

No.:157/TRAI/2019-20/ACTO

Dated: 3rd June, 2019

Shri Vinod Kumar
Jt. Advisor (NSL)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi - 110 002

Ref: **ACTO's counter comments to the responses on TRAI's Consultation Paper [No. 02/2019] dated March29, 2019 on Review of Terms and Conditions for registration of Other Service Providers (OSPs)**

Dear Sir,

This is with reference to the *Consultation Paper on Review of Terms and Conditions for registration of Other Service Providers (OSPs)* issued by Hon'ble Authority. In addition to our comments filed vide letter No. 315/TRAI/2019-20/ACTO dated 20th May,2019 Association of Competitive Telecom Operators (ACTO), is pleased to provide counter comments in support of the specific issues where some of the stakeholders have divergent views.

We hope that our counter comments (enclosed as Annexure - I) will merit the kind consideration of the Hon'ble Authority.

Respectfully submitted,

Yours sincerely,

for Association of Competitive Telecom Operators

Tapan K. Patra
Director

Encl: As above

Annexure-I
Counter Comments on TRAI Consultation Paper
on
Review of Terms and Conditions for registration of Other Service Providers (OSPs)

ACTO had submitted a detailed response to all questions as stated in the consultation paper. Few stakeholders have expressed their views on some of the questions which is at variance with suggestions provided by ACTO. We believe that such views from these stakeholders (Airtel, Vodafone, TCL and COAI) are not accompanied with any substantive reasons though. We have therefore placed our views against each of such issues along with the reasons to counter such varying position for your kind consideration.

1. Registration & Definition of Application Service (Q1 &Q2)

With respect to the issue of registration & definition, few stakeholders namely COAI, Airtel and Vodafone-Idea and have expressed as-

1. *"We believe that the definition given in DoT's guidelines is good enough to capture all possible scenarios of application services."*
2. *"In our views, registration of OSP should be continued as it is required the objectives defined by the government."*
3. *"Yes, the registration of OSPs should be continued so that DoT/TERM Cells can ensure that there is no toll bypass or switched telephony activity being undertaken by OSPs which are non-permissible activities under the scope of registration."*

ACTO's counter comments:

With the rapid technological development, the current definition of OSP does not fit in the realities and requirements of an ever evolving digital world. The definition of "Application Services" is very wide and indicative and it may include OTT applications, as well as every activity which comes under IT/ITES services as well. The reference to the word "Application" itself is not appropriate. Instead the requirement to seek OSP registration should apply to the specific "outsourcing" activity and not all applications / IT/ITES services which may be unrelated to outsourcing operations. So reference to application itself needs to be removed and replaced with the word "outsourcing". Only voice-based calling services should be included in the definition, voice calling can be through PSTN and / or emerging unified collaboration tools like skype, lync, internet telephony etc. Captive services should also be kept out of the purview of OSP registration. **Further it must not include services purely based on data or internet.**

The OSP registration is not granted under Section 4 of Indian Telegraph Act 1885. Another example of registration is IP-1. The same is a four page document with no comparable obligations and seems to be a real registration. However, the OSP registration process is detailed, lengthy and seeks numerous technical details and is always open for government inspection. Therefore, in order to meet the Government requirement, a single page OSP registration similar to IP-1 should suffice.

A light touch regulatory framework with simple compliances for the purposes of meeting three objectives i.e., (i) Statistical information(ii) Ensuring that their activities do not infringe upon the jurisdiction of other access providers(iii) Providing special dispensation to boost the BPO sector, laid out by Government for OSP should be sufficient. The registration should accord right to operate OSP activity not how to operate.

Our recommendation is that the OSP registration should be limited to an online form providing details of the establishment and a self- declaration on compliance with the Indian Telegraph Act, 1885 that no telecom services would be provided from the premises. This should only cover outsourcing units but not for the captive units of companies.

2. Validity of registration (Q3)

With respect to this issue of validity of registration, stakeholders namely COAI, Airtel, TCL and Vodafone-Idea have expressed that *“The validity of OSP and validity period of renewal of OSP registration is sufficiently long and the same may be continued. Presently applicable validity of 20 years and renewal for 10 years can be continued”*.

