GSMA

Satellite Regulatory Playbook

Implications of LEO constellations on regulatory frameworks

GSMA

Access Partnership

About GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com.

Follow us on LinkedIn: GSMA – Policy and Regulation

About Access Partnership

Access Partnership is a global advisory firm specialising in technology, telecommunications and digital policy. The firm supports clients in navigating complex regulatory and policy environments to enable market entry, expansion and compliance across multiple jurisdictions. Working at the intersection of law, policy and commercial strategy, Access Partnership advises on licensing, spectrum access and market access frameworks, while supporting engagement with governments and regulatory authorities worldwide. Its work spans telecommunications, satellite communications, digital infrastructure and emerging technologies, helping to create enabling regulatory environments for innovation and investment.

Access Partnership has been the leading advisor on satellite regulatory policy, advising regulators, satellite operators and service providers on market access, spectrum coordination and evolving regulatory frameworks across global markets.

Through its global presence and cross-sector expertise, Access Partnership delivers practical, policy-grounded solutions that support the deployment and operation of communications and digital services in line with national requirements and international best practices.

In collaboration with Access Partnership, this playbook has been developed by the GSMA Policy and Regulation team.

For further information, please contact:
Michaela Angonius, Head of Policy and Regulation, and Nitin Sapra, Director, Regulatory Advocacy, via publicpolicy@gsma.com.

Published: June 2026

About the Playbook

The accelerated deployment of satellite constellations, driven by advances in Low Earth Orbit (LEO) technology, is enabling a new generation of connectivity services. Increasingly, these systems are capable of providing direct-to-user connectivity — sometimes independent of terrestrial operator partnerships.

As these services evolve, an important policy question arises: are existing regulatory frameworks keeping pace with these developments? Discussions with regulators suggest widespread recognition of the need to update current approaches. This presents a timely opportunity to reassess and modernise policy frameworks to accommodate emerging direct-to-user satellite services. In this context, the GSMA launched a global policy position paper in March 2026.

The GSMA is committed to helping policymakers and regulators navigate this transition, advancing forward-looking frameworks that protect core societal needs, promote fair market access, strengthen consumer trust, and enable sustainable investment. This Satellite Regulatory Playbook has been developed in collaboration with Access Partnership, our knowledge partner.

The Satellite Regulatory Playbook is a globally relevant, practical guide for regulators. It provides a structured framework to help those working to modernise existing regulatory regimes or to develop new ones suited to the rapid evolution of LEO satellite services. It identifies core regulatory dimensions and policy considerations relevant to satellite broadband and direct-to-device services, grounded in emerging international best practices.

Recognising that regulatory frameworks differ across jurisdictions in their maturity, structure and policy priorities, this Playbook does not advocate a one-size-fits-all approach. Instead, it enables regulators to draw on relevant elements and tailor them to their domestic market needs, ensuring flexibility while promoting consistency in high-level regulatory outcomes.

The Playbook introduces the following regulatory themes applicable to emerging satellite services delivered via LEO constellations, including satellite broadband and Direct-to-Device (D2D) services, without partnerships with mobile operators:

1. Local establishment rules

2. National security

3. Consumer protection and operational measures

4. Infrastructure and facility requirements

5. End user terminal deployment

6. Fiscal considerations

7. Emergency services and public safety

8. Enforcement

Contents

Background 6

Satellite services: segments, market definitions and architecture 8

Space versus ground regulation 14

Alignment with GSMA principles 17

Satellite regulatory framework 18
- Regulatory parity 19
- Scope and approach 19

Regulatory pillars 20
- Local establishment rules 22
- National security 24
- Consumer protection and operational measures 26
- Infrastructure and facility requirements 28
- End user terminal deployment 30
- Fiscal considerations 32
- Emergency services and public safety 34
- Enforcement 36

Annex 38

Background

Satellite communications services have existed for several decades. Historically, many satellite operators (SOs) pursued wholesale business models using geostationary orbit (GSO) satellites. These operators sold satellite capacity to customers that owned and operated ground infrastructure and, in turn, provided connectivity services to end users. Satellite networks were primarily used for broadcasting, terrestrial network backhaul, aviation connectivity and private network interconnection, with end users typically accessing services through intermediary providers rather than via direct contractual relationships with satellite operators.

Under this traditional model, GSO SOs were generally subjected to frameworks such as international coordination through the International Telecommunication Union (ITU), registration and authorisation of space objects under United Nation space law instruments, and national landing rights regimes. However, because they traditionally did not operate terrestrial access networks or provide retail connectivity services to end users, they were generally not required to obtain telecommunications service licences or comply with end-user service obligations imposed upon telecommunications providers.

From the late 1990s onwards, some satellite companies did provide voice telephony or narrowband connectivity services. However, these services primarily targeted niche markets — such as maritime safety, aeronautical communications, or connectivity for small user bases in remote and underserved regions — and were typically delivered through local resellers. Due to their limited scope and market penetration, these operations were often subject to relatively light regulatory scrutiny and were frequently addressed through specialised regulatory regimes such as the GMPCS[1] regulatory framework.

From the 2010s, and particularly since 2019, this landscape has evolved significantly. GSO SOs have increasingly transitioned from wholesale capacity models to vertically integrated 'managed services' approaches while low earth orbit (LEO) satellite constellations have become more ubiquitous. Under these models, operators deploy and control ground infrastructure, undertake in-house manufacturing and provide managed connectivity services directly to enterprise customers, resellers or even end users.

This structural shift, from wholesale satellite capacity provision to a diverse range of vertically integrated, managed service and direct-to-device models, has materially altered the regulatory landscape. Today, satellite connectivity is delivered through an increasingly varied set of commercial arrangements: some companies operate as fully integrated providers serving end users directly, many partner in different ways with MNOs, while others still work through resellers, enterprise intermediaries or hybrid models that combine elements of all three.

