Association, EU Cloud CoC, Cloud Industry Forum, etc., these bodies are not co-regulatory in nature, merely have voluntary membership, and conduct related structures with no governmental influence. Due to the assistance of such bodies and in the absence of strict regulatory frameworks for CSPs, the industry has flourished worldwide through its freedom to self-regulate and the support extended to industry players by such organisations.

Both the Union government and various state governments have been coming out with policies such as Digital India to increase India's digital economy, and the purported role of the cloud industry in these efforts is significant. The National Digital Communications Policy, 2018 highlights the Government of India's key interest in "*establishing India as a global hub for cloud computing, content hosting and delivery, and data communication systems and services*". The vision of the Digital India campaign extensively relies on using cloud services to provide benefits of digital lockers, storing citizen entitlements and government documents for each and every citizen.

Several states in India are incentivising investments in data centers and the cloud industry through ICT policies and, in cases such as Telangana, by having specific Data Center policies. Additional regulatory requirements would have the unfortunate effect of slowing down investments in these areas when they should be ramping up.

A co-regulation model does not exist in other countries and having a stringent co-regulatory mechanism will affect the development of the cloud industry, and the cost of providing these services to customers in India will increase. This will, needless to say, affect India's ability to be a sought-after destination for providing cloud services to customers worldwide. There is no pressing reason at this time for India to put

[16] The TRAI can also consider looking at other best practices as prescribed by the International Telecommunications Union (ITU); see "Fast forward digital connectivity for all", 2019 Best Practice Guidelines, Global Symposium for Regulators, https://www.itu.int/en/ITU-D/Conferences/GSR/2019/Documents/GSR19_BPG_V2_E.pdf.

in place any co-regulation with respect to CSPs, especially if India has the opportunity to become a global leader in cloud computing. Such requirements will function as barriers to new entrants and to innovation in the marketplace and are thus less conducive to the scaling of existing players and the entry of new ones in the cloud computing sector in India.

2. **Question 2: What should be the eligibility criteria for an Industry body of CSPs to register with DoT? What is the list of documents that should be required to be submitted as proof of eligibility? What obligations should be cast upon the Industry Bod(y)(ies) after registration with DoT? Please suggest with justification.**

3. **Question 3: What may be the threshold value of parameters such as the volume of business, revenue, number of customers etc. or combination of these for a CSP to mandatorily become member of a registered Industry body? Please suggest with justification.**

4. **Question 4: Whether entry fee, recurring fee etc., need to be uniform for all members or these may be on the basis of type or category of members? How such type or category can be defined? Should such fee be prescribed by DoT or be left to be decided by the Industry body? Please suggest with justification.**

5. **Question 5: What should be the guiding principles for governance by an industry body? How would these principles/ organisation structure ensure fair, reasonable and non-discriminatory functioning of body? Should structure of Governance be prescribed by DoT or should it left for the industry body to decide? How can the industry body achieve the desired deliverables efficiently and effectively? Please suggest with justification.**

6. **Question 6: What policy may be adopted for initial formation of industry body for cloud services? Please suggest with justification.**

7. **Question 7: Any other issue which is relevant to this subject? Please suggest with justification.**

Response to Questions number 2 to 7: Please see our response to Question 1. CSPs are already adequately governed by the MeitY and are subject to existing laws. Moreover, there is no identified compelling harm that further regulation is mean to address. Any additional regulation by DoT/ TRAI, through an industry body or otherwise, would amount to over-regulation and, further, creates the risk of overlapping or conflicting regulatory regimes. This will hinder growth of cloud services in India and increase the costs of cloud services for Indian customers. For the growth of the Indian economy, it is important that the government places an emphasis on supporting the cloud sector in India. This growth will be supported by leaving the sector unregulated by a specific framework, thus incentivising players to develop and innovate their services in the most efficient manner possible and to compete by creating the highest value for Indian customers. Additional regulatory requirements would have the unfortunate effect of slowing down investments in these areas where they should be ramping up. As opposed to regulation by TRAI, DoT etc., efforts by CSPs to meet the industry best practices to remain competitive are more conducive to the market's needs and will result in sustainable and significant growth in the CSP market segment in India.

ANNEXURE-I: EXISTING LAWS APPLICABLE TO CLOUD SERVICE PROVIDERS IN INDIA

This note provides a detailed overview of the existing laws and regulations that currently govern CSPs in India, to demonstrate that the country's cloud computing sector is sufficiently well regulated. For this purpose, we have examined the following laws:

1. Information Technology Act, 2000 ("**IT Act**"), including the following rules under the IT Act:

    a. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**");
    b. Information Technology (Intermediaries Guidelines) Rules, 2011 ("**Intermediaries Guidelines Rules**");
    c. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**Electronic Surveillance Rules**");
    d. Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("**Traffic Data Rules**");
    e. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("**Blocking Rules**");
    f. Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**CERT Rules**");
    g. Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 ("**NCIIPC Rules**") read with the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 ("**Protected Systems Rules**");
    h. Information Technology (Electronic Service Delivery) Rules, 2011 ("**Electronic Service Delivery Rules**");
    i. Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016. ("**Digi-Locker Rules**"),

2. Consumer Protection Act, 2019.

In addition, we have also studied the Personal Data Protection Bill, 2018 ("**PDP Bill**"), as the regulatory framework prescribed under it will also apply to CSPs once it is adopted as enforceable law.

TABLE 1: REGULATION OF CSPS UNDER THE IT ACT

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	CSPs can be authorised, for the purpose of delivery of services to the public through electronic means, to: (i) set up, maintain and upgrade their computerised facilities; (ii) perform specified services; and (iii) collect, retain and appropriate specified service charges, through an order of the central government or any state government.[17]	Section 6A, the IT Act.

[17] Section 6A, the Information Technology Act, 2000.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
2.	Contracts formed through electronic means are valid and enforceable, as provided under Section 10A of the IT Act.[18] Thus, all e-contracts that CSPs are party to, such as click-wrap agreements and terms of use, are enforceable and valid, provided they comply with the requirements of the Contract Act. As a result, any rights and liabilities agreed upon under such contracts will bind CSPs and their consumers.	Section 10A, the IT Act.
3.	Section 43A of the IT Act[19] along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**")[20] requires CSPs to implement reasonable security practices and procedures. This framework comprehensively covers all data management activities of a CSP including the collection[21], disclosure[22], retention[23], transfer[24], security[25], and use of sensitive personal information or data[26]. Additionally, CSPs will also be regulated by the exhaustive data protection and privacy safeguards under the proposed PDP Bill, once it is enacted.	Section 43A, the IT Act read with the SPDI Rules.
4.	If CSPs contravene any rules or regulations made under the IT Act, for which no penalty has been separately prescribed, they can be liable to pay up to INR 25000 for such contraventions.	Section 45, the IT Act.
5.	If CSPs access or secure access to a computer, computer system, computer network or computer resource without the permission of the owner or any other person who is in charge, of such computer, computer system, computer network or resource, they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSPs involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(a) read with Section 66, the IT Act.
6.	If CSPs download, copy or extract any data, computer data base or information from such computer, computer system, computer network or removable storage medium (as *referred to in point 6 above*), they can be required to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSPs involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(b) read with Section 66, the IT Act.
7.	If CSPs person introduce any computer contaminant[27] or computer virus[28] into such computer, computer system or computer network (as *referred to in point*	Section 43(c) read with

[18] Section 10A, the Information Technology Act, 2000.

[19] Section 43A, IT Act.
[20] SPDI.
[21] Rule 5, SPDI Rules.
[22] Rule 6, SPDI Rules.
[23] Rule 5, SPDI Rules.
[24] Rule 7, SPDI Rules.
[25] Rule 8, SPDI Rules.
[26] *See* Rules 4, 5, 6, 7 and 8 of the SPDI Rules..
[27] *Per* the explanation to Section 43, "computer contaminant" means any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network.
[28] *Per* the explanation to Section 43, "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	6 above), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSPs involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 66, the IT Act.
8.	If CSPs are responsible for destroying, altering, deleting, adding, modifying or rearranging any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network (as *referred to in point 6 above*), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(d) read with Section 66, the IT Act.
9.	If CSPs disrupt or cause the disruption of any computer, computer system or computer network (as *referred to in point 6 above*), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(e) read with Section 66, the IT Act.
10.	If CSPs deny access or cause the denial of access to any person authorise d to access any computer, computer system or computer network by any means (as *referred to in point 6 above*), they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(f) read with Section 66, the IT Act.
11.	If CSPs provide any assistance to any person to facilitate access to a computer, computer system or computer network (as *referred to in point 6 above*) in contravention of the provisions of the IT Act or rules framed thereunder, they may have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(g) read with Section 66, the IT Act.
12.	If CSPs charge the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network (as *referred to in point 6 above*), they will have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(h) read with Section 66, the IT Act.
13.	If CSPs destroy, delete or alter any information residing in a computer resource as referred to in point 6 above or diminish its value or utility or affect it injuriously by any means, they shall have to pay damages to the person so affected. If this is done dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	Section 43(i) read with Section 66, the IT Act.
14.	If CSPs steal, conceal, destroy or alter any computer source code used for a computer resource as referred to in point 6 above with the intention to cause damage will have to pay damages to the person so affected and this is done	Section 43(j) read with Section 66, the IT Act.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	dishonestly or fraudulently, the CSP involved can be punished with imprisonment of up to 3 years or fine of up to INR 500000 or both.	
15.	CSPs that knowingly or intentionally conceal, destroy or alter computer source codes that are required to be maintained by law can be punished with imprisonment of up to 3 years or fine of up to INR 200000 or both.	Section 65, the IT Act.
16.	Dishonestly receiving or retaining any stolen computer resource or communication device knowing or having reason to believe the same to be a stolen computer resource or communication device is punishable with imprisonment of up to 3 years or fine of up to INR 100000 or both. Thus, if any CSPs are involved with the above-mentioned activities, they can be liable under this provision.	Section 66B, the IT Act.
17.	Identity theft by way of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any person is punishable with imprisonment of up to 3 years or fine of up to INR 100000 or both. Thus, if any CSPs are involved with such identity theft, they can be liable under this provision.	Section 66C, the IT Act.
18.	Cheating by personation by means of any communication device or computer resource is punishable with imprisonment of up to 3 years or fine of up to INR 100000 or both. Thus, if any CSPs are involved with such cheating, they can be liable under this provision.	Section 66D, the IT Act.
19.	Capturing, publishing or transmitting the image of a private area of any person without their consent, and violating the privacy of such person is punishable with imprisonment of up to 3 years or fine of up to INR 200000 or both. Thus, if any CSPs are involved with the above-mentioned activities, they can be liable under this provision.	Section 66E, the IT Act.
20.	Engaging in cyber-terrorism[29] is punishable with imprisonment which may extend to imprisonment for life. Thus, if any CSPs engage in cyber-terrorism as defined under this provision, they can be liable under this provision.	Section 66F, the IT Act.
21.	Publishing or transmitting obscene material in electronic form is punishable with imprisonment and a fine.[30] Thus, if any CSPs are involved with such publication or transmission, they can be liable under this provision.	Section 67, the IT Act.
22.	Whoever publishes or transmits any material containing any sexually explicit act or conduct in the electronic form is punishable with imprisonment and a	Section 67A, the IT Act.

[29] *Per* Section 66F, cyber terrorism refers to the following:
(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-
(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
(iii) introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or
(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

[30] Upon the first conviction, the punishment shall be imprisonment of up to 3 years and a fine of up to INR 500000 and in the event of second or subsequent conviction with imprisonment the punishment shall be imprisonment of up to 5 years and a fine of up to INR 1000000.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	fine.[31] Thus, if any CSPs are involved with such publication or transmission, they can be liable under this provision.	
23.	Whoever publishes or transmits any material depicting children engaged in any sexually explicit act or conduct in the electronic form is punishable with imprisonment and a fine.[32] Thus, if any CSPs are involved with such publication or transmission, they can be liable under this provision.	Section 67B, the IT Act.
24.	An intermediary is required to preserve such information as may be specified for such duration and in such manner as may be prescribed by the central government. Contravention of this provision will attract imprisonment of up to 3 years as well as a fine. Thus, CSPs that do not abide by the requirements of the central government's directions specified under this provision, can be punished with imprisonment and a fine.	Section 67C, the IT Act.
25.	CSPs can be directed to co-operate with authorised government agencies to facilitate electronic surveillance[33], if it is necessary for certain reasons,[34] as per the procedure prescribed under Section 69 read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.	Section 69, the IT Act.
26.	CSPs can be directed to block public access to any information generated, transmitted, received, stored or hosted in any computer resource by the central government, if it is necessary for certain reasons. [35]	Section 69A, the IT Act.
27.	CSPs can be directed to co-operate with authorised government agencies to enable online access to traffic data for enhancing cyber security.[36] [*Refer to Table 5 for compliance requirements for CSPs under the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009*]	Section 69B, the IT Act.
28.	CSPs that fail to provide information called for by the computer emergency response team[37] ("**CERT**") or to comply with the directions of the CERT, will be punishable with imprisonment of up to 1 year or fine of up to INR 100000 or both.	Section 70B, the IT Act.
29.	Any person in possession of any material containing personal information about any person disclosing the same to another person without the consent	Section 72A, the IT Act.

[31] Upon the first conviction, the punishment shall be imprisonment of up to 5 years and a fine of up to INR 1000000 and in the event of second or subsequent conviction with imprisonment the punishment shall be imprisonment of up to 7 years and a fine of up to INR 1000000.

[32] Upon the first conviction, the punishment shall be imprisonment of up to 5 years and a fine of up to INR 1000000 and in the event of second or subsequent conviction with imprisonment the punishment shall be imprisonment of up to 7 years and a fine of up to INR 1000000.

[33] Section 69(1) of the IT Act allows authorised government agencies to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

[34] As provided under Section 69(1) of the IT Act, these reasons are: in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement of or for investigation of offence.

[35] As provided under Section 69A(1) of the IT Act, these reasons are: in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence.

[36] Section 69B, IT Act.

[37] *Per* Section 70(b)(4), the "computer emergency response team" serves as the national agency for performing the following functions in the area of cyber security: (a) collection, analysis and dissemination of information on cyber incidents; (b) forecast and alerts of cyber security incidents; (c) emergency measures for handling cyber security incidents; (d) coordination of cyber incidents response activities; (e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and (f) such other functions relating to cyber security as may be prescribed.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	of the person concerned or in breach of a lawful contract with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain will be punishable with imprisonment of up to 3 years or fine of up to INR 500000 or both. Thus, if any CSPs are involved with the above-mentioned activities, they can be liable under this provision.	
30.	As intermediaries under the IT Act,[38] CSPs are subject to a wide range of due diligence requirements under Section 79 of the IT Act[39] and the Information Technology (Intermediaries Guidelines) Rules, 2011 ("**Intermediaries Guidelines Rules**"). Failure to comply with these due diligence requirements will result in CSPs losing the protection of the intermediary safe harbour under this provision. The due diligence requirements for CSPs under the Intermediaries Rules include the obligation to appoint grievance officers [40], remove objectionable or otherwise illegal content in a time-bound manner[41] and report cyber security incidents[42]. Significantly, the Ministry of Electronics and Information Technology ("**MeitY**") has recently released a set of proposed amendments to the Intermediaries Guidelines Rules ("**Draft Rules**").[43] These proposed amendments will impose additional obligations on all intermediaries, including CSPs.	Section 79, the IT Act read with the Intermediaries Guidelines Rules.
31.	CSPs are subject to the modes or methods for encryption that are prescribed by the central government under Section 84A of the IT Act.	Section 84A, the IT Act.
32.	Abetting any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by the IT Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act. Thus, if CSPs acts as abettors to any offence under the IT Act, they can be liable under this provision.	Section 84B, the IT Act.
33.	Attempting to commit an offence punishable by the IT Act or causing such an offence to be committed, and in such an attempt doing any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both. Thus, if CSPs attempt to commit an offence under the IT Act, or cause such an offence to be committed, they can be liable under this provision.	Section 84C, the IT Act.

[38] Section 2(1)(w) of the IT Act defines an intermediary as "*any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites online auction sites, online- market places, and cyber cafes.*"

[39] Section 79, IT Act.

[40] Rule 3(11), Intermediaries Guidelines Rules.

[41] Rule 3(2), Intermediaries Guidelines Rules.

[42] Rule 3(9), Intermediaries Guidelines Rules.

[43] Comments/suggestions invited on draft of the Information Technology [Intermediary Guidelines (Amendment) Rules], 2018, Ministry of Electronics and Information Technology, *available at* http://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9C-information-technology-intermediary-guidelines (Last accessed on 12 January 2019).

NO.	PROVISIONS GOVERNING CSPS	PROVISION
34.	Where any company is in contravention of any of the provisions of the IT Act or the rules framed under it, every person who, at the time, was in charge of and responsible to the company for the conduct of business as well as the company, shall be guilty of the contravention unless such person proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention. Thus, persons in charge of and responsible for cloud computing companies can be held liable for any contraventions by the cloud computing companies involved, in certain cases.	Section 85, the IT Act.

TABLE 2: REGULATION OF CSPS UNDER THE SPDI RULES.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	CSPs are required to have a privacy policy in place for handling or dealing in personal information, including sensitive personal data or information.[44] This policy must be published on the website of the CSP and must provide for - (i) clear and easily accessible statements of privacy practices and policies; (ii) types of personal or sensitive personal data or information collected by the CSP; (iii) purpose of collection and usage of such information; (iv) the manner disclosure of information including sensitive personal data or information; and (v) reasonable security practices and procedures.	Rule 4, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
2.	CSPs must obtain consent from providers of sensitive personal data or information before they collect such information.	Rule 5(1), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
3.	While collecting sensitive personal information directly from the person concerned, CSPs must ensure that the person concerned has the knowledge of -- (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of -- (i) the agency that is collecting the	Rule 5(3), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[44] *Per* Rule 3 of the SPDI Rules, sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	information; and (ii) the agency that will retain the information.	
4.	CSPs cannot collect sensitive personal data or information unless -- (a) the information is collected for a lawful purpose connected with a function or activity of the CSP; and (b) the collection of the sensitive personal data or information is considered necessary for that purpose.	Rule 5(2), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
5.	CSPs cannot to retain sensitive personal data or information that is held by them for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law.	Rule 5(4), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
6.	The sensitive personal information collected by CSPs must be used for the purpose for which it has been collected.	Rule 5(5), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
7.	Prior to the collection of information including sensitive personal data or information, CSPs are required to provide an option to the provider of the information to not provide the data or information sought to be collected.	Rule 5(7), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
8.	CSPs are required to keep all information that is collected by them secure.	Rule 5(8), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
9.	CSPs are required to address any user grievances regarding the processing of information in a time bound manner. For this purpose, CSPs must designate a grievance officer and publish his name and contact details on its website. The grievance officer must redress the user grievances within 1 month from the date of receipt of the grievance.	Rule 5(9), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
10.	Disclosure of sensitive personal data or information by CSPs to any third party requires prior permission from the provider of such information, unless such disclosure has been agreed to in the contract between the CSP and provider of information, or where the disclosure is necessary for compliance with a legal obligation.	Rule 6(1), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
11.	CSPs cannot publish sensitive personal data or information.	Rule 6(3), the Information Technology (Reasonable security practices and procedures and

NO.	PROVISIONS GOVERNING CSPS	PROVISION
		sensitive personal data or information) Rules, 2011.
12.	The third party that receives sensitive personal data or information from a CSP cannot disclose it further.	Rule 6(4), the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
13.	CSPs may transfer sensitive personal data or information, including any information, to any other body corporate or person in India or abroad, so long as the body corporate ensures the same level of data protection that is adhered to by the CSPs under these Rules. The transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the provider of information or where the provider of information has consented to a data transfer.	Rule 7, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
14.	CSPs must implement security practices and standards that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected. In the event of an information security breach, the CSP involved with the breach will be required to demonstrate that it had implemented security control measures as per its documented information security programme and information security policies such as IS/ ISO /IEC / 27001 for the protection of sensitive personal information.	Rule 8, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

TABLE 3: REGULATION OF CSPS UNDER THE INTERMEDIARIES GUIDELINES RULES.

No.	Provisions governing CSPs	Provision
1.	As intermediaries under the IT Act,[45] CSPs are subject to a wide range of due diligence requirements under the Intermediaries Guidelines Rules. These requirements include the duty to publish rules and regulations, privacy policies and user agreements for access to/usage of the CSPs computer resources by any person. These rules and regulations/terms and conditions/user agreements must inform CSPs' users not to host, display, upload, modify, publish,	Rules 3(1) and 3(2), the Intermediaries Guidelines Rules.

[45] Section 2(1)(w) of the IT Act defines an intermediary as "*any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites online auction sites, online- market places, and cyber cafes.*"

No.	Provisions governing CSPs	Provision
	transmit, update or share any information ("**Illegal information**") that— (a) belongs to another person and to which the user does not have any right to; (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; (c) harms minors in any way; (d) infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force; e) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature; f) impersonates another person; (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource; or (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents the investigation of any offence or is insulting to any other nation.	
2.	CSPs cannot knowingly host or publish any of the above-mentioned Illegal information. They also cannot initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission of Illegal information.	Rule 3(3), the Intermediaries Guidelines Rules.
3.	Upon receiving a lawful order to do, CSPs must act within 36 hours and where applicable, work with the user or owner of such information to disable such illegal information being hosted or published on their platform. Further the CSP must preserve such information and associated records for at least 90 days for investigation purposes.	Rule 3(4), the Intermediaries Guidelines Rules.
4.	CSPs must inform their users that that they can immediately terminate user access or usage rights and remove non-compliant information in case of non-compliance with their rules and regulations, user agreements and privacy policies.	Rule 3(5), the Intermediaries Guidelines Rules.
5.	CSPs must co-operate with authorised government agencies to assist them with investigative, protective or cyber-security activities. Such assistance shall be provided for the purpose of verification of identity, or for the prevention, detection, investigation or prosecution of cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.	Rule 3(7), the Intermediaries Guidelines Rules.

No.	Provisions governing CSPs	Provision
6.	CSPs must take all reasonable measures to secure their computer resources and information contained therein by following the reasonable security practices and procedures as prescribed in the SPDI Rules.	Rule 3(8), the Intermediaries Guidelines Rules.
7.	CSPs must report cyber-security incidents and also share cyber-security incidents related information with the Indian Computer Emergency Response Team.	Rule 3(9), the Intermediaries Guidelines Rules.
8.	CSPs cannot knowingly deploy/install/modify the technical configuration of a computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform. However, CSPs can develop, produce, distribute or employ technological means for the purpose of securing their computer resource and the information contained therein.	Rule 3(10), the Intermediaries Guidelines Rules.
9.	CSPs must publish the name of their appointed grievance officers and their contact details on their website. Additionally, they must publish the grievance redressal mechanism for users or any victim who suffers as a result of a violation of Rule 3 of the Intermediaries Guidelines Rules. This mechanism must allow complainants to notify their complaints. Grievance officers must redress the complaints within one month from the date of receipt of the complaint.	Rule 3(11), the Intermediaries Guidelines Rules.

TABLE 4: REGULATION OF CSPS UNDER THE INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR INTERCEPTION, MONITORING AND DECRYPTION OF INFORMATION) RULES, 2009 ["ELECTRONIC SURVEILLANCE RULES"]

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	No CSP can carry out electronic surveillance as prescribed under Section 69 of the IT Act, except by an order issued by the competent authority. A competent authority for the purpose of the Electronic Surveillance Rules is either the Secretary, Ministry of Home Affairs (central government or the Secretary, Home Department (state government), as the case may be. In certain unavoidable circumstances and in emergency situations, such orders may be issued by officers (not below the rank of Joint Secretary) or senior security and law enforcement officers.[46]	Rule 3, the Electronic Surveillance Rules.

[46] *Per* Rule 3, "in an unavoidable circumstance, such order may be issued by an officer, not below the rank of Joint Secretary of the Government of India, who has been duly authorised by the competent authority; Provided further that in a case of emergency-
(i) in remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or
(ii) for operational reasons, where obtaining of prior directions for interception or monitoring or decryption of any information generation, transmitted, received or stored in any computer resource is not feasible,
the interception or monitoring of decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency (hereinafter referred

NO.	PROVISIONS GOVERNING CSPS	PROVISION
2.	The competent authorities are empowered to issue a decryption direction [47] to the decryption key holder [48] for decryption of any information involving a computer resource or a part thereof. Thus, CSPs can be directed to decrypt information as per this rule.	Rule 5, the Electronic Surveillance Rules.
3.	The designated officers of CSPs are required to provide all facilities, co-operation and assistance for interception/monitoring/decryption mentioned in the directions issued under Rule 3 of the Electronic Surveillance Rules (*refer to point 2 above*). Such directions must be limited to the extent the information is encrypted by the CSP or the CSP has control over the decryption key.	Rule 13, the Electronic Surveillance Rules.
4.	Every CSP is required to designate an officer to receive and handle requisitions for assistance from the nodal officer [49] for interception/monitoring/decryption of information generated, transmitted, received or stored in any computer resource.	Rule 14, the Electronic Surveillance Rules.
5.	The designated officer of the CSP is required to acknowledge the instructions for electronic surveillance within two hours on receipt of such intimation or direction for interception/monitoring/decryption of information.	Rule 15, the Electronic Surveillance Rules.
6.	The designated officer of the CSP must maintain proper records mentioning the particulars of the information so intercepted or monitored or decrypted including; (i) particulars of persons, computer resource, e-mail account, website address, etc. whose information has been intercepted/ monitored/ decrypted; (ii) the name and other particulars of the officer or the authority to whom the intercepted/ monitored/ decrypted information has been disclosed; (iii) the number of copies made of the intercepted/ monitored/ decrypted information (including corresponding electronic records); (iv) the mode or the	Rule 16, the Electronic Surveillance Rules.

to as the said security agency) at the Central level and the officer authorised in this behalf, not below the rank of the inspector General of Police or an officer of equivalent rank, at the State or Union territory level;
Provided also that the officer, who approved such interception or monitoring or decryption of information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception or monitoring or decryption within three working days and obtain the approval of the competent authority thereon within a period of seven working days and if the approval of competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the competent authority."

[47] *Per* Rules 2(h) and 2(g), the "decryption direction" means a direction issued under rule 3 in which a decryption key holder is directed to- (i) disclose a decryption key; or (ii) provide decryption assistance in respect of encrypted information. "Decryption assistance" means any assistance to -(i) allow access, to the extent possible, to encrypted information; or (ii) facilitate conversion of encrypted information into an intelligible form.

[48] *Per* Rules 2(j) and 2(i), "decryption key holder" means any person who deploys the decryption mechanism and who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications and "decryption key" means any key, mathematical formula, code, password, algorithm or any other data which is used to - (i) allow access to encrypted information; or (ii) facilitate the conversion of encrypted information into an intelligible form.

[49] *Per* Rule 12, the agency authorised by the competent authority under rule 4 shall designate one or more nodal officer(s), not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank, to authenticate and send the requisition conveying direction issued under rule 3 for interception or monitoring or decryption to the designated officers of the concerned intermediaries or person in-charge of computer resource:
Provided that an officer, not below the rank of Inspector of Police or officer of equivalent rank, shall deliver the requisition to the designated officer of the intermediary.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	method by which such copies are made; (v) the date of destruction of the copies (including corresponding electronic record) and (vi) the duration up to which the directions remain in force. This obligation would be applicable to CSPs.	
7.	If a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the nodal officer, the decryption key holder shall within the period mentioned in the decryption direction - (a) disclose the decryption key; or (b) provide the decryption assistance, specified in the decryption direction to the concerned authorised person. This obligation would be applicable to cloud service providers.	Rule 17, the Electronic Surveillance Rules.
8.	Every fifteen days, the designated officers of the CSP shall forward a list of interception/ monitoring /decryption authorisations received by them during the preceding fortnight to the nodal officers for confirmation of the authenticity of such authorisations. Such list shall include details, such as the reference and date of orders, date and time of receipt of such order and the date and time of implementation of such order.	Rule 18, the Electronic Surveillance Rules.
9.	The CSP so directed, is required to provide technical assistance and the equipment including hardware, software, firmware, storage, interface and access to the equipment wherever requested by the agency authorised for performing interception or monitoring or decryption.	Rule 19, the Electronic Surveillance Rules.
10.	The CSP is required to put in place adequate and effective internal checks to ensure the unauthorised interception of information does not take place, extreme secrecy is maintained and utmost care and precaution is taken in the matter of interception or monitoring or decryption of information as it affects privacy of citizens and also that it is handled only by the designated officers of the intermediary and no other person of the intermediary or person in-charge of computer resources shall have access to such intercepted or monitored or decrypted information.	Rule 20, the Electronic Surveillance Rules.
11.	The CSP shall be responsible for any action of their employees also and in case of violation pertaining to maintenance of secrecy and confidentiality of information or any unauthorised interception or monitoring or decryption of information, the intermediary or person in-charge of computer resources shall be liable for any action under the relevant laws.	Rule 21, the Electronic Surveillance Rules.
12.	The CSP shall destroy records pertaining to directions for interception of information within a period of two months of discontinuance of the interception or monitoring or decryption of such information unless otherwise required for the purpose of any ongoing investigation, criminal complaint or legal proceedings. In doing so, they shall maintain extreme secrecy.	Rule 23, the Electronic Surveillance Rules.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
13.	Any person who intentionally or knowingly, without authorisation under rule 3 or rule 4, intercepts or attempts to intercept, or authorises or assists any other person to intercept or attempts to intercept any information in the course of its occurrence or transmission at any place within India, shall be proceeded against and punished accordingly under the relevant laws. However, any such interception, monitoring or decryption of information in computer resource by the employee of or a person duly authorised by the intermediary may be exempted if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices. This obligation would be applicable to the CSPs.	Rule 24, the Electronic Surveillance Rules.
14.	The contents of intercepted or monitored or stored or decrypted information shall not be used or disclosed by intermediary or any of its employees or person in-charge of computer resource to any person other than the intended recipient of the said information. Any CSP who contravenes provisions of these rules shall be proceeded against and punished.	Rule 25, the Electronic Surveillance Rules.

TABLE 5: REGULATION OF CSPS UNDER THE TRAFFIC DATA RULES

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	CSPs can be directed to monitor and collect traffic data by the order of a competent authority[50], as prescribed under Section 69B of the IT Act.	Rule 3, the Traffic Data Rules.
2.	CSPs must designate one or more officers, who are required to receive and handle requisitions from the nodal officers of the competent authority [51] ("**Monitoring requisitions**") for monitoring/collecting traffic data.	Rule 4(3), the Traffic Data Rules.
3.	CSPs must comply with requests to extend all facilities, co-operation and assistance in installation, removal and testing of equipment and also enable online access or to secure and provide online access to the computer resource for monitoring and collecting traffic data or information.	Rule 4(7), the Traffic Data Rules
4.	CSPs must acknowledge the receipt of Monitoring requisitions within a period of 2 hours from the time of receipt.	Rule 4(8), the Traffic Data Rules.
5.	The designated officers of CSPs are required to maintain proper records of the Monitoring requisitions received by them.	Rule 4(9), the Traffic Data Rules.

[50] *Per* Rule 2(d), "competent authority" means the Secretary to the Government of India in the Department of Information Technology under the Ministry of Communications and Information Technology.

[51] *Per* Rule 4(2), the agency authorised by the competent authority under sub-rule (1) shall designate one or more nodal officer, not below the rank of the Deputy Secretary to the Government of India, for the purpose of authenticating and sending the requisition conveying the direction issued under rule 3 to the designated officers of the concerned intermediary or person in-charge of computer resources.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
6.	Designated officers of CSPs must forward a list of Monitoring requisitions to the relevant nodal officer every 15 days. These lists must include details such as the reference and date of the Monitoring requisitions.	Rule 4(10), the Traffic Data Rules.
7.	CSPs must implement adequate and effective internal checks to prevent unauthorised monitoring or collection of traffic data. They must also ensure that extreme secrecy is maintained in the process of monitoring/collecting traffic data. Such matters must only be handled by the designated officer of the CSP.	Rule 5, the Traffic Data Rules.
8.	CSPs can be held liable for the actions of their employees, if such actions lead to: (i) a violation of secrecy and confidentiality of information in contravention of the IT Act; or (ii) for any unauthorised monitoring or collection of traffic data.	Rule 6, the Traffic Data Rules.
9.	CSPs are required to destroy records pertaining to any directions for monitoring/collecting information under these rules. Such records must be destroyed within a period of 6 months of discontinuance of the monitoring/ collection activities, unless they are required for the purpose of any ongoing investigation, criminal complaint or legal proceedings. In case of the latter case, CSPs must maintain extreme secrecy in storing such records.	Rule 8, the Traffic Data Rules.
10.	Any CSP who intentionally or knowingly, monitors/collects traffic data, or attempts to monitor/collect traffic data, or assists any person in monitoring/collecting traffic data *without authorisation,* as is required under these rules, can be proceeded against and punished accordingly under the relevant laws. However, monitoring/collection of traffic data in a computer resource by the employee of the CSP may be exempted if such activities are reasonably necessary for the discharge of such employee's duties as per the prevailing industry practices.	Rule 9, the Traffic Data Rules.
11.	CSPs must maintain strict confidentiality with respect to directions for monitoring or collection of traffic data or information issued by the competent authority under these rules.	Rule 11, the Traffic Data Rules

TABLE 6: REGULATION OF CSPS UNDER THE BLOCKING RULES

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	CSPs can be directed to block public access to any information or part thereof that is generated, transmitted, received, stored or hosted in any computer resource for any of the reasons specified in sub-section (1) of Section 69A of the IT Act. Such directions can be issued by designated officers.[52]	Rule 5 read with Rule 8(1), the Blocking Rules.

[52] *Per* Rule 3, The Central Government shall designate by notification in Official Gazette, an officer of the Central Government not below the rank of a Joint Secretary, as the "Designated Officer", for the purpose of issuing direction for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource under sub-section (2) of section 69A of the Act.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
2.	In case of an emergency, CSPs can be directed to block public access to information by the Secretary, Department of Information Technology without being given the opportunity of a hearing, if the Secretary is satisfied that such action is necessary or expedient and justifiable. The reasons for doing so must be recorded in writing.	Rule 9(2), the Blocking Rules.
3.	In case the CSP fails to comply with the direction issued to it under Rule 9 of the Blocking Rule, the Designated Officer[53] is empowered to initiate appropriate action as may be required to comply with sub-section (3) of section 69A of the IT Act with the prior approval of the Secretary, Department of Information Technology.	Rule 12, the Blocking Rules.
4.	Every CSP is required to designate at least one person to receive and handle the directions for blocking of public access to information under these rules.	Rule 13(1), the Blocking Rules.
5.	CSPs must maintain strict confidentiality regarding all the requests and complaints received under these rules, and actions taken thereof.	Rule 16, the Blocking Rules.

TABLE 7: REGULATION OF CSPS UNDER THE CERT RULES

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	CSPs are required to report cyber security incidents to the Indian Computer Emergency Response Team [54] ("**CERT**") within a reasonable timeframe to allow for timely action.	Rule 12(1)(a) read with Rule 13(2), the CERT Rules.
2.	CERT is empowered collect and analyse information relating to cyber security incidents from CSPs, for the discharge of its functions. CERT must follow applicable legal restrictions, orders of competent Indian courts and ethical practices with regard to the disclosure of the information it collects in this manner.	Rule 13(1) read with Rule 13(2), the CERT Rules
3.	Any officer of CERT, not below the rank of Deputy Secretary of the Government of India, can seek information from CSPs and give them directions, for the purpose of carrying out its functions under Section 70B of the IT Act.[55]	Rule 14(1), the CERT Rules.

[53] *Per* Rule 3, The Central Government shall designate by notification in Official Gazette, an officer of the Central Government not below the rank of a Joint Secretary, as the "Designated Officer", for the purpose of issuing direction for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource under sub-section (2) of section 69A of the Act.
[54] *Per* Rule 2(k), the Indian Computer Emergency Response Team shall be an agency of the Government appointed by the Central Government.
[55] *Per* Section 70B of the IT Act, "The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,-
(a) collection, analysis and dissemination of information on cyber incidents;
(b) forecast and alerts of cyber security incidents;
(c) emergency measures for handling cyber security incidents;
(d) coordination of cyber incidents response activities;
(e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, preventation, response and reporting of cyber incidents; and
(f) such other functions relating to cyber security as may be prescribed.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
4.	CERT is empowered to take recourse to monitoring and collection of traffic data in accordance with Section 69B of the IT Act and the Traffic Data Rules for the purpose of cyber-security. Thus, CSPs must co-operate with CERT in this regard.	Rule 14(2), the CERT Rules.
5.	CERT is empowered to issue directions/advisories to CSPs. The CSPs are required to comply with these directions/advisories and also report to CERT in the manner and within the time period specified by CERT.	Rule 15, the CERT Rules.
6.	CSPs must designate a Point of Contact ("**PoC**") to interface with CERT. The information relating to the PoC must be sent to CERT in the prescribed format and must be updated from time to time. Such PoCs will be responsible for receiving all communications from CERT.	Rule 17, the CERT Rules.
7.	In case CSPs do not comply with directions issued under Rule 15, an officer designated by CERT must submit a non-compliance report to the Director General. Further, all cases of non-compliance with directions under Rule 15 and requests for information under Rule 14(1) of the CERT Rules must be submitted to a review committee[56]. This review committee is empowered to issue directions on the cases of non-compliance submitted to it. On the basis of these directions and the non-compliance report submitted to the him, the Director General of CERT is empowered to file a complaint before a court, as provided under Section 70B(8) of the IT Act.[57]	Rule 19 read with Rule 20, the CERT Rules.

TABLE 8: REGULATION OF CSPS UNDER THE NCIIPC RULES

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	In the event of any threat to critical information infrastructure,[58] the National Critical Information Infrastructure Protection Centre[59] ("**NCIIPC**") is empowered to call for information and issue directions to critical sectors and persons serving/ having critical impact on critical information infrastructure. Thus, CSPs notified as that serving/having a critical impact on critical information infrastructure ("**Critical CSPs**") must comply with the NCIIPC's	Rule 4(13), the NCIIPC Rules.

[56] This review committee shall consist of the Secretary, Department of Electronics and Information Technology; Joint Secretary, Ministry of Law and Justice; Joint Secretary level officer, Department of Telecommunications; Joint Secretary, Ministry of Home Affairs and the Group Co-ordinator (Cyber law and e-security), Department of Electronics and Information Technology.