ACTO’s counter comments:

As OSP Registration is meant for statistical purposes, there is no case for OSPs to operate under limited period and seek renewal thereafter. It should be left to the OSP Company to intimate to DoT if it wishes to stop undertaking OSP activities. Alternatively, there is also a process of cancellation of OSP registration in case of non-compliance relating to non-filing of Annual Returns. IP-I registration accorded by DoT, has no validity, so why should OSP registration (also issued by DoT has a limited validity clause) Limiting the validity does not serves any purpose except placing an obligation on the OSP company to apply for renewals which is not needed given the powers with DoT to cancel the registration in case of non-compliance. Therefore, there needs to be parity across all registrations issued by DoT in terms of validity and OSPs should not be an exception.

3. Internet connectivity to OSP (Q9)

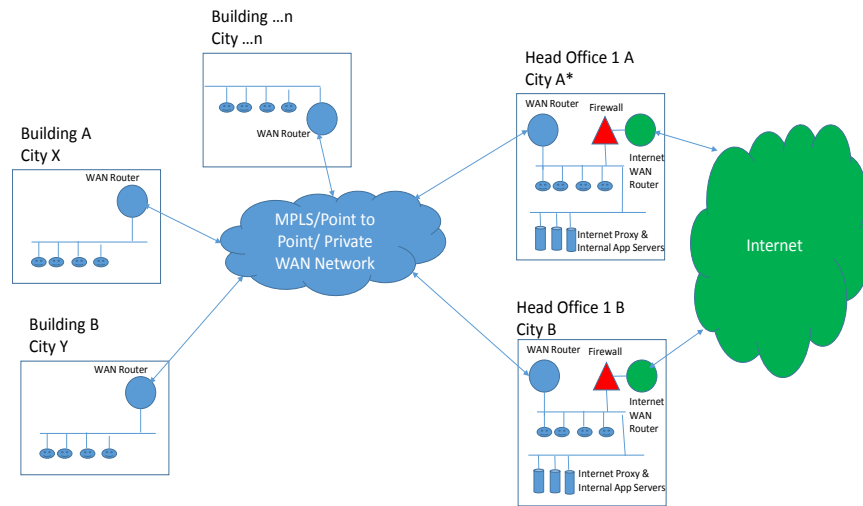
With respect to the issue of internet connectivity to OSP, stakeholders namely COAI and Airtel, have stated that *“The OSPs are not authorized to distribute internet connectivity to any other location. Therefore, OSPs have to obtain internet access service at each location from Licensed ISPs/ Access Service Providers only.”*

ACTO’s counter comments:

We agree that internet connectivity to OSPs should be from authorized ISP only including UL-VNO licensees with Internet authorisation. However, there should not be any mandate to take internet connectivity in each city rather the guidelines should be flexible to allow internet connectivity from a centralized node in India from a category – A, ISP whose scope of service is Pan India and can serve customers anywhere in India through a centralized setup in India. OSPs are not distributing the internet service but securing internet connectivity from authorized ISPs –category –A to provide OSP services as

an end user. Requirement to obtain internet connectivity at each location is required when the internet service is taken from category B or C ISP licensees.

Further there have been, emerging technology formats which permits alternate use of connecting multiple locations through a single logically partitioned bandwidth / leased line for example, VRF (Virtual Routing and Forwarding) explained as below:



*All city locations in India only.

As seen in the above diagram, enterprise customers access the internet service via logically partitioned VPN tunnel. During this, public traffic is not getting connected with VPN/ MPLS as it is logically bifurcated via virtual routing and forwarding. Only backhaul bandwidth is shared for VPN traffic and internet traffic and front-end routers, firewalls etc are separate. Therefore, it is in compliance with respective licenses. Since the OSP guidelines permit a centralized EPABX for both public and private traffic with logical partitioning, the same should also be extended to such emerging technologies so that OSPs as well as ISPs need to set up separate connectivity for carrying internet and VPN traffic. A common VPN/MPLS traffic can be logically partitioned with adequate safeguards wherein both internet and MPLS traffic can move from one location to another without getting mixed.