These varied structures do not map onto regulatory frameworks designed for the traditional wholesale model. As the satellite connectivity landscape evolves, so too must the frameworks governing it.

1. Global Mobile Personal Communications by Satellite.

Satellite services: segments, market definitions and architecture

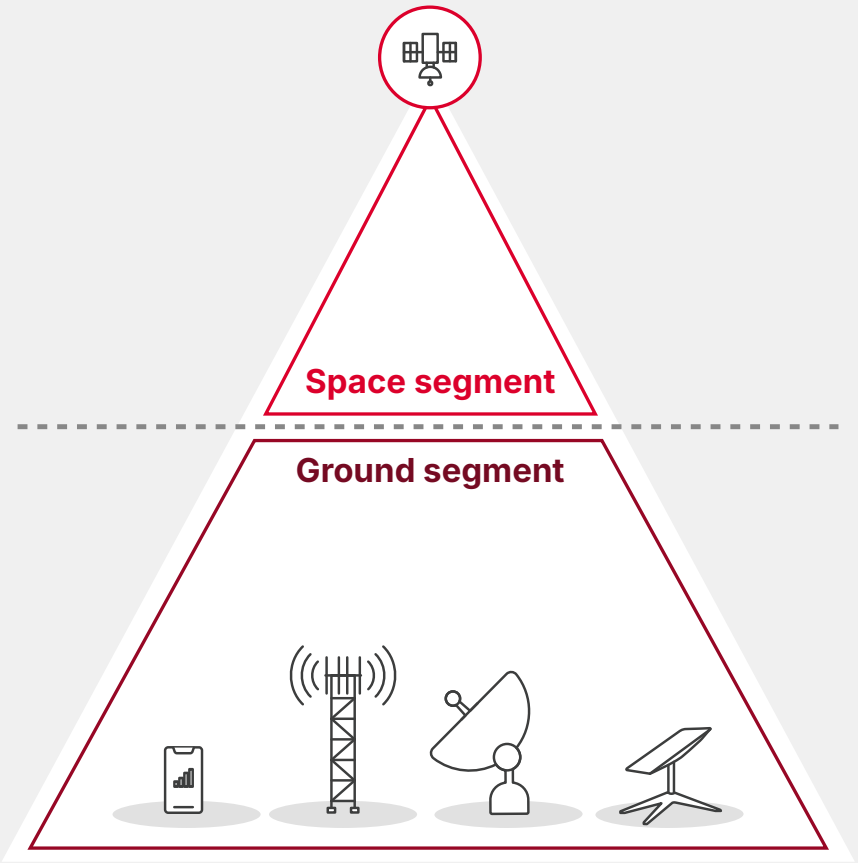
Space and ground segments

Satellite communication frameworks, across commercial, technical and regulatory domains, commonly distinguish between two complementary layers: the space segment and the ground segment.

The space segment consists of all network elements located in space, including satellites, their payloads and bus, and any inter-satellite links. It is responsible for the transmission, reception and processing of signals while in orbit.

The ground segment comprises ground stations (including gateway stations), user terminals, such as VSATs for broadcast services, satellite phones and soon mobile phones with integrated satellite D2D technology — as well as associated terrestrial networks. A ground station refers to any terrestrial facility that supports satellite operations.

Figure 1
Space and ground segments



Source: Access Partnership

Services and market definitions[2]

Satellite operator:

A Satellite Operator (SO) is the legal entity that holds the end-user service contract for the provision of satellite services. A SO may fulfil its service obligations through owned or third-party infrastructure, including satellite capacity, gateway and Telemetry, Tracking and Control (TT&C) earth stations, by one or more separate legal entities.

Satellite broadband:

Satellite broadband is a service, mostly delivered to user terminals via LEO satellite constellations, operating under the fixed-satellite service (FSS) framework. Services are provided via dedicated satellite terminals and supported by ground station gateway infrastructure and are typically commercialised as broadband access solutions for households, enterprises and hard-to-reach locations, effectively delivering 'broadband to the premises' via satellite infrastructure. These networks function as self-contained connectivity platforms, with their own spectrum assignments, ground infrastructure and service ecosystems, positioning them as an alternative access layer alongside terrestrial broadband rather than an extension of mobile networks.

Direct-to-device:

Direct-to-device (D2D) is a communications model that enables smartphones to connect directly to satellites without the need for dedicated satellite terminals or external user equipment. D2D differs from traditional satellite broadband by targeting ordinary consumer devices.[3]

At present, LEO satellite connectivity capabilities are available only on a limited range of devices. However, this is expected to expand rapidly as handset support and network deployments increase. Also, current D2D services remain constrained in scope and performance, affected by factors such as latency, line of sight/indoor coverage, spectrum sharing constraints and power limitations of handheld devices. Most deployments today support low-bandwidth applications, such as emergency messaging or basic text services. Over time, these capabilities are expected to evolve to include significantly more advanced voice and data capabilities.

Numerous models are currently under development, with additional approaches likely to emerge as D2D satellite services continue to mature.[4] From a regulatory perspective, these models differ primarily according to who provides the service to the end user and which regulatory framework applies. Broadly, they can be categorised into two main models:

— **D2D in partnership with a mobile network operator**
In this model, the satellite operator works in partnership with a mobile network operator, leveraging the MNO's licensed network resources. The satellite component is integrated into the mobile network and operates as an extension of the terrestrial connectivity service. The customer relationship remains with the MNO.

— **D2D without partnership with an MNO**
In this model, the satellite operator provides connectivity directly to devices without using an MNO's licensed spectrum or network infrastructure. The satellite system therefore operates independently of the terrestrial mobile network framework. The customer would contract directly with SO.

2. For the purpose of this report, these definitions are used.
3. And other services, such as IoT.
4. These could include other models such as 'base station in the sky' architectures and roaming.

Network architecture

To provide broadband services, a SO must deploy and maintain a satellite network and associated TT&C earth stations to control and monitor its satellites. Gateway earth stations, end-user terminals and points of presence (PoPs) within the ground network are required to deliver broadband connectivity to end customers.

