MyOperator

Cloud Communications Platform (CPaaS)

Date: 19-April-2026

Ref: TRAI/TCCCPR-Amend-3/2026

To,

Sh. Deepak Sharma

Advisor (QoS-II)

Telecom Regulatory Authority of India

World Trade Centre, Tower-F (4th to 7th Floors),

Nauroji Nagar, New Delhi – 110029

Subject: Comments on the Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 — issued vide No. RG-25/(25)/2023-QoS dated 13 March 2026.

Dear Sir,

At the outset, we thank the Honourable Authority for issuing this consultation paper addressing emerging challenges in Unsolicited Commercial Communication, including AI/ML-based detection, regulation of Application-to-Person (A2P) voice calls, accountability of call management applications, and refinement of the consent framework. The proposed amendments represent a substantive evolution of the TCCCPR framework and respond to genuine regulatory gaps identified during implementation of the 2018 and amended 2025 regulations.

MyOperator is a Cloud Communications Platform (CPaaS) provider serving enterprises and a large base of micro, small and medium enterprises (MSMEs) for compliant, auditable, and multi-channel business communication. For the purpose of this submission, the term “Cloud Communications Platform” or “CPaaS” refers to a platform that provides programmable voice, messaging and related communication capabilities to businesses through APIs and managed infrastructure, while maintaining digital records of customer onboarding, consent, and call/message detail.

Our submission focuses on those proposed amendments where, based on operational experience of running a regulated communication platform, we believe targeted modifications will improve the implementability of the framework, reduce the risk of disproportionate impact on legitimate businesses, and strengthen the partnership between regulated platforms and the regulatory framework in addressing UCC.

We support the broad direction of the proposed amendments and offer the following specific comments in the format prescribed in the covering letter to the consultation paper. Sl. No. 1 sets out a foundational framework for platform safe harbour and primary liability of the Sender (Principal Entity), to which several subsequent rows cross-refer.

Sl. No.	Regulation No.	Sub-regulation / Item	Modification proposed to the draft amendment	Reasons / full justification for the proposed modification
1	**25 (new sub-regulation 7); cross-applies to 21A, 26, 27**	Platform Safe Harbour and Primary Liability of Sender (PE)	Insert new sub-regulation 25(7) as follows: "(7) Where a Sender (Principal Entity) makes commercial communications through a Registered Cloud Communications Platform (RCCP) or other registered intermediary that maintains (a) digital KYC of the Sender, (b) a documented consent-management framework requiring every Principal Entity to maintain digital consent records for each commercial communication, with contractual rights for the platform to obtain such records on demand for the purpose of investigation under regulation 25 or notification under regulation 21A, (c) Call Detail Records and Message Detail Records traceable to the relevant content template, and (d) an internal abuse-detection and customer-action mechanism, the following shall apply: (i) Primary penal action for any violation of these regulations shall lie against the Sender, not against the RCCP or registered intermediary; (ii) The RCCP shall, on receipt of a notification under regulation 21A or a complaint under regulation 25, produce the relevant KYC, CDR and MDR records, and procure from the Sender and produce the relevant consent records, to the OAP within three business days, and shall co-operate with the OAP's investigation; (iii) The RCCP shall have the right to suspend or terminate the services of the violating Sender on its platform pursuant to its terms of service, without such action constituting a violation of any regulation; the RCCP shall report such suspension or termination, with reasons, to the concerned OAP and to the Authority within fifteen days of the action; (iv) Financial disincentives, suspension of telecom resources, and blacklisting under these regulations shall apply to the violating Sender and not to the RCCP, save where the RCCP itself has failed to maintain the records prescribed under (a) to (d) above or has failed to co-operate with the investigation under sub-clause (ii); (v) Nothing in this sub-regulation shall affect the obligations of the OAP under	The TCCCPR ecosystem currently treats the platform through which commercial communications are delivered with the same enforcement intensity as the violating Sender itself. This creates two distinct problems. First, it disincentivises platforms from investing in KYC, consent and abuse-detection infrastructure, since investment in compliance does not reduce regulatory exposure. Second, it conflates the actor responsible for the harmful conduct (the PE) with the conduit through which the conduct occurred (the platform). The principle of regulatory action should follow the principle of evidence. Where the platform maintains digital records that establish the Sender's consent, KYC and communication history, and where the platform itself takes action against the violating Sender, the platform is acting as an enabler of enforcement, not as a participant in the violation. The proposed sub-regulation creates a clear and conditional safe harbour: platforms that meet defined compliance thresholds and co-operate with investigation are shielded from primary penal action, while platforms that fail to meet these thresholds remain fully exposed. This mirrors the structure of Section 79 of the Information Technology Act, 2000 — the foundational framework for intermediary liability in India — which the Authority has itself referenced in the proposed amendment to regulation 34A. The right to disconnect a violating Sender, expressly recognised under sub-clause (iii), resolves a current regulatory ambiguity: platforms that take internal action against violating clients today face the risk of those clients complaining to the Authority that they were "wrongly disconnected", putting the platform in the position of defending its own compliance action. Express recognition of this right — coupled with a fifteen-day reporting requirement to the OAP and the Authority — aligns the platform's commercial interest with the regulatory objective and ensures that violating Senders cannot simply move from one platform to another without regulatory visibility.