[57] *Per* Section 70B(8) of the IT Act, no court can take cognizance of any offence under Section 70B of the IT Act, except on a complaint made by an officer authorised in this behalf by CERT."

[58] *Per* Explanation to section 70 (1) of the Act, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

[59] *Per* Rule 3(1), the NCIIPC shall be the national nodal agency under the administrative control of National Technical Research Organisation ("**NTRO**") and designated under section 70A of the Act in respect of critical information infrastructure protection.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	directions issued under this provision. In addition, any CSPs notified to form a part of critical information infrastructure will be required to comply with the Protected System Rules.	
2.	The NCIIPC is empowered to issue guidelines, advisories and vulnerability/ audit notes relating to practices, procedures, prevention and response for the protection of critical information infrastructure in coordination with the CERT and other concerned organisations.	Rule 4(11), the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.
3.	The NCIIPC is empowered to exchange information relating to cyber incidents/ attacks and vulnerabilities with the CERT-In and other concerned organisations.	Rule 4(12), the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.
4.	The NCIIPC is empowered to issue advisories or alerts and provide guidance and expertise-sharing in addressing threats or vulnerabilities for protection of critical information infrastructure. Such advisories/alerts/guidance/expertise-sharing can serve as guidance for Critical CSPs.	Rule 5(3)(a), the NCIIPC Rules.
5.	The NCIIPC is empowered to take recourse to the monitoring and collection of traffic data in accordance with the Section 69B of the IT Act and the Traffic Data Rules for the protection of critical information infrastructure. Thus, the NCIIPC can direct CSPs to monitor and collect traffic data in accordance with this provision.	Rule 5(3)(c), the NCIIPC Rules.
6.	The NCIIPC is empowered to take recourse to electronic surveillance and blocking of cyber information for the purpose of protection of critical information infrastructure. Thus, the NCIIPC can direct CSPs to undertake electronic surveillance and block public access to information in accordance with this provision.	Rule 5(3)(d), the NCIIPC Rules.

TABLE 9: REGULATION OF CSPS UNDER THE ELECTRONIC SERVICE DELIVERY RULES

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	CSPs that are:	Rule 3(1), the Information Technology (Electronic Service Delivery) Rules, 2011.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	(i) engaged as authorised agents[60] of the government (the central government/state governments/union territory administrations)[61]; (ii) for the delivery of public services; (iii) through any electronic services delivery[62] mechanism, are subject to these rules.	
2.	The government and its agencies have the power to specify: (i) the form and the manner of electronic service delivery; and (ii) the norms on service levels that must be complied with by CSPs that are engaged as authorised agents under these rules.	Rule 3(2) & 3(8), the Information Technology (Electronic Service Delivery) Rules, 2011.
3.	The government is empowered to determine the manner of encrypting sensitive electronic records that require confidentiality while they are electronically signed. CSPs that are engaged as authorised agents under these rules may be required to ensure compliance with the government's directions in this regard.	Rule 3(3), the Information Technology (Electronic Service Delivery) Rules, 2011.
4.	The government is empowered to authorise CSPs to collect, retain and appropriate specified service charges from persons availing specified services. This includes the power to specify, by notification, the scale of service charges which may be charged and collected by CSPs for various kinds of services.	Rule 3(6) & 3(7), the Information Technology (Electronic Service Delivery) Rules, 2011.
5.	The government is empowered to specify the security procedures in respect of the electronic data, information, applications, repository of digitally signed electronic records and information technology assets under their respective control. CSPs that are engaged as authorised agents of the government may be required to comply with these security procedures.	Rule 5(4), the Information Technology (Electronic Service Delivery) Rules, 2011.
6.	The government is empowered to direct CSPs engaged as authorised agents to keep an updated and accurate account of the transactions, receipts and vouchers relating to the delivery of electronic services. The government may also specify the formats for maintaining the accounts of transactions and receipt of payment in respect of electronic services delivered. The above-mentioned CSPs must produce these records for inspection and audit by agencies/persons nominated by the government.	Rule 7, the Information Technology (Electronic Service Delivery) Rules, 2011.
7.	The government is empowered to initiate an audit of the affairs of CSPs engaged as authorised agents. Such audits may be conducted at such intervals as deemed necessary.	Rule 8(1), the Information Technology (Electronic

[60] *Per* Rules 2(c) and (m), an "authorised agent" means an agent of the appropriate Government or service provider and includes an operator of an electronically enabled kiosk who is permitted under these rules to deliver public services to the users with the help of a computer resource or any communication device, by following the procedure specified in the rules. A "service provider" includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

[61] *Per* Rules 2(b), the "appropriate Government" means the Central Government or the State Government or a Union Territory Administration.

[62] *Per* Rules 2(i), "Electronic Service Delivery" means the delivery of public services in the form of filing receipt of forms and applications, issue or grant of any license, permit, certificate, sanction or approval and the receipt or payment of money by electronic means by following the procedure specified under rule 3.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
		Service Delivery) Rules, 2011.
8.	CSPs engaged as authorised agents are required to provide information and assistance to the audit agencies nominated by the government. They must comply with the directions given by the audit agencies and rectify the defects and deficiencies pointed out by the audit agencies within the time limit specified.	Rule 8(3), the Information Technology (Electronic Service Delivery) Rules, 2011.
9.	All CSPs that are engaged as authorised agents are required to submit a due declaration for protecting the data of every individual transaction and citizen. Any unauthorised disclosure to anyone without the written consent of either the individual or the government will debar the CSP involved from providing services any further. The CSP involved would also be liable to pay a penalty of INR 25000.	Rule 8(4), the Information Technology (Electronic Service Delivery) Rules, 2011.

TABLE 10: REGULATION OF CSPS UNDER THE DIGI-LOCKER RULES

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	Certain CSPs can be authorised to serve as Digital Locker Service Providers ("**DLSPs**") by the Digital Locker Authority[63] ("**DLA**"). DLSPs are required to provide a Digital Locker[64] ("**Digi-Locker**"), access gateway[65] and/or a repository facility[66] electronically, in accordance with these rules.	Rule 3(3), the Digi-Locker Rules.
2.	The central government and the DLA are empowered to authorise CSPs that are authorised DLSPs to set up Digi-Locker portals, access gateways or repositories for efficient use of the Digi-Locker system.	Rule 10(2), the Digi-Locker Rules.
3.	All CSPs that are authorised DLSPs must conform and comply with the binding authorising terms, including the standards, guidelines and specifications as laid down by the central government and the DLA.	Rule 10(3), the Digi-Locker Rules.

[63] *Per* Rule 3(1), the DLA is responsible for establishing, administering, and managing the government's Digital Locker system ("**Digi-Locker**"). As per MeitY, Digi-Locker is a key initiative under Digital India, the Indian Government's flagship program that aims at transforming India into a digitally empowered society and knowledge economy. Targeted at the idea of paperless governance, DigiLocker is a platform for issuance and verification of documents & certificates in a digital way, thus eliminating the use of physical documents. Indian citizens who sign up for a DigiLocker account get a dedicated cloud storage space that is linked to their Aadhaar (UIDAI) number. Organizations that are registered with DigiLocker can push electronic copies of documents and certificates (e.g. driving license, Voter ID, School certificates) directly into citizen's lockers. Citizens can also upload scanned copies of their legacy documents in their accounts. *See* MeitY, Digital Locker, *available at* http://meity.gov.in/digital-locker (Last accessed on 25 January, 2019).
Per Rule 2(h), "Digital Locker authority" means an authority as designated by the government for the licensing, empanelment and management of DLSPs.

[64] *Per* Rule 2(f) and 2(g), "Digital Locker" means the Government owned and operated web and mobile based hosting of Digi-Locker system. It could also mean a service of preservation, retention of electronic records by the subscriber and delivery of electronic records to the subscriber.

[65] *Per* Rule 2(b), access gateway means an authorised system to provide access to repositories under the Digi-Locker system.

[66] *Per* Rule 2(r), "repository" means an electronic repository of digitally signed and/or digitised electronic records, maintained by any DLSP or an issuer for the purpose of accessing such records and delivering them to the users.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
4.	Every CSP that is an authorised DLSP is required to ensure that every person employed or otherwise engaged or associated with it complies, in the course of such employment or engagement, with the provisions of the IT Act and the rules, regulations and orders made thereunder.	Rule 11, the Digi-Locker Rules.
5.	Every CSP that is an authorised DLSP is required to publish on its website, the name of the grievance officer and his contact details as well as mechanism by which any users/aggrieved persons may notify their complaints. The grievance officer is required to redress the complaints within one month from the date of receipt of complaint.	Rule 12(1), the Digi-Locker Rules.
6.	CSPs that are authorised DLSPs must charge such fee or service charges from subscribers or users, as may be notified by the central government or DLA. A DLSP is also required to provide an up-to-date fee schedule or scale of service charges to all its subscribers and users.	Rule 15, the Digi-Locker Rules.
7.	CSPs that are authorised DLSPs must get their operations audited annually by an auditor and conduct a yearly audit of the security policy, physical security and planning of their operation, system and all associated interfaces, systems, tools and processes.	Rule 17, the Digi-Locker Rules.
8.	CSPs that are authorised DLSPs must ensure that their employees have access to confidential information[67] on a "need-to-know" and "need-to-use" basis. The process of maintaining confidentiality of information has to be included in the Digital Locker Practise Statement.[68] The back-up of all information is required to be kept offsite in a disaster recovery facility. Additionally, CSPs that are authorised DLSPs must ensure that no confidential information is preserved and retained outside India.	Rule 20, the Digi-Locker Rules.
9.	CSPs that are authorised DLSPs are required to observe and maintain reasonable security practices as mandated under the SPDI Rules.	Rule 21(1), the Digi-Locker Rules.
10.	CSPs that are authorised DLSPs are required to observe and maintain the Information Technology Security Guidelines as mandated under Schedule II of the Information Technology (Certifying Authorities) Rules, 2000.	Rule 21(2), the Digi-Locker Rules.