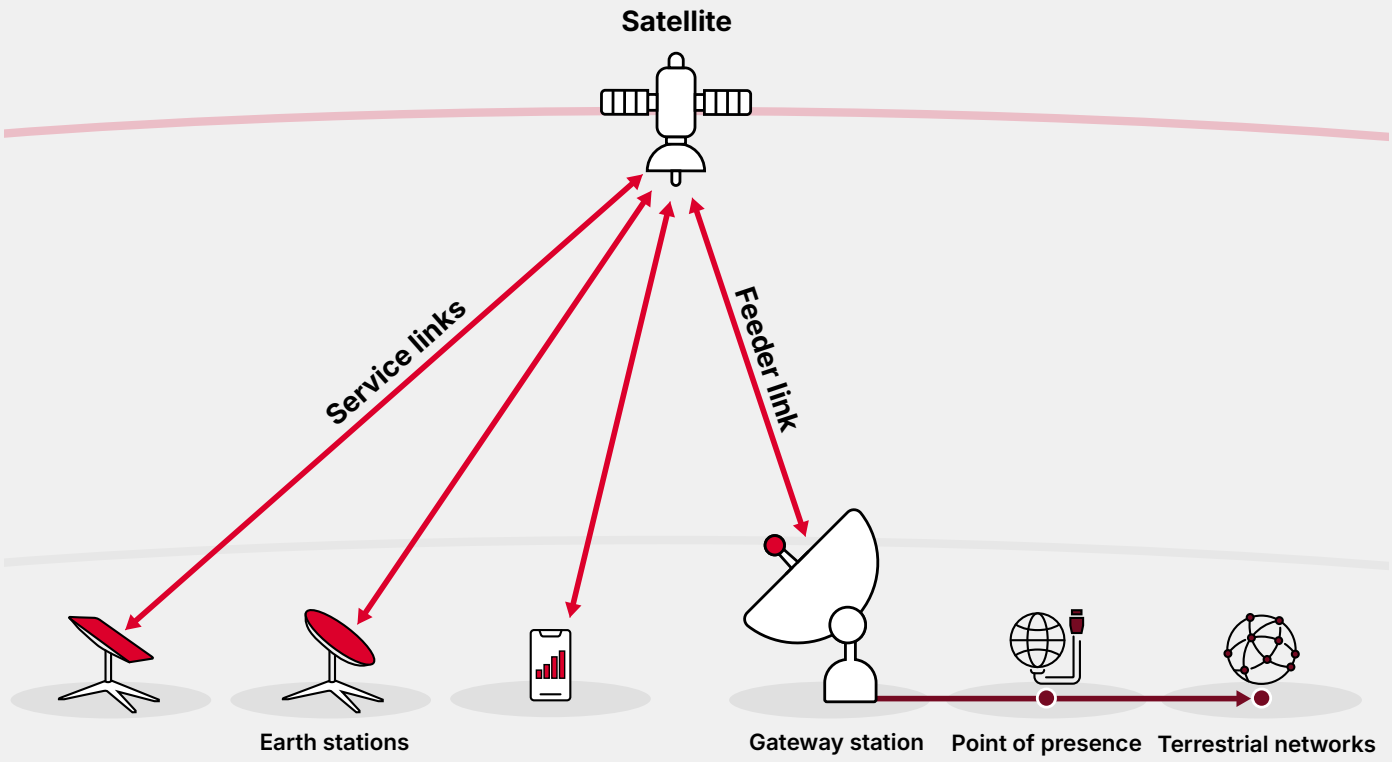
A gateway earth station is a specialised earth station that connects satellites to the main network on the ground, acting as a bridge between space and terrestrial networks. And end user terminals are stations that are used by end users to connect.

In current LEO satellite broadband networks serving homes and businesses, end-user earth stations typically take the form of consumer or enterprise terminals installed at the user's premises. These terminals receive the signal from the satellite and provide local connectivity — usually via Wi-Fi — to the end user's devices. Traffic is transmitted from the end-user terminal to the satellite and onward to a gateway earth station.

In a D2D setup, the functions enabled by the traditional earth stations are the mobile devices. The figures in the Annex show the basic network architectures for satellite broadband and D2D services.

The diagram below illustrates a typical satellite network architecture:

Figure 2
Satellite communication architecture



Source: Access Partnership

A point of presence (PoP) is a network access point where satellite networks interconnect with terrestrial networks, internet backbones or data centres. PoPs may be part of the satellite infrastructure, or remain part of the terrestrial network, depending on the model implemented. In the context of mobile networks, a PoP is a logical or physical connection point where a mobile operator connects its network to other networks or critical infrastructure. Data transmitted from an earth station is routed through a satellite to a gateway and then forwarded from the gateway to a PoP.

PoPs can be located next to a gateway earth station or in a different country, enabling data to be transferred to that location. The difference between a gateway earth station and a PoP is that a gateway earth station provides the physical radio-frequency interface between space and earth, enabling traffic to be transmitted between satellites and terrestrial infrastructure. A PoP, by contrast, is a network access point where data received from the satellite network is interconnected with other networks, such as the public internet, private backhaul networks or cloud service providers.

PoPs serve as an interface between the satellite network and terrestrial internet infrastructure and therefore can serve as locations where lawful interception take place. PoPs are significantly less expensive to deploy than gateway earth stations and, in jurisdictions where SOs are subject to lawful interception requirements, they may provide a practical point at which authorities can access transmitted data in accordance with applicable laws and regulations.

Lastly, satellite communications rely on two distinct types of links. The service link refers to the radio link between the satellite and the end-user terminal, enabling the provision of connectivity services to users. The feeder link refers to the link between the satellite and the gateway earth station, through which user traffic is backhauled into the terrestrial network.