			regulations 21A, 25, 26 and 27, or the obligations of the RCCP under any registration framework prescribed by the Authority."	The sub-regulation does not weaken enforcement. It strengthens it by formally enrolling compliant platforms as enforcement partners while focusing penal action on the entity actually responsible for the violation. We recognise that the safe harbour framework proposed here is novel in the TCCCPR context and may benefit from phased introduction — for example, by first applying to a defined registered class of platforms with reporting and compliance milestones, before broader application. We are happy to engage with the Authority on the specific implementation pathway.
2	**2(ea)**	Definition of A2P call	Insert proviso after the proposed clause (ea): "Provided that voice calls where each individual call is triggered by a discrete human action of a specific identified human user, directed to a specific identified recipient as part of a one-to-one transactional or service interaction — including but not limited to click-to-call applications, agent-initiated dialler systems, and field-staff calling applications such as those used by delivery personnel, sales agents, and customer-service representatives — shall not be treated as A2P calls for the purpose of these regulations."	The proposed definition captures every call initiated through an application, which would inadvertently include legitimate one-to-one calls made by delivery personnel, field sales agents, and customer-service representatives using click-to-call functionality. Such calls have a specific identified human originator triggering each individual call to a specific identified recipient, and are not bulk in nature. Treating these as A2P would impose the entire compliance burden — pre-declaration under regulation 4, termination charge under regulation 35A, and the UCC enforcement framework — on legitimate person-to-person business interactions, with no corresponding consumer-protection benefit. The regulation should target what causes consumer harm: bulk autodialers, predictive dialers, robo-calls, and pre-recorded or artificial-voice broadcasts. The proposed proviso preserves the regulatory intent while protecting MSME and enterprise field operations from collateral capture.
3	**2(y)**	Definition of Explicit Consent	Support the proposed substituted clause. Insert additional proviso: "Provided that legacy consent registered under this clause shall be accompanied by an audit trail demonstrating the time, mode, and content of consent capture, and the Recipient shall be intimated of such registration within seven days, with a clear and accessible mechanism to revoke such consent."	The proposed recognition of legacy consents addresses a genuine business-continuity concern where lawfully obtained consents existed prior to the CRF framework. We support this change. Without safeguards, however, this provision risks being misused to retrospectively legitimise consents that were not validly obtained. A mandatory audit trail at the time of registration, combined with recipient intimation within seven days and a clear revocation mechanism, will preserve the consumer's right to be informed and to opt out, while