Lastly, in the event of a disaster, OSPs should be allowed to leverage infrastructure and internet connectivity located in the cloud (outside India) from a recovery/business continuity purposes for a limited period. Once the steady state is attained the connectivity can be restored to the Indian telecom service provider. If need be an intimation mechanism which currently exists in the guidelines can be extended to cover such force majeure / disaster recovery situations.

4. CCSP/HCCSP (Q 21)

With respect to this issue of CCSP/HCCSP stakeholders namely COAI, Airtel and TCL, have suggested that-

1. "Due to the scope defined under the license only access providers can provide CCSP/HCCSP service to the OSP."
2. "CCSP/HCCSP may be brought under OSP registration with a separate category of OSP viz CCSP/HCCSP or platform as a service provider and separate terms and conditions to be followed by such CCSP/HCCSP. It is also

proposed to have as separate category as CCSP/HCCSP OSP which could serve domestic and international OSP customers from their setup established in India. In this scenario, OSPs shall continue to take resources from authorized TSPs, hence there is no infringement of the scope of service of authorized TSPs.”

ACTO’s counter comments:

In our submission to this consultation paper, we have explained in detail along with diagram, how HCC solution does not infringe local TSPs scope of services and on the contrary it acts as a complimentary service as TSP’s are likely to deploy these solutions for their enterprise customers under a centralized model. HCC solutions can be offered by existing telecom service providers as per their respective scope of service and is not restricted only to access service providers. If need be service providers can buy resources or connectivity from each other (as permitted) to provide HCC solution to their customers. In such models, the connectivity is always provided by licensed telecoms service providers which include Access, ISP, NLD and ILD licensees. Such services should be provided by all telecom licenses to the extent permitted under their respective licenses. There should not be any additional registration for entities which do not hold any telecom licenses provided such entities undertake to not provide any service which falls under the domain of respective telecom licenses.

As far as the call flow is concerned, we would like to illustrate below each scenario clearly for ease of TRAI reference:

- a) **Domestic Off-Net Call:** A user at India OSP site, wishes to make/receive a domestic call using the office PSTN lines. In such scenario the call will at all time remain in India and only a signaling will transmit to HCC site. Thus, there is no revenue loss to the access operator. There will be voice gateway deployed at each site to cater to these PSTN call based requirements and all logical separation from IP lines and logs/CDRs will be kept at HCC.
- b) **International Off-Net Call:** A user at OSP India site, wishes to make an International Off-Net Call. The call will be generated over OSP VPN at India end and it would reach the far end (country where the call needs to terminate) and from there the call will be handed over to domestic operator for the final leg. This is exactly how the call flow will be if PBX is hosted at customer site. Thus, there is no negative revenue impact on revenue of domestic TSPs.
- c) **On-Net Call:** A user at India site, wishes to make between two office sites of theirs either within or outside of India. Call between customer sites would happen via IP VPN to/from another customer site (also connected IP VPN) without further break-out into/from PSTN network). There is no negative revenue impact, as the call flow is same as in tradition on site PBX set-up.

The CCSPs/HCCSP’s should be seen as technology enablers and not conventional telephony service providers. The use of multi-tenanted IP-EPABX/EPABX hosted on public cloud or private cloud at non-Indian location should be permitted as long as CDR’s are preserved by OSP’s. Usually, CCSP’s and HCCSP’s provide full access to OSP’s respective tenants and facility to store CDR’s & other QoS reports on cloud or export to their premises based servers. For periodical inspection purposes, OSP get full access to platform and should be able to demonstrate access to CDR’s stored on cloud or copy of it on their local servers.

We therefore suggest that -

- i. HCC/ CCSP solutions are the innovative multi-tenant technological solutions for better working of outsourcing sector in the country with minimal investment by OSPs.
- ii. Considering HCC/CCSP solutions are at the nascent stage in India, thus any form of regulatory oversight could be detrimental to this Industry. There is no need for any additional regulatory oversight as such services are predominantly provided by licensed TSPs. For non-licensed entities not providing any switching or routing facilities, there should not be any license or regulation.
- iii. There should be no registration or additional license to provide HCC/CCSP services in India and current TSPs including Access, NLD and ILD operators should continue be allowed to provide these solutions to their enterprise customers.
- iv. OSPs should be free to outsource their equipment's and services to HCC/ CCSP and extent of hosting should be left to mutual agreement between OSPs and their CCSPs.
- v. Since OSPs would front end all the compliances thus there should not be a need for any regulatory intervention.