Space versus ground regulation

The distinction between space and ground segments reflects different regulatory objectives. Space-segment authorisations address international coordination and oversight of space activities, while ground-segment licensing ensures that retail services offered within a country are subject to local laws such as national telecommunications law, competition law, consumer protection and enforcement mechanisms.

Regulatory frameworks therefore need to treat satellite connectivity as comprising two distinct but complementary layers of authorisation, reflecting the separation between activities that take place in outer space and those that occur within national territory.

Space segment

The space segment relates to the satellite system operating in orbit, including the satellites themselves and the associated space-based network that transmits radio signals between space and Earth. Authorisations at the space-segment level determine whether a satellite system, particularly a satellite system filed in a third-party country, is permitted to provide coverage or capacity over a country's territory. These permissions are often referred to as 'landing rights' or 'foreign satellite registration'.

Landing rights are a central mechanism through which governments regulate access by foreign satellite systems to national territory. They concern permission for the satellite system itself to operate in relation to the national territory and do not, on their own, confer the right to offer telecommunications services in the country.

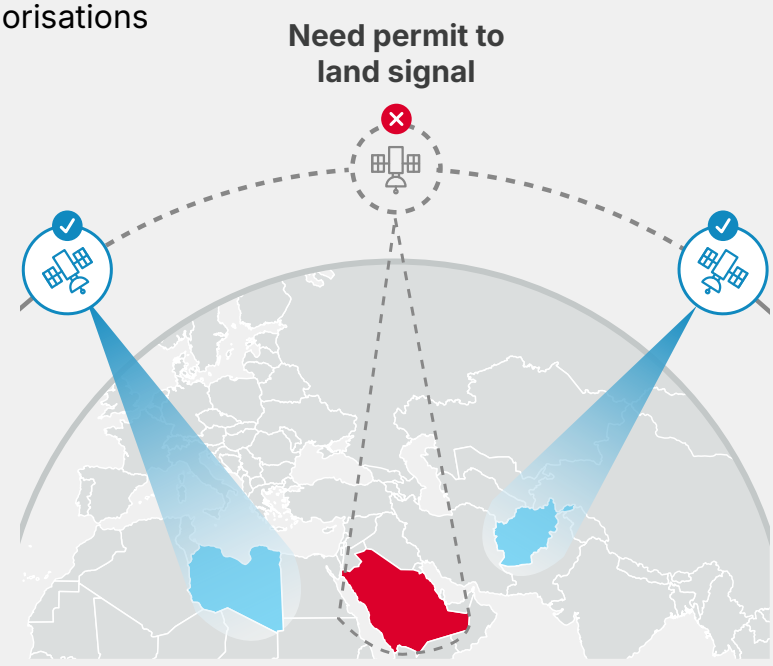
Many jurisdictions[5] have adopted **Open Skies approaches** under which no landing-rights registration or authorisation is required for foreign satellite systems, allowing satellite capacity to be used freely subject to domestic service and radio frequency licensing.[6] Some jurisdictions apply **formal licensing or registration processes** for foreign satellites, requiring satellite operators to apply for approval before their systems are permitted to cover the country. Other jurisdictions rely on **lighter-touch notification mechanisms**. In such cases, the focus is on ensuring regulatory visibility and accountability rather than imposing a full licensing regime at the satellite level.

The emergence of LEO systems does not necessarily require a fundamentally different regulatory model when it comes to international space regulation, but it does increase the importance of ensuring that the chosen framework is clear, proportionate, harmonised and capable of accommodating high-volume, dynamic satellite operations.

Where landing rights are required, regulators may request information such as the satellite system's filing and coordination status with the International Telecommunication Union (ITU), key technical and operational parameters of the satellite network, confirmation of international coordination where relevant, and corporate or ownership information relating to the satellite operator. These requirements are generally intended to support transparency, national oversight and consistency with international obligations, rather than to regulate retail service provision.

For details on Space Regulatory Obligations, refer to the Annex.

Figure 3
Landing rights authorisations



Source: Access Partnership

5. Such as the EU.
6. It could vary in some countries depending upon bands (IMT or MSS).

Ground segment

The ground segment, by contrast, encompasses all infrastructure and activities located on Earth that enable the delivery of satellite-based connectivity to users. This includes user terminals such as satellite dishes, modems or satellite-enabled consumer devices; ground stations and gateways that connect satellites to terrestrial networks or the internet; and the operational and commercial activities associated with service provision, including customer management, billing and support.

Ground-segment authorisations determine whether an entity is permitted to establish or operate communications networks and to provide communications services to the public.

Where a satellite operator or service provider operates ground-based infrastructure within national territory — such as gateways or hubs — regulators should require that they obtain a licence or permit authorising the operation of a communications network. This requirement reflects the traditional regulatory treatment of physical network infrastructure, regardless of whether the access network is terrestrial or satellite-based ensuring a level regulatory playing field.

Separately, where LEO satellite broadband and D2D services are offered directly to users, regulators require a licence or authorisation to provide communications services, triggering obligations associated with retail service provision.[7] Depending on the jurisdiction, these may include consumer protection rules, service quality requirements, reporting obligations, equipment type approvals and compliance with broader telecommunications law. These issues are covered in detail in subsequent sections.

LEO satellite broadband

LEO satellite broadband is now offered as a retail connectivity service to households, enterprises and public-sector users, often in direct competition with terrestrial broadband. Regulatory treatment should therefore be guided by technology neutrality and LEO operators providing retail broadband should be subject to equivalent obligations to those applied to terrestrial services, covering satellite networks, gateways, earth stations and user terminals.

D2D

D2D services integrate satellite connectivity directly into the mobile ecosystem, but the applicable regulatory framework depends on the service model.

— **D2D in partnership with an MNO:** The existing mobile regulatory framework generally applies. The MNO remains the retail service provider and carries responsibility for licensing, consumer protection and quality-of-service obligations. The satellite operator acts as a technical enabler rather than a retail provider, though responsibility for gateway licensing and feeder link compliance remains with the SO.