				permitting orderly migration of historical consents to the digital framework.
4	**2(bb)**	Definition of Relationship	In sub-clause (ii) of the substituted definition, replace the words "application regarding products or services made by or submitted by recipient to sender within the three months immediately preceding" with: "an explicit inquiry or application regarding products or services made by or submitted by the Recipient to the Sender through a verifiable channel within the seven days immediately preceding".	The proposed removal of the "inquiry" basis from the definition of Relationship will eliminate a legitimate ground on which businesses respond to customer-initiated enquiries. A customer who enquires about a property, an educational programme, an insurance product, or a service quote naturally expects a follow-up communication; treating this as UCC creates a regulatory paradox where the customer's own action triggers a compliance violation by the business. The Authority's concern about misuse of the inquiry exception is acknowledged. The proportionate response is to narrow the inquiry window to seven days — aligned with the seven-day Explicit Consent validity under the first proviso to sub-regulation 2(bh) — and to require the inquiry to be made through a verifiable channel; not to remove the inquiry basis entirely. This preserves legitimate customer-initiated business interactions while preventing extended exploitation of the inquiry exception.
5	**3(1)**	Proviso — Sender Classification (RCCP definition)	Support the proposed proviso. Additionally insert second proviso: "Provided further that for the purpose of classification under the preceding proviso, the Authority shall recognise, among other classes, senders served through Registered Cloud Communications Platforms (RCCPs) — being platforms that provide programmable voice and messaging capabilities to businesses through APIs and managed infrastructure — who maintain (i) digital KYC of every Principal Entity onboarded, (ii) a documented consent-management framework requiring every Principal Entity to maintain digital consent records for each commercial communication, with contractual rights for the platform to obtain such records on demand for the purpose of investigation under regulation 25 or notification under regulation 21A, (iii) traceability linking every Call Detail Record and Message Detail Record with the relevant content template and consent, and (iv) internal abuse-detection mechanisms based on call pickup rate, call duration, message delivery patterns, complaint rate and volume patterns across	The enabling provision for sender classification is welcome and addresses the current framework's "one-size-fits-all" limitation. The sender ecosystem includes large enterprises, MSMEs served via Cloud Communications Platforms (CPaaS), government bodies, BFSI entities, and individual senders — each with materially different risk profiles. Cloud Communications Platforms occupy a distinct position in this ecosystem: they aggregate MSME and enterprise communication, maintain digital KYC and consent infrastructure with a level of traceability not available through unstructured calling channels, and are technically capable of self-policing through real-time analytics on call and message patterns. Recognising RCCPs as a defined class — with corresponding obligations and proportionate enforcement — converts compliant platforms from a regulatory blind spot into an active partner in spam control while protecting MSMEs whose business depends on legitimate digital communication. This definitional row should be read together with the proposed safe harbour

			voice and messaging channels; and the Authority may prescribe differentiated registration, declaration, complaint-threshold and enforcement criteria for such class of senders."	framework under regulation 25(7) at Sl. No. 1 above. The RCCP definition establishes who qualifies; the safe harbour establishes the consequential treatment. Without an explicit reference to this class within the classification framework, the differentiated treatment enabled by the proposed proviso is likely to benefit only banks and government entities, leaving the broader MSME economy exposed to enforcement designed for bulk telemarketers.
6	**4**	Intimation regarding A2P calls	After the substituted regulation, insert proviso: "Provided further that in respect of senders served through a Registered Cloud Communications Platform (RCCP), the RCCP may submit a single annual declaration to the Originating Access Provider on behalf of all such senders, identifying the categories of A2P calling in use, with updates submitted within seven days of any material change in such categories."	A per-sender or per-campaign pre-declaration model is operationally unworkable at the scale at which Cloud Communications Platforms onboard MSMEs (frequently several thousand customers per platform). A platform-level annual declaration, with update obligations on material change, achieves the same regulatory visibility — the OAP knows the categories of A2P calling supported by the platform and can take action accordingly — without imposing a per-customer declaration burden. Without this proviso, the declaration requirement will either (a) push customers away from regulated platforms back to SIM-based calling, defeating the digitisation objective, or (b) generate volumes of paperwork the OAP cannot meaningfully process. The proviso preserves the deterrent effect of the declaration requirement (failure to declare = UCC) while making compliance practically achievable.
7	**21A**	AI/ML-based UCC_Detect cascade	After clause (b), insert new clause (b-1): "(b-1) The notification under clause (b) shall provide the sender with a representation window of five business days from the date of receipt of such notification, during which the sender, or the Cloud Communications Platform (CPaaS) provider through which the sender is served, may submit consent records, KYC documents, and contextual justification to the OAP. The OAP shall examine such representation within three business days of receipt and, where the records are found prima facie satisfactory, the flagged CLI shall be delisted from the cascade for the purposes of clauses (c) to (e); subsequent flagging of the same sender within thirty days of such delisting shall, however, proceed without further representation	The proposed cascade triggers cross-network identification of all telecom resources of a sender within one business day of an AI flag, and triggers full enforcement at five flagged CLIs over ten days — all without any opportunity for the sender to provide consent or contextual justification. The clause (b) notification is informational only. AI/ML systems, however well trained, produce false positives, particularly in sectors where call patterns naturally resemble spam patterns: delivery and logistics, e-commerce confirmations, education enquiry follow-ups, customer-support callbacks, real-estate enquiry response, travel and hospitality confirmations, and field-sales operations. Permitting the cascade to run end-to-end

			window." Additionally, the Authority should consider directing Access Providers to maintain transparency with OSPs and Telemarketers regarding the specific behavioural parameters or signals on which a call or message has been flagged as suspected UCC, to enable platforms to investigate efficiently and to refine their internal abuse-detection mechanisms.	based purely on AI flags plus the 5-CLI threshold, with the first opportunity for representation occurring only after physical KYC verification has been initiated, creates disproportionate operational and reputational risk for legitimate businesses. A five-business-day representation window between AI flagging and cascade progression — with a one-time-per-thirty-days limit to prevent abuse — preserves the deterrent value of the AI system, ensures that only genuine UCC senders enter the enforcement ladder, and protects legitimate businesses from cascade-based service disruption. This row should be read with the safe harbour framework proposed at Sl. No. 1: where the sender is served through an RCCP, the platform is operationally best placed to make the representation on the customer's behalf within the timeline, since the platform holds the relevant KYC and consent records.
8	**22(1)(a)**	Misuse of Headers / Content Templates — corrective action timelines	In sub-clause (ii):• Item 1: substitute "within 24 hours" with "within 48 hours".• Item 2: substitute "within 2 business days" with "within 5 business days".• Item 3: substitute "within next 5 business days" with "within next 10 business days".• Item 4(a): retain "within 10 business days".	The graduated response in the proposed amendment — suspending only misused headers and templates initially while allowing the sender to take corrective action — is a welcome and proportionate change. However, the timelines proposed are operationally tight, particularly for senders served through Cloud Communications Platforms who may have hundreds of headers and templates. A 24-hour credential reset across all access providers and telemarketers is achievable only through fully-automated infrastructure that not all senders possess. A 2-business-day window for filing a formal law enforcement complaint is unrealistic, particularly where the cause of misuse requires investigation before a meaningful complaint can be filed. The modest extensions proposed retain the urgency of the response while making compliance achievable for legitimate senders without forcing wholesale traffic suspension.
9	**23(1)(c)**	Appellate Authority	Support the proposed insertion. Additionally insert at the end of the proposed clause (c): "Provided that a Sender or Telemarketer against whom action has been taken under regulation 25 may also prefer an appeal under this clause within fifteen days of the receipt of such action, in addition to the	The proposed Appellate Authority mechanism is a positive customer-protection measure. The same mechanism, however, should be made available to senders and telemarketers who are subjected to action by the OAP — currently their only recourse is "representation" under regulation 29, which

			representation provided under regulation 29.”	is a less structured process and requires payment of restoration charges. Extending the appellate route to senders aligns with natural-justice principles, reduces the volume of frivolous representations to the Authority under regulation 29, and provides a faster internal-resolution mechanism for sender disputes. The same designated Appellate Authority can handle both customer and sender appeals.
10	**25(4)(a)**	Notification of complaint to Sender — inclusion of CPaaS / Aggregator	After the words “notify the receipt of the complaint to the Sender immediately with such details which help the Sender to start the investigation immediately”, insert: “; and where such Sender is served through a Registered Cloud Communications Platform (RCCP) or other registered intermediary, the OAP shall simultaneously notify the RCCP or registered intermediary, providing (i) the calling number, (ii) the date and time of the complained communication, (iii) the complaint category, and (iv) the reason for the complaint, but not the identity or contact details of the complainant. The RCCP or registered intermediary shall use such notification solely for the purpose of investigation and action under its terms of service against the violating Sender, and shall not use such information for any other purpose.”	Cloud Communications Platforms typically serve a large number of Principal Entities, frequently several thousand per platform. When a complaint is generated against a calling number routed through such a platform, the platform itself is operationally best placed to identify the specific PE responsible, examine the consent and call records, and take action under its terms of service against the violating Sender. Under the current framework, this notification flow is between the OAP and the Sender alone. The platform — which holds the KYC, consent and CDR records and has the operational ability to disable the violating PE’s access — is not in the notification chain. This creates a delay between the complaint being received and the platform being able to act, during which the violating PE may continue to make further unsolicited communications. The proposed amendment introduces the platform into the notification chain with clear privacy safeguards: only the calling number, timestamp, complaint category and reason are shared, never the complainant’s identity or contact details. The amendment also restricts the platform’s use of such information to investigation and action against the violating Sender. This amendment, read with the safe harbour framework at Sl. No. 1, completes the platform’s role as an enforcement partner: the platform receives the signal, takes action under its terms of service, and reports the action back to the OAP and the Authority within fifteen days.
11	**25(4)(d)**	Second proviso — Wrong template categorisation: 1-	In the proposed second proviso, substitute the words “if five content templates of such sender are blacklisted for registration under wrong category, the OAP shall suspend the services of the sender, for one month” with:	The proposed 1-month sender suspension upon blacklisting of 5 templates is disproportionate where the underlying cause is a single classification methodology error replicated across multiple similar templates. A sender

		month sender suspension	"if five content templates of such sender are blacklisted for registration under wrong category within a period of ninety days, and such templates relate to two or more distinct categorisation errors, the OAP shall suspend the services of the sender for one month".	legitimately using transactional templates may have multiple templates flagged for the same reason — for example, a single sentence that the OAP reads as promotional appearing across multiple templates. Suspending all services in such a case causes customer harm without achieving deterrence beyond what template-level blacklisting already provides. The modifications proposed: (a) a 90-day window so historical errors do not accumulate indefinitely, and (b) a "two or more distinct categorisation errors" requirement so the suspension targets repeat patterns rather than single errors replicated across templates — make the consequence proportionate to the underlying conduct while preserving the deterrent against systematic misclassification.
12	**25(4)(f)**	Second proviso — sender classification (Registered Senders)	Support the proposed proviso. Cross-reference: as detailed against Sl. Nos. 1 and 5 above, the classification framework should expressly recognise senders served through Registered Cloud Communications Platforms (RCCPs) as a defined class with proportionate enforcement criteria, operating under the safe harbour framework proposed at Sl. No. 1.	Recognising RCCP-served senders as a defined sender class — with proportionate complaint thresholds and enforcement criteria reflecting the platform's KYC, consent and self-policing infrastructure — is essential to give effect to this proviso for the broader MSME economy. Without such recognition, this proviso will likely be applied only to large enterprises, leaving CPaaS-served MSMEs subject to enforcement designed for bulk telemarketers.
13	**25(5)(d)**	Second proviso — sender classification (UTM-related complaints)	Support the proposed proviso. Cross-reference: as detailed against Sl. Nos. 1 and 5 above, the classification framework should apply uniformly across registered-sender enforcement and UTM-related enforcement, in conjunction with the safe harbour framework proposed at Sl. No. 1.	RCCP-served senders should be treated according to their classification under regulation 3(1) rather than defaulting to UTM-grade enforcement merely because the regulation's structure separates registered and unregistered telemarketer flows. Uniform application of the classification framework prevents arbitrage between the two enforcement paths.
14	**25(5)(d)(i)**	Lowered complaint threshold (3 with AI corroboration)	In the proposed clause, after the words "the OAP shall immediately suspend the outgoing services of the telecom resources of the Sender which were utilized for sending UCC and simultaneously initiate an investigation as provided for in the sub-regulation (6)", insert proviso: "Provided that, before such suspension, the OAP shall serve a notice to the sender and the Cloud Communications Platform (CPaaS) provider (where applicable) and provide a representation window of three	Reducing the complaint threshold from 5 to 3 unique recipients — combined with AI corroboration as the trigger — significantly increases the risk of suspension based on incorrect AI flagging plus a small number of complaints, some of which may themselves be erroneous (e.g., recipient confusion between legitimate and unwanted communication, or recipient remorse after opting in). For truly unregistered telemarketers without digital KYC and consent records,

			business days during which consent records, KYC documents, and contextual justification may be submitted; suspension shall proceed only where the sender fails to respond, or the response does not establish prima facie compliance, within such window. Where prima facie compliance is established, the matter shall be examined under the regular investigation process under sub-regulation (6) without immediate suspension.”	pre-suspension justification will not be possible; in those cases the suspension will proceed as currently drafted. However, where a sender is served through a Cloud Communications Platform with KYC and consent infrastructure, immediate suspension based on a 3-complaint AI-corroborated threshold is disproportionate. A short pre-suspension representation window of three business days, read together with the safe harbour framework at Sl. No. 1, maintains regulatory deterrence while preventing suspension of legitimate businesses. AI systems improve through feedback, and the representation mechanism also generates the corrective signal the AI system needs to refine its detection over time.
15	**26(4A)**	TRAI CDR audit power	Support the proposed insertion. Additionally insert proviso: “Provided that CDRs requested under this sub-regulation shall be limited to the period necessary for analysis of the relevant complaints, shall not include the content of communications, and shall be subject to confidentiality safeguards. The Authority shall publish an annual summary of audit findings and corrective actions in aggregated form.”	The CDR audit mechanism is necessary in light of the data showing 11.4% of complaints closed on “CDR mismatch” grounds during August–November 2025. We support the audit power. Express limitations on scope (period necessary for analysis), exclusion of communication content, and confidentiality safeguards — combined with annual aggregated publication of findings — will give the audit process credibility, build public confidence in complaint handling, and protect the privacy interests of subscribers whose CDRs may be examined.
16	**27(1)(a)**	Financial disincentive for wrong header / template registration	Support the proposed amendment regarding the financial disincentive of one thousand rupees per valid complaint on the registering Access Provider for wrong header registration, and on both the OAP and the registering Access Provider for wrong content-template categorisation. No modification proposed.	The financial-disincentive structure correctly aligns liability with the entity that performed the registration or processed the traffic under the wrong category. Read with the safe harbour framework at Sl. No. 1, this disincentive should not extend to the platform through which the sender is served, where the platform has discharged its prescribed obligations.
17	**29**	Proviso — partial restoration charges	No modification proposed.	The proposed minimum restoration charge of half the full restoration cost balances the deterrent effect with the legitimate need for partial restoration in genuine cases. We have no comment on this provision.
18	**34A**	Call management applications	Strongly support the proposed substituted regulation in its entirety — sub-regulations (1) to (4). No modification proposed.	Call management applications and third-party dialler apps that blanket-tag, block or filter communications from designated commercial number series (140xx, 1600xx) currently undermine the regulatory framework. The 140 and 1600 series exist precisely so that consumers can identify

				the nature of incoming commercial communications and so that legitimate businesses can communicate transparently. When a third-party app blocks all 140-series calls without distinguishing between fraudulent senders and registered senders complying with regulation, the consumer loses access to legitimate transactional communications — delivery confirmations, OTPs delivered via call, appointment reminders, banking alerts, government notifications — and businesses lose the ability to reach customers who have explicitly opted in. The proposed mechanism — non-discrimination on designated series, mandatory reporting of user spam reports to DLT, loss of intermediary safe harbour for non-compliance — correctly aligns app behaviour with the regulatory framework and is strongly supported.
19	**35A**	Termination charge for A2P calls	After clause (v), insert clause (vi) and a proviso: "(vi) any A2P calls originated by senders served through a Registered Cloud Communications Platform (RCCP) recognised by the Authority under the classification framework, where such senders maintain digital KYC and consent records as prescribed by the Authority: Provided that the Authority may, by notification, prescribe a graded termination-charge structure for A2P calls under this clause, based on the sender's classification, complaint history and such other parameters as the Authority may specify."	A flat ₹0.05 per minute termination charge on A2P calls — without exemption for senders with verifiable digital KYC and consent infrastructure — will be passed through to MSME and enterprise customers, materially increasing their cost of legitimate business communication. Compliance with the regulations (KYC, consent registration, template approval) already imposes substantial cost on businesses served through Cloud Communications Platforms. The Authority's stated rationale for the termination charge is to deter bulk callers exploiting cheaper P2P routes. This rationale is already addressed by the proposed exemption under clause (v) for the 140xx and 1600xx series. Extending the exemption to senders served through RCCPs — with the option for the Authority to apply graded charges where warranted — preserves the deterrent against unverified bulk callers while protecting the economics of the legitimate communication infrastructure that is central to MSME digitisation. Without such exemption, the termination charge will operate as a blunt cost levied uniformly on compliant and non-compliant senders alike, with the burden ultimately borne by MSMEs who depend on Cloud Communications Platforms for routine transactional and service calls (OTPs, appointment confirmations, delivery

				notifications, customer support callbacks).
20	**Schedule I, item 4(3)(m)**	Secondary validation by every OAP	In sub-clause (iii), insert proviso: "Provided that where an Access Provider undertaking secondary validation arrives at a categorisation different from that approved by the registering Access Provider, the matter shall be referred to a centralised dispute-resolution mechanism established jointly by all Access Providers under the Common Code of Practice within seven business days, and traffic from the sender shall not be suspended on grounds of categorisation pending resolution."	The introduction of secondary validation by every OAP, combined with independent liability for each OAP's categorisation decision, creates a real risk of inconsistent decisions across access providers — a content template approved as "Service" by one OAP may be categorised as "Promotional" by another. This places the sender in an impossible compliance position and may lead to traffic suspension by some OAPs while the same template is permitted by others. A centralised dispute-resolution mechanism, with a defined timeline and a no-suspension-pending-resolution rule, is necessary to make secondary validation operationally workable for senders without compromising the regulatory objective of accurate template categorisation.
21	**Schedule II, item 1**	Service-type CC merged with Promotional CC	Support the proposed amendment treating service-type CC based on explicit consent as promotional CC for blocking purposes, and exempting service-type CC from time-band and day-type restrictions alongside transactional CC. No modification proposed.	The proposed amendment correctly recognises that service-type CC linked to ongoing customer transactions (balance alerts, flight delay information, product updates) requires the same time-flexibility as transactional CC, while service-type CC obtained through explicit consent should be treated as promotional for opt-out purposes. This dual treatment appropriately distinguishes between service communications that are operationally necessary and those that are consent-based extensions of the customer relationship. We have no modification to propose.
22	**2(ea), 4, 35A and the regulation generally**	Treatment of AI agent communications under the A2P framework	We propose the following framework for the treatment of communications involving Artificial Intelligence (AI) agents, to be incorporated through suitable amendments to regulations 2(ea), 4 and 35A, and through a Direction or Schedule clarifying the position: (i) Inbound calls answered by an AI agent — where the call originates from a Recipient (subscriber) and is answered by an AI agent operated by the called business — shall be expressly excluded from the definition of A2P calls under regulation 2(ea), as the call origination is not by an application but by the subscriber. (ii) Outbound voice calls made by an AI agent in response to, or in performance of, a service or transactional interaction with	AI agents are increasingly being deployed by businesses to deliver service and transactional communications at scale — appointment confirmations, OTP voice delivery, customer-support callbacks, and post-transaction feedback. The current draft amendment, which captures every "application-initiated" call without distinguishing between consent-based AI service interactions and unsolicited AI bulk campaigns, will impose the entire A2P compliance burden on legitimate consent-based AI use cases. We expressly accept and concede that AI agents making outbound bulk calls without consent are a legitimate target of the A2P framework, and that any regulatory carve-out should not extend to such use cases.

			explicit consent of the Recipient (including but not limited to AI-driven appointment confirmations, AI-driven OTP voice delivery, AI-driven feedback calls following a transaction, and AI-driven customer-support callbacks) shall be treated under the existing service or transactional category, as applicable, and shall not be escalated to the bulk-A2P category solely on account of the use of AI voice technology. (iii) Outbound voice calls made by an AI agent without explicit consent of the Recipient shall continue to fall within the A2P framework and shall be subject to the regulations applicable to A2P calls in their entirety. (iv) The Authority is requested to develop, in consultation with industry, a dedicated regulatory framework for AI-driven communications that addresses the distinct technical and consent-architecture characteristics of AI agents, rather than catching such communications reactively under the existing definitions of autodialler, robo-call, and pre-recorded or artificial-voice technologies.	The principled position is that the regulatory treatment should follow the consent and use-case basis of the call, not the technology by which the voice is generated. Inbound calls answered by AI agents are technically already outside the A2P definition (which is by construction outbound from application to person), but express exclusion will remove ambiguity and allow businesses to deploy AI-based customer-service answering without regulatory uncertainty. A dedicated AI Communications regulatory framework, developed in consultation with industry, will allow the Authority to address the genuinely novel consent and accountability questions raised by AI — including identification of the AI to the Recipient, transparency around the AI's capabilities, and the boundary between AI-assisted and fully-automated interactions — in a structured manner, rather than through the indirect application of definitions written for an earlier generation of technology.
23	**26 / Schedule IV; cross-references to DPDPA, 2023**	Regulatory clarity on DPDPA-permitted data analysis for UCC pattern detection	We respectfully request the Authority to: (i) Issue a clarification, by way of a Direction or an Explanatory Note to these regulations, that the analysis by Access Providers, registered Telemarketers, and Registered Cloud Communications Platforms (RCCPs) of Call Detail Records, Message Detail Records, call patterns, message patterns, and complaint data — for the purpose of detection, prevention and reporting of Unsolicited Commercial Communications under these regulations — constitutes processing for compliance with law within the meaning of section 7(b) of the Digital Personal Data Protection Act, 2023, and does not require separate consent of the Data Principal under that Act, subject to the safeguards prescribed below. (ii) Prescribe, in consultation with the Ministry of Electronics and Information Technology, the safeguards applicable to such processing, which should include, at a minimum: (a) limitation of analysis to the purposes set out in (i) above, (b) prohibition on individual subscriber profiling for purposes other than UCC detection, (c) data-retention limits aligned with the three-year history requirement under regulation	The proposed amendment relies extensively on AI/ML-based detection of UCC at the Access Provider level (regulation 21A and Schedule IV). The same intelligence — pattern analysis of CDRs, message patterns, complaint data, pickup rates, call durations, abandoned-call rates — can be deployed by registered Telemarketers and Cloud Communications Platforms at the platform level, materially improving early detection of UCC at the source rather than at the network edge. However, in the absence of explicit regulatory clarity, platforms are uncertain whether such pattern analysis is permitted under the Digital Personal Data Protection Act, 2023. Section 7 of the DPDPA permits processing without consent for compliance with law (sub-clause (b)) and for fair and reasonable purposes (sub-clause (i) and related provisions), but the boundary of these exceptions in the context of platform-level UCC detection has not been authoritatively settled. This uncertainty has two adverse consequences: (a) platforms invest less than they otherwise would in UCC detection capabilities, leaving the burden disproportionately on Access Providers;

			24(3), (d) prohibition on the use of analysis outputs for commercial purposes unrelated to UCC detection, and (e) annual reporting of the categories of data analysed and the actions taken on the basis of such analysis. (iii) Engage with the Ministry of Electronics and Information Technology to confirm inter-regulator alignment on the position set out in (i) and (ii) above, and publish the agreed position for the benefit of all stakeholders in the UCC detection ecosystem.	and (b) UCC senders move their activity to platforms with weaker detection capabilities, undermining the overall regulatory objective. The proposed clarification, with the safeguards prescribed at sub-clause (ii), resolves the uncertainty without compromising data-protection principles. It also formally enrols platforms as co-detectors of UCC, complementing the Access Provider-level AI/ML systems contemplated under regulation 21A. The request for inter-regulator alignment with the Ministry of Electronics and Information Technology recognises that DPDPA interpretation is the domain of the Ministry, and that lasting clarity requires alignment between the two regulatory frameworks. This row should be read with the safe harbour framework at Sl. No. 1: a platform that conducts compliant pattern analysis to detect UCC at source is acting as an enforcement partner; the legal certainty proposed here enables that role to be discharged at scale.

We remain committed to supporting the Authority in building a compliant, efficient, and innovation-friendly communication ecosystem, and would be happy to provide any further clarification or supporting data the Authority may require.

Respectfully submitted,

Avneet Bhargava
Vice President – Operations & Compliance
MyOperator

[Email: resource@myoperator.co | Phone: 8882802803]