Government of India
Ministry of Communications
Department of Telecommunications
20-Ashok Road, Sanchar Bhawan, New Delhi-110 001

No. 18-8/2020-CS-I (Pt.)   Dated the 23rd June, 2021

Subject: Revised Guidelines for Other Service Providers (OSPs)

The Guidelines for Other Service Providers (OSPs) were liberalized vide Department of Telecommunications (DoT)'s Order No. 18-8/2020-CS-I dated 5th November, 2020.

These Guidelines have now been further simplified and revised. Accordingly, in supersession of the earlier orders, Revised Guidelines for OSP are enclosed herewith. These will come into force with immediate effect.

A copy of these Guidelines is being placed on the DoT's website. (https://dot.gov.in/carrier-services)

Enclosed: Annexure.

(Ajay Negi) 23/6/21
Director(CS-I)
Tel. No. 011-23036253

Revised Guidelines for Other Service Providers (OSPs)
(Applicable w.e.f. 23.06.2021)

Chapter – 1   Definitions

The terms used in this document, unless the context otherwise requires, have the following meaning:

1. 'Authority' means Department of Telecommunications or its designated field units (Licensed Service Areas or LSAs).

2. 'Company' means an Indian Company, registered under the Indian Companies Act, 2013 or a Partnership Firm or an organization registered under Shops and Establishments Act.

3. 'LLP' means a Firm incorporated and registered under Limited Liability Partnership Act-2008 in India.

4. 'Other Service Provider' (OSP) is an Indian company, registered under the Indian Companies Act, 2013 or an LLP (Limited Liability Partnership) registered under LLP Act, 2008 or a partnership firm or an organization registered under Shops and Establishment Act providing voice based Business Process Outsourcing (BPO) services to their customers located world-wide including in India.

5. 'Voice based BPO services' means call centre services provided by the OSPs wherein the customers access the network of the OSP through PSTN/PLMN/ISDN.

6. 'OSP Centre' means the infrastructure of an OSP at a location in India.

7. 'Point of Presence' (POP) is a location where OSP places equipment like Private Automatic Branch Exchange (PABX), Interactive Voice Recording System (IVRS) etc., to act as an extension of its OSP Centre for collecting, converting, carrying and exchanging the telecom traffic related to its services.

8. 'Telecom Service Provider' (TSP)/ Telecom Licensee means an entity who has been granted a valid licence under Section-4 of the Indian Telegraph Act, 1885 to provide Telecom Service as per the License in a Licensed Service Area (LSA).

9. 'Telecom Resource' means Telecom facilities provided by TSPs and used by the OSPs including, but not limited to Public Switched Telecom Network (PSTN), Public Land Mobile Network (PLMN), Integrated Services Digital Network (ISDN), Leased Lines (NPLC/ IPLC), MPLS VPN, internet leased lines, Broadband connectivity (wireline/ wireless), BRA/PRI lines to carry traffic.

10. **Toll Bypass:** Toll bypass for the present guideline shall mean illegal carriage of voice traffic infringing upon the jurisdiction of authorised TSPs in the following ways:

    (a) Voice calls between public network (PSTN/ PLMN/ ISDN) in India and Foreign country by transiting it through their own network.

    (b) Voice calls between public network (PSTN/ PLMN/ ISDN) of one city and the other city in India by transiting it through their own network.

11.

PSTN – Public Switched Telephone Network	PLMN – Public Land Mobile Network
IPLC – International Private Leased Circuit	NPLC – National Private Leased Circuit
MPLS – Multi-Protocol Label Switching	VPN – Virtual Private Network
CUG – Closed User Group	ISDN – Integrated Services Digital Network
BRI/PRI – Basic/Primary Rate Interface	SD-WAN – Software Defined Wide Area Network

Chapter - 2   General Guidelines for OSPs

1.   Registration: The distinction between international OSPs and domestic OSPs has been removed and no registration will be required for OSP centres in India.

2.   Bank Guarantee: No Bank Guarantee whatsoever will be required for any facility or dispensation under these Guidelines.

3.   Special dispensations for OSPs:

3.1   For the OSPs the collection, conversion, carriage and exchange of the incoming PSTN/PLMN/ISDN traffic is permissible over any wide area networking technology like MPLS VPN/NPLC or SD-WAN over NPLC/MPLS VPN interconnecting the different OSP Centres.

3.2   The OSPs are allowed to carry the aggregated switched voice traffic (incoming/ outgoing) between their POP and their OSP centre in India over any wide area networking technology like IPLC/NPLC/MPLS VPN or SD-WAN (over IPLC/NPLC/MPLS VPN) and transiting it between other OSP centres in India over NPLC/MPLS VPN or SD-WAN (over NPLC/ MPLS VPN).

3.3   Interconnectivity of voice calls between two or more OSP Centres of the same Company or group of companies or unrelated companies is permitted for OSP operations.

3.4   Interconnection of Remote Agent to the OSP centre is permitted using any technology including broadband over wireline/wireless.