— **D2D without partnership with an MNO:** This model does not fit neatly within existing mobile or satellite service categories. It has the potential to evolve into a distinct service category, requiring new or adapted regulatory treatment. Subsequent sections of this playbook provide guidance on how regulators may approach these emerging arrangements.

7. In several jurisdictions, the provision of wholesale managed services to resellers may also trigger a requirement to obtain a licence or authorisation to provide communications services.

Alignment with GSMA principles

The evolution of policy frameworks for satellite needs to be aligned with the five core principles set out in the GSMA's global position paper 'Regulatory preparedness for satellite services — direct-to-user LEO connectivity services'.[8]

1 **Principle 1: Transparency and predictability**

Ensure clear and transparent regulatory requirements to facilitate efficient market entry and build industry confidence.

2 **Principle 2: Regulatory parity**

Allow for equitable treatment of sectoral laws and regulations across all service providers.

3 **Principle 3: Harmonisation**

Align regional and international policies to reduce fragmentation and enhance regulatory efficiency.

4 **Principle 4: Collaboration and consultation**

Strengthen dialogue among governments, regulators and industry stakeholders for informed and inclusive policymaking.

5 **Principle 5: Balance innovation with regulation**

Encourage technological progress while maintaining compliance, consumer protection and national security to build trust.

Taken together, these principles enable a balanced policy framework for LEO Satellite services that supports innovation and facilitates market access, while ensuring regulatory coherence and delivering investment, consumer trust and wider societal benefits.

8. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2026/02/Regulatory-Preparedness-for-Satellite.pdf.

Satellite regulatory framework

The global satellite sector is evolving at an unprecedented pace, with the rapid emergence of LEO satellite constellations growing global connectivity. Services are rapidly expanding beyond initial narrow use cases, such as emergency messaging, towards consumer services offering constant connectivity. These developments, however, challenge long-standing regulatory models that were designed for traditional satellite services.

Regulatory parity

As satellite services scale towards widespread consumer use, national regulatory frameworks need to adapt accordingly. In this context, clear, predictable and transparent regulatory frameworks become increasingly important. From a consumer and societal perspective, regulatory approaches should ensure consistent outcomes across functionally equivalent services.

Where similar services are subject to different regulatory treatment, this may result in uneven levels of consumer protection, unfair competitive advantages, gaps in service reliability and inconsistencies in areas such as lawful access and security. Such divergences may also fragment broader connectivity policy objectives and create challenges for public authorities. This would amount to a de facto regulatory subsidy and could distort investment incentives for terrestrial networks, especially in marginal and rural areas.

To address this, regulatory frameworks should be technology-neutral and proportionate to the nature and scale of the service provided. Where satellite operators offer direct-to-user services, equivalent obligations should apply, notwithstanding differences in network architecture. A consistent approach is essential to support fair competition, regulatory clarity and sustained investment across an increasingly diverse connectivity ecosystem.

Effective and clear regulatory obligations facilitate orderly market entry, provide legal certainty for investors and operators and support fair competition. From a public policy perspective, they also allow regulators to safeguard consumer protection, national security and service quality while encouraging innovation and the expansion of infrastructure into underserved areas.

Scope and approach

This section introduces the regulatory frameworks applicable to emerging satellite services delivered via LEO constellations, including direct-to-home satellite broadband and direct-to-device services delivered directly to end users without partnerships with mobile operators. It focuses on the authorisations required to provide services to end users and the associated market access conditions.

Recognising that regulatory frameworks vary across jurisdictions due to differing levels of market maturity and policy evolution, this section does not advocate a single regulatory model. Instead, it provides an overview of key regulatory dimensions and policy considerations relevant to national approaches to LEO satellite broadband and direct-to-device services. This can also be linked to national goals and digital strategies.

Spectrum policy is not addressed in this Playbook. Spectrum access and assignment frameworks for LEO satellite services are evolving rapidly, with satellite operators pursuing increasingly diverse spectrum strategies across licensed, shared and unlicensed bands. Tying the regulatory guidance in this Playbook to specific spectrum rules would risk making this playbook quickly outdated. Nothing in this Playbook should be read as GSMA expressing a position on whether satellite operators should or should not have access to IMT spectrum. However, shared use of radio spectrum licensed to a mobile operator must only be allowed with the agreement of the primary holder of the terrestrial rights. It is also essential that sufficient safeguards are in place to ensure that D2D operations in mobile bands do not cause harmful interference to existing mobile services. GSMA's spectrum policy work for satellite services is addressed separately and updated on an ongoing basis.[9]

9. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/satellite/.

Regulatory pillars

Regulatory pillars

Local establishment rules

Satellite operators offering direct-to-user services should maintain a local legal presence and comply with foreign ownership rules to enable effective oversight and accountability.

National security

Satellite operators should comply with data governance rules (covering data protection, retention, privacy and localisation) and meet cybersecurity and lawful interception requirements.

Consumer protection and operational measures

Consumers using satellite services should receive equivalent protections to terrestrial users, including pricing transparency, quality-of-service safeguards, complaints handling and, where applicable, KYC requirements.

Infrastructure and facility requirements

Satellite infrastructure should be authorised under clear, proportionate frameworks that include requirements related to international connectivity, traffic routing and cross-border gateways.

End user terminal deployment

Satellite terminals should comply with national equipment certification, authorisation and installation requirements to ensure safety and prevent interference.

Fiscal considerations

Retail satellite services should face equivalent regulatory fees and taxes to terrestrial providers to ensure fair competition and affordability.

Emergency services and public safety

Satellite services should enable access to emergency numbers, localisation information and public warning systems, ensuring consistent public-safety outcomes across connectivity platforms.

Enforcement

Satellite operators providing equivalent services to those offered by terrestrial providers should be subject to credible enforcement mechanisms and comparable penalties.