TABLE 11: REGULATION OF CSPS UNDER THE CONSUMER PROTECTION ACT, 2019

NO.	PROVISIONS GOVERNING CSPS	PROVISION
1.	The Consumer Protection Act defines an "electronic service provider"[69] to mean a person who provides technologies or	Section 2(17), the Consumer Protection Act.

[67] *Per* Rule 19, The following information shall be treated as confidential, namely:--
(a) Digital Locker account application; (b) Digital Locker account information collected from the subscriber or elsewhere as part of the registration; (c) subscriber agreement; (d) Digital Locker contents; (e) document URI; and (f) any other information as may be notified by the DeitY.
[68] *Per* Rule 2(k), "Digital Locker Practice Statement" means a statement by the Digital Locker service provider describing the services and flow of the services being offered by the provider.
[69] Section 2(17), the Consumer Protection Act.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	processes which enable product sellers to engage in advertising or selling goods/services to consumers. CSPs provide a number of cloud computing services to businesses as well as individual consumers. Some of these services allow product sellers to engage in advertising and selling goods/services. For instance, CSPs allow users to carry out remote hosting of their websites which may be used to sell goods and services, as well as analytics and media related services provided by CSPs can enable business/individual consumers who are product sellers to advertise or sell their good/services.[70] CSPs who provide such services would therefore qualify as electronic service providers for the purposes of the Consumer Protection Act.	
2.	A "service" has been defined to mean a service of any description which is made available to potential users.[71] This would include cloud-based services that are provided by CSPs to their users.	Section 2(42), the Consumer Protection Act.
3.	"E-commerce" has been defined to mean the buying or selling of goods or services, including digital products over digital or electronic networks.[72] Thus, the buying or selling of cloud-based services would qualify as "e-commerce" for the purposes of the Consumer Protection Act.	Section 2(16), the Consumer Protection Act.
4.	A "product service provider" has been defined to mean a person who provides any service in respect of a product.[73] A number of CSPs provide, *inter alia*, cloud-computing services such as cloud storage services, data transfer services and data warehousing services, which can be accessed and utilised through products on the Internet of Things, such as mobile phones and laptops.[74] Thus, to the extent that CSPs provide services in respect of such products, they can be considered product service providers for the purposes of the Consumer Protection Act.	Section 2(38), the Consumer Protection Act.

[70] For instance, Amazon Web Services ("**AWS**") provides digital marketing services on its platform that helps businesses by offering real-time analytics to increase the speed and efficiency of digital marketing. *See,* AWS for Digital Marketing at https://aws.amazon.com/digital-marketing/ (Last accessed on 25 January, 2019). Similarly, Microsoft Azure, Google Cloud, IBM and Tata Communications also offer such services. *See* Microsoft Azure, Digital Marketing Solutions, *available at* https://azure.microsoft.com/en-us/solutions/digital-marketing/; https://cloud.google.com/solutions/media-entertainment/; IBM, Cloud services, *available at* https://www.ibm.com/services/cloud; Tata Communications, Cloud analytics services, *available at* https://www.tatacommunications.com/services/cloud/cloud-platforms/izo-cloud-analytics/ (Last visited on 25 January, 2019).

[71] Section 2(42), the Consumer Protection Act.

[72] Section 2(16), the Consumer Protection Act.

[73] Section 2(38), the Consumer Protection Act.

[74] *See* Microsoft, Internet of Things: Overview, *available at* https://azure.microsoft.com/en-us/overview/iot/ ; Microsoft, Data Warehouse, *available at* https://azure.microsoft.com/en-us/solutions/data-warehouse/; Google Cloud, Internet of Things, *available at* https://cloud.google.com/solutions/iot/ ; Google Cloud, Storage, *available at* https://cloud.google.com/products/storage/; Google Cloud, Data transfer, *available at* https://cloud.google.com/products/data-transfer/ ; Google Cloud, Data transfer products and services, *available at* https://cloud.google.com/products/data-transfer/; AWS, Internet of Things, *available at* https://aws.amazon.com/iot/?nc2=h_m1 (Last visited on 25 January, 2019).

NO.	PROVISIONS GOVERNING CSPS	PROVISION
5.	The Central Consumer Protection Authority ("**Central Authority**")[75] is empowered to conduct inquiries into violations of consumer rights or unfair trade practices, either *suo motu* or on a complaint received or on directions from the central government. District Collectors are also empowered to inquire into and investigate complaints regarding violation of consumer rights, unfair trade practices and false/ misleading advertisements, within their jurisdiction, either upon receiving a complaint or upon a reference made by the Central Authority or the commissioner of a regional office. CSPs may be subject to such inquiries as service providers. Under the Consumer Protection Act, consumer rights include[76]: (i) the right to be protected against services hazardous to life and property, (ii) the right to be informed about the quality, quantity, potency, purity, standard and price of the services, (iii) right to be heard at appropriate forums, (iv) right to seek redressal, (v) right to consumer awareness and (vi) right to access services at competitive prices.	Section 18(2)(a), Section 16 the Consumer Protection Act.
6.	After conducting an inquiry and upon being satisfied of the existence of a *prima facie* case of violation of consumer rights or unfair trade practices or false/ misleading advertisements, the Central Authority is empowered to cause an investigation to be made by the Director General[77] or the District Collector. CSPs may face such investigation as service providers.	Section 19(1), the Consumer Protection Act.
7.	On the basis of such investigation, upon being satisfied that there is sufficient evidence to show the violation of consumer rights or unfair trade practice by a person, the Central Authority is empowered to pass such order as may be necessary[78] after giving the concerned person an opportunity of being heard. Failing to comply with such order of the Central Authority shall be punishable with imprisonment of up to 6 months or with fine which may extend to INR 20 lakhs or with both. Thus, CSPs that are found to violate consumer rights or have unfair trade practices can be directed to comply with the orders	Sections 20 and 88, the Consumer Protection Act.

[75] *Per* section 10 of the Act, the central government shall, by notification, establish the Central Authority to regulate matters relating to violation of rights of consumers, unfair trade practices and false or misleading advertisements which are prejudicial to the interests of public and consumers and to promote, protect and enforce the rights of consumers.
[76] Section 2(9), the Consumer Protection Act.
[77] *Per* section 15(2) of the Act, the Central Government may appoint a Director General who have experience in investigation and possess such qualifications, in such manner, as may be prescribed.
[78] *Per* section 20, such order may include: (a) recalling of goods or withdrawal of services which are dangerous, hazardous or unsafe; (b) reimbursement of the prices of goods or services so recalled to purchasers of such goods or services; and (c) discontinuation of practices which are unfair and prejudicial to consumers' interest.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	of the Central Authority[79], and failure to comply with such order will result in the CSP being punishable with imprisonment of up to 6 months or with fine which may extend to INR 20 lakhs, or with both.	
8.	A service provider who causes a false or misleading advertisement to be made which is prejudicial to the interest of consumers shall be punished with imprisonment for a term which may extend to two years and with fine which may extend to INR 1000000; and for every subsequent offence, be punished with imprisonment for a term which may extend to five years and with fine which may extend to INR 5000000. On the basis of investigation, upon being satisfied that any advertisement is false/misleading/prejudicial to consumer interests or in contravention of consumer rights, the Central Authority is empowered to: (i) issue cease and desist directions or modifications, by order, to the concerned trader/ manufacturer/ endorser/ advertiser/ publisher; (ii) to impose a penalty; [80] (iii) prohibit, by order, the endorser of a false/ misleading advertisement from making endorsement of any product or service for a period of up to one year.[81] Failing to comply with such order of the Central Authority shall be punishable with imprisonment of up to 6 months or with fine which may extend to INR 2000000, or with both. Thus, CSPs that are found to publish false/misleading/otherwise prejudicial advertisements can be directed to comply with the above-mentioned orders of the Central Authority. Failure to comply with such order will result in the CSP being punishable with imprisonment of up to 6 months or with fine which may extend to INR 2000000, or with both, if the Consumer Protection Act is enacted.	Section 21, 88 and 88, the Consumer Protection Act.
9.	The Central Authority is empowered to recommend adoption of international covenants and best international practices on consumer rights to ensure effective enforcement of consumer rights. CSPs may be made subject to such covenants/practices on consumer rights recommended by the Central Authority, if the Consumer Protection Act is enacted.	Section 18(2)(e), the Consumer Protection Act.
10.	The Central Authority is empowered to issue safety notices to alert consumers against dangerous or hazardous or unsafe	Section 18(2)(j), the Consumer Protection Act.

[79] *Per* section 20, such order may include: (a) recalling of goods or withdrawal of services which are dangerous, hazardous or unsafe; (b) reimbursement of the prices of goods or services so recalled to purchasers of such goods or services; and (c) discontinuation of practices which are unfair and prejudicial to consumers' interest.

[80] *Per* section 21(2), such penalty may extend up to INR 1000000 and upon a subsequent contravention, such penalty could extend up to INR 5000000.