3.5   An OSP having multiple centres may obtain internet connection from authorised TSP at a centralised location anywhere in India. This internet can be accessed from other OSP centres of the same company or Group companies using NPLC/ MPLS VPN or SD-WAN (over NPLC/MPLS VPN).

4.   Entities that are not carrying out voice-based business process outsourcing services shall not be regulated under the OSP Guidelines.

5.   Inspection and reports: The OSPs have to self-regulate their operations in such a manner that there is no toll bypass and infringement on the jurisdiction of authorized TSPs. There is no requirement to submit any report/ information to the DOT HQ or its field units on normal routine basis. However, the OSPs have to maintain Call Data record (CDR), Usage Data Record (UDR) and System logs for all customer calls for the required period as mentioned in Chapter-5 "Security Conditions" and submit it to LEAs/ DOT, if requested. No audit/inspection on routine basis of the OSP centres shall be carried out by DoT.

Chapter -3: **Guidelines for sharing infrastructure, Use of Distributed Architecture of EPABX and Interconnection**

1. **Sharing the Infrastructure:** Sharing the Infrastructure including EPABX and PSTN/PLMN lines of OSP Centres for office use is permitted.

2. **Foreign EPABX:** EPABX at foreign location is allowed for the OSPs. However, the OSP will take all the necessary measures to comply with the requirements of relevant provisions of Indian laws. In addition, the OSP shall maintain a copy of CDR/ UDR and System logs at any of its OSP centres in India.

3. **Use of distributed architecture of EPABX for OSP centres across India:**

3.1 OSPs can have a distributed architecture of EPABX (main EPABX at a centralized location and media gateways at individual OSP centres) for their OSP centres across India, where the EPABX is owned by OSP.OSPs may place their self-owned EPABX in 3rd party data centres in India. OSPs can also take EPABX services from the TSPs.

3.2 OSP centres which do not make outgoing calls to the PSTN/PLMN in India may also use a centralised media gateway.

4. **Interconnection:**

4.1 There are no restrictions on data interconnectivity between any OSP centres of same company or group company or any unrelated company.

4.2 The voice interconnectivity for internal communication (i.e. within CUG) is permitted among the OSP centres for the same company or same group of companies.

Chapter-4   Work-From-Home (WFH)/ Work-From-Anywhere (WFA)

The concept of Work-From-Home is being encouraged under these guidelines and has been extended to allow Work-From-Anywhere in India. This facility of Remote Agent Position (i.e. Work-From- Home/Anywhere) is permitted with the following conditions:

1.   The agents at home/ anywhere in India shall be treated as Remote Agents of the OSP Centre.

2.   Interconnection of remote agents to the OSP centre is permitted using any technology including broadband over wireline /wireless.

3.   The remote agent of an OSP centre may connect directly with the centralised EPABX/ EPABX of the OSP/ EPABX of the customer.

4.   The OSP shall be responsible for any violation related to toll-bypass.

Chapter -5   **Security Conditions**

1.   The OSP shall not engage in the provision of any Telecom Services.

2.   For EPABX installed at locations different than the OSP Centre, the remote access of all CDRs, System log, configurations of EPABX and routing tables shall be made available on demand from Authority/ Law Enforcing Agencies from at least one of the OSP centres.

3.   OSP will take all the necessary measures to comply with the requirements of relevant provisions of Indian laws.

4.   On specific instances of infringements such as carriage of objectionable, obscene, unauthorized messages or communications infringing copyright, intellectual property etc. in any form on their networks, the OSP shall ensure that the carriage of such material on the networks is prevented immediately.

5.   The OSP shall extend support to the Authority in tracing any nuisance, obnoxious or malicious calls, messages or communications transported through its equipment and network.

6.   OSPs shall be required to preserve the CDRs for all the voice traffic carried using the EPABX. OSP shall maintain a copy of CDR and System logs at any of its OSP centres in India. The CDRs shall be segregated for each OSP centre/ media gateway. It shall be possible to view the CDR data along with details of the agent manning the position by remote login to CDR machine/ server. The time-stamp in the CDRs in the system(s) of the OSP shall be synchronized with the Indian Standard Time.

7.   The CDR/ UDR/ system logs etc. should contain all relevant information which is essential for the LEAs for tracking/forensic purpose. The CDR/ UDR shall consist of Calling Number, Called Number, Date, Start Time, End time/ duration, Identity of the Device used for making the call (MAC ID, Device signature etc.), User identity (login name) initiating the session, MGW identity/ Soft-switch ID and Trunk ID etc. System log shall consist of User/ login identity, date & time of login, date & time of logout, commands/ activities performed, response of command/ activities.

8.   For Remote Agents, the OSP shall ensure that the system logs are tamper-proof and the CDRs/ all logs of the activities carried out by the Remote Agent shall be maintained for one year.

9.   In all the above cases, CDRs / UDRs / System logs, etc. shall be maintained for a period of one year.