Local establishment rules

Policy recommendation

Satellite operators offering direct-to-user services without MNO partnership should be required to establish an appropriate local legal presence (such as a subsidiary, branch or authorised representative) to ensure effective regulatory oversight and compliance aligned with existing licensing requirements. This is particularly important where services are provided directly to end users without a terrestrial intermediary.

In addition, satellite operators should be prepared to navigate foreign ownership and investment frameworks, which may include equity caps, local shareholding requirements and prior approval mechanisms. These rules are typically linked to broader national policies on telecommunications, critical infrastructure and security, and should apply even where services are delivered on a cross-border basis.

Overview

Local establishment requirements are generally linked to several core regulatory objectives. Where SOs provide direct-to-user LEO services, there should be no unjustified divergence in how local establishment requirements are applied, for the following reasons:

First, local establishment supports **regulatory supervision and enforcement** by ensuring that authorities have a clearly identifiable and legally accountable entity within national jurisdiction. This facilitates compliance monitoring and dispute resolution, particularly where services are provided directly to end users.

Second, local presence requirements are closely linked to **consumer protection objectives**. Regulators often require licensed/notified entities to maintain a domestic point of contact for customer complaints, dispute resolution and regulatory inquiries. This is particularly relevant where satellite broadband or D2D services are offered on a retail basis.

Third, such requirements are often tied to **taxation and fiscal considerations**, including the collection of corporate taxes, sector-specific levies or contributions to universal service or other public funds. Establishing a local legal presence enables authorities to apply domestic fiscal rules in a manner consistent with those applied to terrestrial telecommunications operators.

Finally, local presence obligations are increasingly associated with **national security and public interest considerations**, including lawful interception, data access and compliance with national security directives. Requiring the establishment of a domestic legal entity or representative can facilitate coordination with competent authorities and ensure that providers are subject to national legal frameworks governing security and public safety.

Legal presence

The requirement to maintain a local legal presence is a long-standing feature of telecommunications regulation and is intended to ensure that providers offering connectivity services are subject to effective regulatory oversight and domestic legal accountability.

Local legal presence requirements typically take one of the following forms:

- *A locally incorporated subsidiary*, established under national company law and holding the relevant telecommunications licence or being a notified entity in its own name;
- *A registered branch office of a foreign entity*, authorised to operate commercially within the jurisdiction and subject to domestic regulatory and tax obligations; or
- *A formally appointed local representative or agent*, empowered to act on behalf of the foreign provider for regulatory, legal and administrative purposes.

The specific form required may depend on the type of services being offered, the related licence or notification obligations and whether the provider engages directly with end users.

Where the satellite operator provides D2D services directly to customers, without an MNO acting as the retail intermediary, regulators would require the establishment of a local legal presence and the granting of a separate national authorisation to the satellite operator. This also applies when satellite broadband is provided directly to end users.

Foreign ownership

Foreign ownership and investment restrictions can represent a key determinant of market entry conditions for LEO satellite services. These conditions are typically embedded within broader national frameworks governing telecommunications licensing or notification obligations, foreign direct investment (FDI) and national security, and would therefore be likely to apply to LEO satellite-based service providers.

Foreign participation in licensed communications entities may be subject to one or more of the following constraints:

- *Caps on foreign ownership*, limiting the maximum equity stake that non-domestic investors may hold in a licensed telecommunications operator;
- *Mandatory local shareholding or participation requirements*, which may require a minimum percentage of ownership by domestic individuals or entities, sometimes linked to broader economic or social policy objectives; and
- *Investment screening or approval mechanisms*, under which foreign investors must obtain prior clearance from designated authorities before acquiring equity, control or significant influence in a licensed entity.

These mechanisms may apply cumulatively, particularly in jurisdictions that treat telecommunications infrastructure and services as strategically sensitive.

Even where satellite operators are headquartered abroad and operate global or regional constellations, the provision of satellite broadband or D2D services to end users in a jurisdiction would be likely to trigger foreign ownership and investment rules. Satellite systems operating on a cross-border basis with gateways located within national territory may also be classified as critical infrastructure and subject to foreign ownership limitations or prior government approval.

National security

Policy recommendation

The national security and telecommunications requirements applied to satellite operators should be comparable to those applied to terrestrial networks, when providing direct-to-user services. This includes, where applicable, complying with data protection and data localisation rules, ensuring lawful data processing, and meeting data retention obligations where services are functionally equivalent to mobile or fixed connectivity.

Satellite operators should also be required to implement robust cybersecurity laws and measures, including risk assessments, incident reporting and adherence to national cybersecurity frameworks, to safeguard users, networks and critical infrastructure.

In addition, satellite providers should support lawful interception obligations, enabling authorised access for law enforcement and national security purposes. Achieving this will require technical capabilities, such as local gateways or routing arrangements, to ensure interception is feasible within national jurisdictions and to avoid regulatory gaps that could otherwise undermine public safety.

Overview

National security is a core pillar of tele-communications regulation and is increasingly relevant to LEO satellite communications. As these networks deliver mass-market services, they raise the same regulatory issues as terrestrial networks in areas such as data governance, cybersecurity, lawful interception and access to data. This reflects the critical role that communications infrastructure plays in public safety and the digital economy. This section outlines the key regulatory domains for LEO satellite services and the extension of existing frameworks to satellite operators. A consistent and proportionate approach is essential to protect national interests and end users, while supporting growth and investment across the communications ecosystem.

Data protection, data privacy, data localisation and retention

Telecommunications services are typically subject to data protection frameworks governing the confidentiality of communication and the collection, processing, storage and transfer of personal data. These frameworks often include requirements for data localisation, restrictions on cross-border data transfers and obligations to retain certain categories of data for given periods of time to support law enforcement and national security objectives. In some jurisdictions, the processing of communications data is subject to sector-specific rules, reflecting the perceived particularly sensitive nature of such data.

Satellite operators that process or control personal customer data should be subject to the same data protection and privacy laws as terrestrial telecommunications providers. For example, regulators should require satellite operators that process or control communication data and personal customer data to comply with national data protection laws concerning the lawful processing of data, the storage of certain data domestically or the cross-border transfer of data.

This is essential to ensure consistent levels of privacy protection for consumers, while also safeguarding broader societal interests such as trust in digital communications and the integrity of national data governance frameworks.

Data retention obligations (where applicable), traditionally focused on mobile and fixed operators, should also be extended to satellite providers where services are functionally equivalent to terrestrial connectivity. This is necessary to ensure that law enforcement authorities retain effective access to relevant communications data for the purposes of investigating and prosecuting crime, and to avoid the emergence of regulatory gaps that could be exploited to circumvent such capabilities.

Cybersecurity requirements

Cybersecurity obligations can form an important aspect of national security regulation for both satellite and MNO networks. It is expected that the regulators will require LEO satellite operators to implement technical and organisational security measures, conduct risk assessments, report incidents and adhere to national cybersecurity strategies. Satellite operators should also be expected to uphold high cybersecurity standards, especially for gateway infrastructure, network control systems and data handling. This serves to protect consumers from service disruptions, data breaches and misuse of their communications, while also safeguarding the resilience and security of communications infrastructure on which societies increasingly depend.

In some jurisdictions, these requirements are reinforced by telecom-specific security legislation and regulatory codes of practice. For example, if there is a data or security breach, the operator must notify the relevant telecom or law enforcement authorities. In others, enhanced security requirements — such as vendor security assessments and additional risk-mitigation measures — may apply to critical infrastructure, including 5G networks. In the future, satellite networks delivering equivalent services should be subject to the same requirements.

Lawful interception

Across both sectors, the core regulatory expectation is that operators must not prevent or obstruct lawful interception and must support authorised access at appropriate network interception points. Regulators require service providers to enable government authorities, acting under lawful authorisation, to intercept communications for law enforcement, national security, public safety or other legally permitted purposes. This obligation reflects national sovereignty over communications within a state's territory and is reflected in both telecommunications law and international regulatory principles.

For mobile networks, lawful interception requirements are quite explicit, with interception capabilities embedded within the core network. Satellite operators have historically been subject to limited lawful interception obligations, particularly where services were non-interactive, broadcast-only or enterprise-focused. However, where satellite operators provide direct-to-user services, such as satellite broadband or direct-to-device connectivity, regulators should apply lawful interception obligations that are comparable to those imposed on mobile operators. This is necessary to ensure that law enforcement authorities can maintain effective and consistent investigative capabilities, and to prevent the emergence of gaps that could allow equivalent communications services to be used to circumvent lawful interception frameworks.

These conditions are typically enforced through licence conditions or market-access authorisations rather than standalone interception statutes. Where necessary, regulators may require satellite operators to cooperate with lawful interception requests, provide access to relevant traffic or route communications through approved domestic gateways to facilitate interception within national jurisdiction.

Regulatory concerns may arise where no gateway or PoP exists within the country where services are provided, making lawful interception technically infeasible within national territory. In such cases, regulators may require local routing arrangements or the establishment of mechanisms to ensure lawful interception obligations can be met. This may include the use of a domestic PoP, the deployment of a gateway station within the service jurisdiction or arrangements enabling interception via a foreign PoP in compliance with applicable laws and regulations.

In addition, related law enforcement conditions — such as requirements for the use of locally security-cleared staff and access to secure sites — should also be equally applied.

Consumer protection and operational measures

Policy recommendation

As LEO satellite broadband and D2D services are delivered directly to consumers without partnerships with mobile network operators, users should benefit from the same level of protections as those using terrestrial networks.

No consumer should face reduced rights or safeguards simply because of how connectivity is delivered. Consumer protection obligations should therefore apply consistently based on service type, covering areas such as subscriber identity verification (where applicable), transparent pricing and contract terms, billing accuracy, effective complaints handling and access to dispute resolution mechanisms.

Where relevant, proportionate subscriber registration or Know Your Customer (KYC) requirements should be applied to support security, lawful access and scam prevention, while avoiding regulatory gaps or arbitrage.

Regulatory frameworks should also be updated to reflect satellite-specific technical characteristics, ensuring consistent enforcement across different delivery platforms.

Where quality-of-service (QoS) frameworks are implemented, they should enable consumers to make informed decisions based on clear, transparent and comparable service performance information. This requires that QoS monitoring and reporting outputs are consistent across technologies and that information provided for LEO satellite services allows meaningful comparison with terrestrial offerings.

Satellite operators should also anticipate compliance with pricing-related regulatory frameworks that already apply to terrestrial providers, including transparency requirements, tariff notification or approval processes and affordability safeguards.

Overview

Where satellite services target mainstream consumers, regulators expect equivalent levels of transparency, service quality and consumer protection. With the emergence of LEO satellite broadband as a retail consumer offering, consumer-protection obligations should be determined by the type of service provided rather than the underlying technology.

A robust consumer protection framework for LEO satellite operators providing services directly to users (without partnerships with mobile network operators) should address areas such as subscriber registration, pricing transparency, contract terms, quality of service, complaints handling, end-user device warranties and serviceability and billing accuracy. The overarching regulatory objective should therefore be to protect consumers by preventing misleading information and ensuring that licence obligations are effectively monitored and enforced.

Subscriber registration

Subscriber registration is a regulatory mechanism that enables authorities to associate communications services with identifiable users. Typically implemented through KYC obligations, it is often promoted as supporting law enforcement, national security and fraud prevention.

As LEO satellite services expand into direct-to-user and consumer broadband connectivity, equivalent registration requirements become increasingly important in jurisdictions where such frameworks are in place. Where services are functionally similar to terrestrial offerings, the ability to identify users is critical to prevent misuse and to ensure the effectiveness of lawful-access regimes.

In those markets where KYC requirements are applied, inconsistent application across providers could create enforcement gaps and opportunities for regulatory arbitrage, undermining the effectiveness of existing security and lawful access frameworks.