[81] *Per* section 21(3), up to 3 years upon a subsequent contravention.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	goods or services. Such safety notices may be issued to alert users of CSPs about hazardous/unsafe cloud computing services.	
11.	The Central Authority is empowered to issue necessary guidelines to prevent unfair trade practices and protect consumers' interest. Such guidelines may relate to the trade practices of CSPs.	Section 18(2)(l), the Consumer Protection Act.
12.	For the purpose of investigation under section 19(1), the Central Authority, the Director General or the District Collector may call upon any person accused of a violation of consumer rights, unfair trade practices and false/ misleading advertisements and also direct such person to produce any document or record in his possession. CSPs that violate any consume rights/commit unfair trade practices/cause any false or misleading advertisements may be directed to produce documents/records under this provision.	Section 19(3), the Consumer Protection Act.
13.	For the purpose of conducting an investigation under section 19(1), the Director-General or any other officer authorised by him in this behalf as well as District Collectors, have the powers of search and seizure,[82] if they have any reason to believe that any person has violated any consumer rights or committed unfair trade practice or caused any false or misleading advertisement to be made. CSPs that violate any consume rights/commit unfair trade practices/cause any false or misleading advertisements may be made subject to a process of search and seizure under this provision.	Section 22(1), the Consumer Protection Act.
14.	A product liability action may be brought by a complainant against a product service provider for any harm caused to him on account of a defective product. Thus, such complaints may be brought against CSPs that qualify as product service providers under the Consumer Protection Act.	Section 83, the Consumer Protection Act.
15.	A product service provider shall be liable in a product liability action and may be required to pay compensation, if-- (a) the service provided by it was faulty/ imperfect/deficient/inadequate in quality, nature or manner of performance which is required under any law or contract or otherwise; or (b) there was an act of omission/commission/negligence/conscious withholding of any information which caused harm; or (c) the service provider did not issue adequate instructions or warnings to prevent any	Section 85, the Consumer Protection Act.

[82] *Per* section 22(1), these powers would include: (a) entering at any reasonable time into any such premises and searching for any document or record or article or any other form of evidence and seizing such document, record, article or such evidence; (b) making a note or an inventory of such record or article; or (c) requiring any person to produce any record, register or other document or article.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	harm; or (d) the service did not conform to express warranty or the terms and conditions of the contract. Thus, CSPs that qualify as product service providers under the Consumer Protection Act can be held liable in a product liability action in the situations outlined above.	
16.	The District Commission[83] is empowered to requisition from an electronic service provider, such information, documents or records, as may be required for the purpose of proceeding with a complaint in relation with services provided by such electronic service provider. Thus, CSPs that qualify as electronic service providers under the Consumer Protection Act will have to comply with this requirement.	Section 38(4), the Consumer Protection Act.
17.	Where the District Commission is satisfied that any of the allegations contained in the complaint relating to the services or claims for compensation under product liability are proved, it may order, *inter alia* that: (i) the service provider pay such compensation or punitive damages to the consumer as may be awarded; (ii) the service provider pay the compensation awarded in a product liability action; (iii) the deficiencies in the services be removed; (iv) the service provider desist from offering services which are hazardous in nature; (v) the service provider pay such sum as may be determined, not being less than twenty-five per cent. of the value of defective service provided; (vi) the service provider adequate costs be paid to the parties; and (vii) the service provider cease and desist from issuing any misleading advertisement CSPs as service providers may therefore be subject to such directions from the District Commission.	Section 39(1), the Consumer Protection Act.
18.	Electronic service providers are required to designate a nodal officer to accept and process notices that may be served by the District/ State [84] / National [85] Commissions. Thus, CSPs that qualify as electronic service providers under the Consumer Protection Act will have to comply with this requirement.	Section 65(2), the Consumer Protection Act.
19.	The central government is empowered to take measures for the purposes of preventing unfair trade practices in e-commerce,	Section 94, the Consumer Protection Act.

[83] *Per* section 2(15) read with section 28, the "District Commission" means the District Consumer Disputes Redressal Commission established by the State Government in every district of the State.
[84] *Per* section 2(44) read with section 42(1), the State Commission means the State Consumer Disputes Redressal Commission established by the State Government.
[85] *Per* section 2(29) read with section 53(1), the National Commission means the National Consumer Disputes Redressal Commission established by the Central Government.

NO.	PROVISIONS GOVERNING CSPS	PROVISION
	direct selling and also to protect consumer rights and interests. Such measures may relate to the trade practices of CSPs.	

TABLE 12: REGULATION OF CSPS UNDER THE PDP BILL

No.	CSP obligations/regulatory framework	Relevant provision under the PDP Bill
1.	All CSPs owe a duty to their users to process their personal data in a fair and reasonable manner and maintain their privacy.[86] Personal data must be *inter alia* collected and processed only for clear, specific and lawful purposes and collection must take place under a notice which informs the data principal of a number of certain prescribed information regarding the collection, processing, etc. Failure to process personal data in accordance with these provisions may result in penalties of up to INR 150000000 or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher. In any other case, failure to comply with this requirement could result in the CSP being liable to pay a penalty of up to INR 25,00,000.[87]	Section 4 read with Section 69, 73, PDP Bill.
2.	CSPs must comply with the grounds for processing as contained in Chapter III with respect to personal data and Chapter IV with respect to sensitive personal data. In case of failure to process data in compliance with this requirement, CSP may face penalties of up to INR 150000000 or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher.	Chapters III and IV, Section 69, PDP Bill
3.	CSPs and employees of CSPs are required to process data only as per the instructions of the data fiduciaries that engage/appoint/use their services. Additionally, CSPs/their employees are under a duty to keep all personal data as confidential.[88]	Section 37, PDP Bill.
4.	Having regard to the nature and scope of processing of personal data undertaken by CSPs, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, CSPs must implement appropriate security safeguards, including: (i) the use of methods such as encryption and de-identification; (ii) taking steps	Section 31, PDP Bill.

[86] *Per* Section 4, "Any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal."

[87] *Per* Section 73,"Where any person fails to comply with any provision of this Act, or rules prescribed or regulations specified thereunder as applicable to such person, for which no separate penalty has been provided, then such person shall be liable to a penalty subject to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in all other cases."

[88] *Per* Section 37 – "(1) The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.
(2) The data processor referred to in sub-section (1) shall not further engage, appoint, use, or involve another data processor in the relevant processing on its behalf except with the authorisation of the data fiduciary, unless permitted through the contract referred to in sub-section (1).
(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential."

No.	CSP obligations/regulatory framework	Relevant provision under the PDP Bill
	necessary to maintain the integrity of personal data; (iii) taking steps to prevent the misuse, modification, unauthorised access and destruction of personal data.[89] Additionally, all CSPs must undertake a review of their security safeguards periodically, as may be specified.	
5.	Any CSP/employee of a CSP that knowingly, intentionally or recklessly engages in the re-identification and processing of de-identified personal data can be punished with imprisonment for 3 years or/and fine of INR 2,00,000.[90] Where a CSP is held liable for an offence under this provision, every person who was in charge of, and was responsible for the conduct of the business of the CSP ("**Responsible personnel**") shall be deemed guilty of the offence and shall be liable to be proceeded against and punished accordingly.[91]	Section 92 read with Section 95, PDP Bill.
6.	If a CSP/employee of a CSP unlawfully (i) obtains; (ii) discloses; (iii) transfers; or (iv) sells or offers to sell any personal data in any manner, resulting in any harm to a data principal, it may face up to 3 years of imprisonment and/or fine up to INR 2,00,000.[92] Where a CSP is held liable for an offence under this provision, the Responsible personnel of the CSP shall be deemed guilty of the offence and shall be liable to be proceeded against and punished accordingly.[93]	Section 90 read with Section 95, the PDP Bill.
7.	If a CSP/employee of a CSP in any manner unlawfully (i) obtains; (ii) discloses; (iii) transfers; or (iv) sells or offers to sell any sensitive personal data, resulting in any harm to a data principal, it may face up to 5 years of imprisonment and/or fine up to INR 3,00,000.[94] Where a CSP is held liable for an offence under this provision, the Responsible personnel of the CSP shall be deemed guilty of the offence and shall be liable to be proceeded against and punished accordingly.[95]	Section 91 read with Section 95, the PDP Bill.

[89] *Per* Section 31, "(1) Having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data fiduciary and the data processor shall implement appropriate security safeguards including: (a) use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; and (c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data. (2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly."

[90] *Per* Section 92 – "(1) Any person who, knowingly or intentionally or recklessly - (a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or (b) re-identifies and processes such personal data as mentioned in clause (a) without the consent of such data fiduciary or data processor, then such person shall be punishable with imprisonment for a term not exceeding three years or shall be liable to a fine which may extend up to rupees two lakh or both. (2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided under this section, if she proves that - (a) the personal data belongs to the person charged with the offence under sub-section (1); or (b) the data principal whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act."

[91] Section 95, the PDP Bill.
[92] Section 90, the PDP Bill.
[93] Section 95, the PDP Bill.
[94] Section 91, the PDP Bill.
[95] Section 95, the PDP Bill.

No.	CSP obligations/regulatory framework	Relevant provision under the PDP Bill
8.	A CSP must ensure storage of a serving copy of personal data on a server located in India and may only transfer personal data outside the country if any of the following conditions are met: (i) if the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Data Protection Authority ("**DPA**"); (ii) if the transfers are to a country, a sector in a country or to an international organisation that the central government in consultation with the DPA deems permitted; (iii) in a situation of necessity as determined by the DPA; (iv) in addition to conditions (i) and (ii) above, if the consent of the data principal is obtained for the transfer of personal data or the explicit consent of the data principal has been obtained for the transfer of sensitive personal data. Additionally, certain information may be notified as 'critical personal data' under the PDP Bill, which shall only be processed in a server or data centre located in India.	Chapter VIII, PDP Bill
9.	The Data Protection Authority ("**DPA**") is required to perform a number of functions under the PDP Bill. In particular, the following functions of the DPA are relevant for CSPs: (i) the power to monitor and enforce provisions of the PDP Bill; (ii) the power to promote measures for innovation in protection of personal data; (iii) the power to monitor cross-border transfers of personal data; (iv) the power to issue codes of practice; (v) the power to advise the central/state governments and Parliament on measures to be taken for data protection; (vi) the power to issue guidance on any provision of the PDP Bill; (vii) the power to monitor technological developments and commercial practices that may affect the protection of personal data; (viii) the power to promote measures and undertake research for innovation in the field of protection of personal data; and (ix) the power to receive and handle complaints (such as user complaints seeking compensation from CSPs under Section 75) under the PDP Bill.[96] As detailed in the rows below, the DPA is empowered to issue codes of practice, issue directions, call for information, conduct inquiries and authorise search and seizure activities for the discharge of its functions under the PDP Bill. Thus, CSPs may be required to comply with directions/calls for information/codes of practice/inquiries/search and seizure activities that are authorised by the DPA in exercise of its powers.	Section 60, the PDP Bill.
10.	As mentioned above, the DPA can issue codes of practice to facilitate compliance with the obligations of the PDP Bill. In particular, the DPA is	Section 61, PDP Bill.

[96] Section 60, the PDP Bill.

No.	CSP obligations/regulatory framework	Relevant provision under the PDP Bill
	empowered to issue codes of practice on the following matters that may be relevant for CSPs[97]: (i) the exercise of data principal rights, such as the right to seek compensation under Section 75 of the PDP Bill; (ii) the requirement for data processors to process data only as per the instructions of the data fiduciaries, as required under Section 37 of the PDP Bill; (iii) standards for security safeguards to be maintained by data processors under section 31 of the PDP Bill; (iv) methods of de-identification and anonymisation to be used by data processors while implementing the security safeguards under Section 31 of the PDP Bill; (v) appropriate action to be taken by data processors in response to a personal data breach under Section 32 of the PDP Bill.	
11.	The DPA can issue directions to CSPs to discharge its functions under the PDP Bill.[98] Failure to comply with these directions can result in the CSP being liable to pay a penalty which may extend to INR 5,000 per day, and if such default continues, a maximum of INR 50,00,000.[99]	Section 62 read with Section 72, the PDP Bill.
12.	The DPA can call for such information from CSPs as may be reasonably required for the discharge of its functions under the PDP Bill. This information must be provided in the format prescribed by the DPA.[100] Failure to furnish information will make the CSP liable to pay a penalty of up to INR 25,00,000.[101]	Section 63 read with Section 73, the PDP Bill.
13.	The DPA can conduct an inquiry into the activities of a CSP, if it has reasonable grounds to believe that the CSP: (i) conducts any activity that is detrimental to public interest; (ii) violates any provision of the PDP Bill, its rules and regulations; or (iii) does not adhere to any direction of the DPA.[102] On the basis of such inquiry, the DPA can (i) issue a reprimand to the CSP; (ii) ask the CSP to cease and desist the problematic activity; (iii) require the CSP to change its business model; (iv) direct the CSP to suspend or discontinue its business; or (v) suspend or cancel its registration, if any.[103] If the CSP fails to adhere to the order of the DPA, it will be liable to pay INR 5,000 per day up to INR 50,00,000.[104]	Section 64 read with Section 65 read with Section 72, PDP Bill.
14.	The DPA can require CSPs or any of its employees to furnish any information, books or records that it deems necessary for purposes of an inquiry. [105] If a CSP fails to furnish such information, the DPA can (i) enter	Section 64 and Section 66 read with Section 73, PDP Bill.

[97] Section 61, the PDP Bill.
[98] Section 62, the PDP Bill.
[99] Section 72, the PDP Bill.
[100] Section 63, the PDP Bill.
[101] Section 73, the PDP Bill.
[102] Section 64, the PDP Bill.
[103] Section 65, the PDP Bill.
[104] Section 72, the PDP Bill.
[105] Section 64, the PDP Bill.

No.	CSP obligations/regulatory framework	Relevant provision under the PDP Bill
	and search any premises where such information is kept; (ii) seize any books, register or documents; (iii) access any computer resource or device having any information; or (iv) make copies of any information or documents retrieved. [106] The DPA may also impose a penalty of up to INR 25,00,000 if the CSP fail to comply with any such request for information.[107]	
15.	The DPA can issue regulations on the manner of periodic review of security standards required to be implemented by CSPs under Section 31 of the PDP Bill.[108]	Section 108, the PDP Bill.
16.	If CSPs fail to pay any penalty payable by them under the provisions of the PDP Bill, the DPA may appoint a recovery officer to recover such amount by (i) attaching and selling immovable and movable properties of the CSP; (ii) attaching the bank accounts of the CSP; (iii) arresting or detaining Responsible Personnel of the CSP in prison; or (iv) appointing a receiver to manage the CSP's movable and immovable properties.[109]	Section 108, the PDP Bill.

[106] Section 66, the PDP Bill.
[107] Section 73, the PDP Bill.
[108] Section 108, the PDP Bill.
[109] Section 78, the PDP Bill.

ANNEXURE II

TABLE OF INDUSTRY BODIES MENTIONED IN THE TRAI CONSULTATION PAPER ON CLOUD SERVICES

No.	Industry body	Provisions showing voluntary nature of the organization	Provisions showing self-regulation and no government intervention
1.	**Cloud Industry Forum (CIF)**	The CIF Code of Practice[110] ("**CIF Code**") does not specify any best practices for CSPs, except with respect to transparency. CSPs complying with the CIF Code are required to conduct themselves in an open and transparent manner, so as to facilitate decision-making and management by purchasers of their services. However, the CIF Code does not intend to make decisions for purchasers; it only seeks to ensure that essential information about the cloud services is available to them.	CIF is a membership-based, not-for-profit organisation. As per its website[111], it 'answerable' only to its members. Organizations claiming to be compliant with the CIF Code need to conduct an annual self-certification. After confirming the successful results of this certification to the CIF, they are authorized by CIF to use CIF's 'certification mark' for the following year. CIF operates a Compliance Committee to oversee complaints and decide on their validity. There is no government intervention in the functioning of CIF[112].
2.	**Cloudcode- New Zealand Cloud Computing Code of Practice**	The CloudCode is a voluntary code of practice[113]. A CSP which becomes a signatory to the code represents to the public that they comply with the CloudCode's requirements. The CloudCode does not in any way place legal obligations on signatories to the Code. However, CSPs would be liable for non-compliance with the code where it amounts to a	The CloudCode does not provide for any kind of government intervention in its functioning, whether directly or indirectly. It has only a complaints committee which considers complaints regarding member CSPs not meeting the CloudCode requirements, which may result in withdrawal of such CSP's signature from their register.

[110] CIF Code of Practice, Cloud Industry Forum, https://www.cloudindustryforum.org/content/cif-code-practice.
[111] Governance Framework, Cloud Industry Forum, https://www.cloudindustryforum.org/content/governance-framework-0.
[112] Complaints and procedures, Cloud Industry Forum, https://www.cloudindustryforum.org/content/complaints-and-procedures-0
[113] CloudCode- Cloud Computing Code of Practice- New Zealand, Version 2.0, July 2013, https://cloudcode.nz/upload/files/NZCloudCode.pdf.

No.	Industry body	Provisions showing voluntary nature of the organization	Provisions showing self-regulation and no government intervention
		violation of any general law (e.g. for misleading and deceptive conduct, an offence under fair trading legislation in most countries).	
3.	**Cloud Computing Innovation Council of India (CCICI)**	The CCICI has voluntary membership.	They have a governing board and executive committee. However, there is no government intervention of any kind.
4.	**EU Data Protection Code of Conduct for Cloud Service Providers, or EU Cloud Code of Conduct**	The EU Cloud Code of Conduct[114] ("**EU Cloud CoC**") is a voluntary document under Article 40 of EU's General Data Protection Regulation ("**GDPR**"). Any CSP may choose to sign up any or all of its cloud service offerings to the EU Cloud CoC, provided that the CSP meets all requirements of the EU Cloud CoC. It is a comprehensive code, and covers areas such as data processing, customer audits and cross-border transfer of personal data.	The EU Cloud CoC provides for a monitoring body which looks into complaints of violation of any provisions of the code. The monitoring body is also empowered to impose sanctions on the CSP, which range from public reprimand of the CSP to revocation of membership. However, there is no government intervention in the functioning of the EU Cloud CoC. Governments are, however, entitled to register themselves as 'supporters' in the General Assembly formed under the code. Supporters do not enjoy any kind of voting powers in the General Assembly.
5.	**Asia Cloud Computing Association (ACCA)**	Membership is completely voluntary. There is no code of conduct or rules or regulations for members.	The organization does not have any kind of government intervention in its functioning.
6.	**National Association of Software and Services Companies (NASSCOM)**	Membership is completely voluntary. There is no code of conduct or rules or regulations for members.	The organization does not provide for any kind of government intervention in its functioning.

[114] Request the EU Cloud Code of Conduct, https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html.

No.	Industry body	Provisions showing voluntary nature of the organization	Provisions showing self-regulation and no government intervention
7.	**Telecommunications Standards Development Society, India (TSDSI)**	Membership to the society is completely voluntary. However, the society's rules allow government representatives to also become members of the society [115] . Even government departments or agencies can become corporate members of the society. The Governing Council of the society must have certain number of members from the relevant government departments.	The rules and regulations of the society do not provide for any kind of government intervention in its functioning. However, if a government is a member of the society, then it cannot be dissolved without the consent of that government.
8.	**Association of Mutual Funds in India (AMFI)**	Membership to the AMFI is completely voluntary.	The AMFI code of ethics[116] does not provide for government intervention in their functioning.

[115] Rules and regulations, Telecommunications Standards Development Society of India (TSDSI), https://tsdsi.in/wp-content/uploads/2019/08/TSDSI-PLD-30-V1.0.0-20141217.pdf.

[116] Code of Ethics, Association of Mutual Funds of India, 11 September 1997, https://www.amfiindia.com/Themes/Theme1/downloads/AMFI_Code_of_Ethics.pdf.