



Tax alert: TRAI Direction to Access Providers on Digital Consent Acquisition

5 June 2023

The Telecom Regulatory Authority of India (TRAI) has issued new directions¹ (“Direction”) to all Access Providers (“AP”) to curb spam calls/messages through Unsolicited Commercial Communication (“UCC”) under the Telecom Commercial Communication Customer Preference Regulations (“TCCCPR”), 2018².

The Direction comes as a result of TRAI’s observations on the following:

- (a) promotional messages are being sent without scrubbing (verification) of the consents of the customers registered under ‘service message’ category
- (b) there exists no uniform process for registering consent of subscribers and users
- (c) consents acquired by Principal Entities (“PE”) i.e., the various entities such as banks, other financial institutions, insurance companies, trading companies, business entities seeking to send promotional messages are being used by the AP without re-verification and updation as provided for in the regulations
- (d) Digital Consent Acquisition and Revocation facilities are yet to be developed.

In a nutshell



APs must develop and deploy the **Digital Consent Acquisition (“DCA”)** facility for creating a **unified platform** and process to register customers’ **consent digitally** across all service providers and PEs.



The DCA facility must have methods to **seek, maintain and revoke customer consent**. The consent data shall be shared on **Digital Ledger Platform (“DLT”)** for **scrubbing** by all APs.



The Direction also lays down in detail the **content and modalities of the consent seeking message** to be sent to users. A period of **2 months** has been given to APs to **comply** with the same.



Scroll down to read the detailed alert

¹ https://www.trai.gov.in/sites/default/files/Direction_02062023.pdf

² <https://tra.gov.in/sites/default/files/RegulationUcc19072018.pdf>

Summary

On noticing that several APs have not complied with the regulations under the TCCPR, 2018 including scrubbing/verification of promotional messages, TRAI has now directed all APs to:

- a. Ensure that no promotional messages are sent to subscribers without their consent
- b. Ensure that that no promotional messages are sent to subscribers under the 'Service Message' category
- c. Develop and deploy a DCA facility within 2 months from the date of the Direction
- d. Update the Code of Practice within 15 days from the date of the Direction
- e. Submit monthly progress report to the TRAI (in the format prescribed)

These Directions are issued under Section 13 r/w Section 11(1)(b)(i) and (v) of the TRAI Act, 1997³.

The DCA should be the primary facility via which subscribers/users can record their consent and revoke the same as under the regulations. APs must ensure that a consent seeking message is sent to all subscribers using the same short code '127'.

Further, APs must also develop a SMS/IVR/Online facility to register unwillingness of the customers to receive any consent seeking message initiated by any PE (example, banks). APs are also required to whitelist the telephone numbers of these customers to ensure that no consent seeking message shall be sent to them once they have already revoked their consent.

The consent seeking message sent under the short code shall adhere to the following:

- a. Clearly mention the scope and PE/Brand name willing to send the promotional message
- b. PEs must whitelist existing URLs/APKs/OTT links/ Call back number within one month after the development of DCA facility and after that only whitelisted URLs/APKs/OTT links/call back number shall be used in the consent seeking messages
- c. Consent acquisition confirmation message sent to customers shall also have information on how to revoke the consent
- d. If a customer has rejected or not responded to the consent seeking requests, no such messages to the customer shall be initiated by the same PE for next ninety days for the same consent. However, customers shall have the right to initiate the consent registration request on their own
- e. The PE initiated consent acquisition process shall begin only one month after the DCA facility is fully functional and advertised or 30 days must have passed since the implementation of the DCA, whichever is earlier. Until then, only customer-initiated consent acquisition shall be followed.

In the first phase, i.e., the first month after the commencement of the PE-initiated consent acquisition process, only PEs belonging to banking, insurance, finance, and trading-related sectors are onboarded to initiate the consent acquisition process. Remaining sectors will be onboarded in the following two months.

PEs shall be educated by the APs about the process of taking consent and its verification through APs and facilitate the on-boarding of PEs. The DCA shall be publicised as much as possible and after the implementation of this new facility, no other consent acquisition method shall be used.

APs are required to update their Code of Practice within fifteen days of the issue of this Direction (i.e., 17th June 2023), ensure compliance as per the stated timelines and submit a monthly progress report in the format as may be prescribed by TRAI.

³ https://traai.gov.in/sites/default/files/The_TRAI_Act_1997.pdf

Key Timelines

1	Development and Deployment of the Digital Consent Acquisition Facility	By 31 st July, 2023
2	User- initiated consent acquisition	To begin from 1 st August, 2023
3	Whitelisting of existing URLs/APKs/OTT/Links/call-back numbers	By 31 st August, 2023
4	PE-initiated consent acquisition	To start from 1 st September, 2023
5	Phase 1: On-boarding of PEs in the banking, finance, insurance, and trading sectors	By 30 th September, 2023
6	Phase 2: On-boarding of PEs belonging to remaining sectors	By 30 th November, 2023

Key Takeaways

The consent framework is aligned to the Digital Data Protection Bill, 2022⁴ and access providers will now need to develop a compliance mechanism to ensure that only those entities whose messages are verified, scrubbed or whitelisted, can send such messages to customers.

⁴ https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material and the information contained herein prepared by Deloitte Touche Tohmatsu India LLP (DTTI LLP) is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). This material contains information sourced from third party sites (external sites).

DTTI LLP is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such external sites. None of DTTI LLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering professional advice or services. This information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this material.

©2023 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited