Dear Ofcom team,

I am submitting this response to the proposed Wireless Telegraphy (Direct to Device Satellite Communications) (Exemption) (Amendment) Regulations 2026.

The current drafting accurately reflects the intended extension of permitted frequencies and associated technical parameters for Direct-to-Device services, as outlined in the consultation document.

However, the proposal remains primarily focused on spectrum access and transmission parameters, without addressing the system-level implications of integrating satellite-based communication into mass-market mobile networks.

In particular, the introduction of a satellite communication layer raises important considerations regarding:

- the integrity and validation of communication identity (including CLI);
- the traceability of communications across hybrid terrestrial–satellite routes;
- the allocation of operational responsibility between mobile network operators and satellite infrastructure providers.

These aspects are not explicitly addressed in the proposed Regulations, which may create gaps in scenarios involving misuse, spoofing or cross-network routing complexity.

Given that Direct-to-Device services introduce a structurally different communication model, I respectfully suggest that these elements be considered alongside the technical framework, to ensure consistency, accountability and resilience.

For clarity and practical relevance, I have included a short Annex with structured regulatory considerations that may support further analysis.

Kind regards,
Claudiu Viorel Raica

NGO '' CETATEA VIITORULUI '' Romania

ANNEX – STRUCTURED REGULATORY CONSIDERATIONS

🔴 1. Identity Integrity

A1 – Communication Identity Validation
Communication identity (including CLI) should remain verifiable across the full transmission chain, including satellite segments.

A2 – Prevention of Unverified Identity Transmission
Communications carrying non-verifiable identity should be subject to restriction or filtering mechanisms.

🔴 2. Traceability

A3 – End-to-End Traceability
Communications should remain traceable to a verifiable origin, regardless of the number of network layers involved.

A4 – Logging Responsibility
Clear responsibility should be assigned for maintaining communication logs across terrestrial and satellite components.

🔴 3. Operational Responsibility

A5 – Responsibility Allocation
Operational responsibility should be clearly defined between mobile network operators and satellite infrastructure providers.

A6 – Incident Response Coordination
Procedures should exist for coordinated response in cases of misuse, fraud or abnormal communication patterns.

🔴 4. Hybrid Network Risks

A7 – Anomaly Detection
Baseline mechanisms should be implemented to detect abnormal routing or usage patterns specific to hybrid networks.

A8 – Cross-System Consistency
Rules applicable in terrestrial networks should remain enforceable in satellite-integrated communication paths.

🔴 5. Principle of Balanced Control

A9 – Proportionality
Any control mechanisms should be proportionate and limited to preventing misuse, without affecting legitimate communications.

A10 – Distributed Responsibility
Control over communication integrity should not be concentrated in a single entity, but distributed with clear accountability.

ANNEX 2 – Proposed Amendments to D2D Exemption Regulations

(9) The use of Direct-to-Device satellite services shall be subject to the condition that the origin of any communication is capable of being verified by appropriate technical means.

(10) For the purposes of paragraph (9), a communication shall be considered verified where the identity information associated with the communication is authenticated and has not been altered in transmission.

(11) Where the origin of a communication cannot be verified in accordance with paragraph (9), such communication shall be treated as unverified and may be subject to restriction, limitation or blocking.

(12) Providers shall take all reasonable steps to ensure the integrity of Calling Line Identification (CLI) information transmitted via Direct-to-Device services.

(13) The transmission of CLI information which is misleading, invalid or not capable of verification is prohibited.

(14) Providers shall ensure that communications transmitted via Direct-to-Device services are traceable to a verifiable origin across all relevant network components, including satellite and terrestrial elements.

(15) Providers shall maintain appropriate records and logs sufficient to enable post-event analysis and investigation of communications where required.

(16) Mobile network operators and satellite service providers shall ensure that responsibilities in respect of communication integrity, traceability and service operation are clearly defined and effectively coordinated.

(17) Providers shall implement proportionate and effective measures to detect and mitigate abnormal or suspicious patterns of communication associated with Direct-to-Device services.

(18) Any measures taken under paragraphs (11) and (17) shall be proportionate, targeted and limited to what is necessary to prevent misuse, and shall not unduly interfere with lawful communications.

Interpretation

“verified communication” means a communication in respect of which the origin and associated identity information have been authenticated using appropriate technical mechanisms;

“unverified communication” means a communication in respect of which the origin cannot be authenticated or validated;

“Direct-to-Device services” means satellite-based communication services enabling direct connectivity between user equipment and satellite infrastructure without reliance on terrestrial base stations.

Explanatory Note

These amendments introduce provisions relating to the integrity of communication identity, traceability and operational accountability in the context of Direct-to-Device satellite services. They aim to ensure that the introduction of satellite-based communication layers does

not reduce the ability to verify communication origin, prevent misuse or maintain effective regulatory oversight.