5. Monitoring provisions for use of CUG for internal communications (Q24)

With respect to this issue of monitoring provisions for use of CUG, stakeholders namely COAI, Vodafone-Idea and Airtel, have suggested *“Yes, we agree for monitoring provisions for use of CUG for internal communications of OSP mentioned in the OSP guidelines.”*

ACTO's counter comments:

CUG is for internal communication only which uses extension as against 10 digit or 8 digit dialing and requires no connectivity to PSTN/PLMN network. Such communication is internal to the company and should not be privy to anyone. It can also be captive and / or non OSP in nature. Therefore, monitoring provisions for use of CUG for internal communications is not justifiable as it may lead to monitoring of all private communications. CUG communications is governed by internal policies of the company and does not require any additional oversight or monitoring by way of a regulatory or policy intervention. This is unrelated to OSP guidelines as the agent or employee may need to communicate internally within the organization for their administrative or internal issues.

6. Work from Home (Q25)

With respect to this issue of Work from Home, stakeholders namely Vodafone-Idea, has stated that – *“Agree with the provisions for Work from Home as mentioned in the OSP guidelines.”*

ACTO's counter comments:

We strongly suggest for the removal of the barriers like requirement of PPVPN, Bank Guarantee etc as there is a urgent need to facilitate work from home concept to give the technological benefits, fillip to rural BPOs, employment generation / startup missions especially at the remote, tier 2 and 3 cities. Due to the current strict policies including the financial entry barriers, work from home as a concept and

registration has not met with the desired success. More importantly, when there are alternate and convenient technological tools available which enable access to office VPN from home to work, where is the incentive left to register as an OSP under work to home category. In such a situation the guidelines on work to home are infructuous and outdated. The objective of work from home has the ability to provide and generate employment especially for women who would like to work from home. This concept is good but it should come with the attached flexibility for the purpose it was created and should be kept outside the ambit of OSP guidelines. Corporations today permit their employees to work from home as per the work requirements. The objective is to make working flexible which is the case in a non OSP scenario. In case of OSP such flexibility has been taken away due to burdensome compliances and obligations. At the most the work from home locations can be filed on intimation basis. The need for PPVPN and / or submission of bank guarantees creates cost barriers for enterprises to flourish. The guidelines also have never provided any explanation to these aspects. Therefore, given the fact that the concept has been more or less a non starter, more flexibility needs to be accorded for entities those who plan to allow their staff to work from home or create BPOs for job creation in rural and far flung areas where connectivity, electricity etc are irregular. There should not be a need to have only PPVPN or submission of bank guarantees. This is important for the proliferation of rural BPOs as well as a major game changer in terms of job creation in tier 2 and 3 cities.

7. Domestic operations by International OSPs for serving their customers in India may be allowed (Q26)

With respect to this issue of Domestic operations by International OSPs, stakeholders namely Airtel, COAI, Vodafone-Idea, has suggested that-

1. "OSP is not allowed to provide or resell telecommunication services or infringe upon the domain of licensed service provider. Operation by OSP in any manner cannot result in revenue loss to the government & TSPs which can be way of reselling of telecom services, toll bypass etc."
2. "As per the current conditions domestic traffic not be routed to any place outside India. Therefore domestic operations by International OSPs for serving their customers in India may not be allowed. Such dispensation may have security implications which also need to be kept in view."
3. "International & Domestic OSPs are separate and distinct categories under the OSP guidelines/framework."

ACTO's counter comments:

Firstly, the point mentioned in serial no.2 above is not correct. The actual license condition emanated from Press Note 3 of 2007 states: *"For security reasons, domestic traffic of such entities as may be identified /specified by the licensor shall not be hauled/routed to any place outside India" (emphasis supplied)"*

No entities have been identified so far. The above License requirement applies to all licensed TSPs and not to registered OSPs. OSPs will have connectivity as permitted to their underlying TSP. If there is something which the underlying TSP is not permitted by virtue of their license or otherwise, OSPs cannot use the said connectivity. Therefore, if the TSP is directed to route traffic of such entities as may be identified or specified by the DoT, it will have to comply and so will be the case of OSP. However, in

the absence of the same, the requirements cannot be extended to OSP and restrictions be imposed such that a separate domestic OSP registration is required to be taken. This is not reselling of telecom services or infringement upon the domain of licensed TSPs as has been noted.

By allowing international OSP to serve the domestic customer will be a perfect example towards ease of doing business in India. From security point of view, all CDRs may be maintained in India and be available to Law Enforcement Agency (LEA) and it will help to reduce the business cost.

ACTO members fully support domestic operation by international OSP. The consultation paper has highlighted the issue not from any security but largely from infringement perspective. Once it is ensured that there is no infringement and the requirements of the LEA's are met by OSPs, in such a scenario it should be left for the OSP companies how to operate as the resources are always taken from licensed TSPs and used as required under the telecom rules and regulations, so this should be permitted. Additionally, OSPs are always governed by TSPs though suitable documentation related to KYC followed by periodic site inspections. So both OSPs and TSPs are aware about the requirements and how to use the telecom resources and connectivity thus subscribed.

8. EPABX at foreign location and Security conditions in Chapter V of OSP guidelines (Q27 & 28)

With respect to this issue of EPABX at foreign location and Security conditions, stakeholders namely COAI, Vodafone-Idea, have suggested that

1. *"We are of the view that use of EPABX at a foreign location in case of International OSPs should not be allowed in view of national security."*
2. *"The use of EPABX at foreign location in case of international OSP should not be allowed as there will be no means to undertake periodic inspection of the EPABX at the foreign location."*

ACTO's counter comments:

We disagree with such restrictive view and reiterate that there should not be any mandate on in country location of EPABX. OSPs should be given flexibility to set up the EPABX at any of their identified locations provided during the course of OSP registration. We have given a detailed submission on this issue in our response to this consultation paper. On security issue, if all logs, Call Data Records (CDRs) are available at customer site as well. Customer can show /share the system logs and also show CDRs over the laptop from customer premises itself at any point of time. Thus, all functionality can be shown to DOT at any point of time for each of the OSP center in similar manner to a physically located localized PBX on a real time basis. The location of the PBX is not material to the submission of information for audit purposes.

In addition, customer can also be asked to keep CDRs at their location by retrieving CDRs on periodic intervals as stipulated by DOT and can also store the same for the stipulated period.

It is also very detrimental for the OSPs to create a separate infrastructure including call manager in India which is highly taxing on their business models and challenging for technical integration point of view. To clarify, international clusters/ call managers which are based on big multitenant platforms cannot easily sync with local on-site EPABX and customer may need to comprise on various functionality.

In today's world, location of physical box like EPABX is immaterial as far as security or monitoring is concerned. EPABX requires hardware but all functions are implemented in software. There is a drastic change in last two decades. The security concern will not be met just by having the physical entity in desired location.

Keeping the physical infrastructure at one place based on scale and serving it to many place even different countries are the current business practice across the globe. It makes business more effective and efficient in super competitive market. As long as security concern is met relating to access to data is met, policy/regulation should not mandate to have equipment in a preferred place but this should be left to the OSP as to how they plan their network to derive maximum efficiencies from cost and technology perspective.

ACTO members support rules which permit setting up of EPABX anywhere in the cloud being at any country and not tied to a particular location or country. Irrespective of the location, security related requirements will be met. There is a need to allow to deployment of EPABX in Cloud datacenter. The cloud infrastructure at location of choice of customer whether in India or outside India shared between several customers and accessed remotely by customer and for monitoring purpose.

ACTO recommends that the OSP regulations should be suitably amended to allow the user to be able to embrace the cloud based contact center solution to leverage best of the technology solution for its business needs while at the same time meeting the reasonable regulatory requirements. This will be in line with the realities as stated under DoT's reference dated 10th September, 2018 to TRAI on the subject paper.