Existing regimes are often designed around SIM-based mobile services and may not fully capture satellite use cases, where connectivity may rely on user terminals or non-SIM-based authentication. Regulatory frameworks therefore should evolve towards technology-neutral approaches.

In practice, satellite operators providing direct-to-user services should be subject to the same KYC obligations, where such requirements apply, including identity verification and record-keeping aligned with the nature of the service and consistent with obligations applicable to terrestrial service providers. This ensures consistent regulatory outcomes while supporting security and public safety objectives.

Quality of service

Quality-of-service regulations are another area where consistent application at the service level is important. QoS frameworks are employed by regulators in some markets as a tool to help ensure customers experience a consistent and reliable service, are able to make informed choices and assess whether contractual commitments are being fulfilled. As with regulatory domains, QoS frameworks for LEO satellite services should be transparent, technology neutral and applied on an equitable basis to all relevant operators. This will enable consumers to make informed choices about the communication services they purchase, including LEO services.

Where applicable, QoS regulatory frameworks typically include monitoring, reporting and publishing requirements, with defined performance indicators and minimum thresholds. For example, under the European Electronic Communications Code (EECC), regulators may require providers of broadband and public peer-to-peer communication services to publish comprehensive, comparable and up-to-date information on the quality of their services. These transparency obligations are technology-neutral and depend on the nature of the service rather than the platform used to deliver it.

Technical differences may require some differentiation of QoS standards between mobile and satellite internet services. However, this should not result in different overall service quality outcomes. Any distinctions should be limited to accounting for technical nuances when designing relevant frameworks and corresponding obligations, ensuring that measurements remain accurate and meaningful.

Consumer tariff rules

In addition to direct fees, some jurisdictions impose pricing-related regulatory requirements on licensed telecommunications service providers, which should also apply to LEO satellite-based retail services. These may include:

- *Tariff filing or notification obligations*, requiring providers to submit pricing structures or service plans to the regulator for information or monitoring purposes;
- *Tariff approval requirements*, under which prices must be approved prior to commercial launch;
- *Price controls or caps*, applied either generally or to specific services, user categories or geographic areas; and
- *Cost-orientation or non-discrimination requirements*, obliging providers to demonstrate that tariffs are based on underlying costs or applied fairly across comparable customer groups;

While such measures have traditionally been associated with terrestrial operators or legacy services, they should be extended to satellite-based retail offerings to reflect regulators' growing focus on consumer protection and affordability as satellite services expand beyond niche applications.

Other safeguards

Consumer-protection safeguards ensure that end users receive clear, fair and reliable services. These obligations typically apply to providers offering services directly to consumers and are designed to promote transparency, accountability and trust in communications markets.

Key safeguards include billing accuracy, ensuring that charges are correctly calculated and transparently presented; pricing transparency, including clear disclosure of tariffs, fees, and any usage limitations; and the provision of accessible information allowing users to understand service characteristics, performance expectations and contractual terms.

In addition, terrestrial operators are typically required to maintain effective complaints handling mechanisms, allowing users to raise and resolve issues in a timely and transparent manner. This includes clear procedures, response timelines, and, where applicable, access to independent dispute resolution mechanisms.[10]

Consistent and proportionate application of these safeguards to satellite operators providing direct-to-consumer services is essential to maintain consumer trust, regulatory coherence and fair competition across the connectivity ecosystem.

10. Some jurisdictions have other requirements to reduce scam messages and scam voice calls.

Infrastructure and facility requirements

Policy recommendation

As LEO satellite services provided directly to users become part of national communications infrastructure, the planning, security and deployment standards that apply to terrestrial networks should apply equally to satellite networks. This is essential to protect users, communities and national interests. Policymakers should establish clear, transparent and proportionate frameworks for the approval and deployment of satellite infrastructure, including user terminals, gateway earth stations and points of presence (PoPs), ensuring alignment with broader telecommunications and planning regulations.

Regulatory requirements related to routing, international connectivity and cross-border gateways should be designed to address legitimate national security and data sovereignty objectives, while avoiding unnecessary restrictions that could hinder service deployment and innovation. Policymakers are also encouraged to promote infrastructure efficiency, including enabling voluntary co-location and shared use of passive facilities where feasible, to reduce costs, minimise environmental impact and support timely network roll-out.

Overview

Infrastructure and facility requirements are a core component of the regulatory framework applicable to LEO satellite communications, as they govern the deployment and operation of the physical and network elements underpinning service delivery. As satellite systems increasingly provide mass consumer market connectivity, regulators are placing greater emphasis on approvals for user terminals, gateway earth stations and network interconnection points, as well as on rules relating to routing, international connectivity and infrastructure sharing.

This section provides an overview of these requirements, highlighting how they can be applied to support network deployment while addressing policy objectives such as interference management, national security and efficient use of infrastructure.

User terminal, gateway earth station and other approvals

The deployment of both terminals and gateway earth stations require an operator to obtain approvals. These approvals, among others applying across different jurisdictions, can include the following:

— *Gateway/earth station licensing*
This is usually an earth station licence, an apparatus/facilities licence, or any other equivalent national authorisation. It can cover location, antenna parameters, emissions and power limits, as well as interference obligations. This authorisation is applicable to gateways, associated feeder links and other ground facilities.

— *Equipment certification (type approval)*
Equipment certification is required to protect health and safety, ensure electromagnetic compatibility and prevent harmful interference. These requirements apply to all radio equipment, including end-user terminals, gateway equipment and other components of satellite ground network infrastructure.

— *Installation (planning, land use and construction) approvals:*
These can be issued by local, municipal or national planning authorities. They cover land use and zoning, as well as environmental and safety compliance.

— *PoP*
To deliver services at a PoP, operators must hold the relevant national licences for the telecommunications or radio services they intend to deliver. Some countries require operators to declare or register PoP locations to meet local telecom obligations, while others impose service authorisations that implicitly include PoPs as part of the public communications infrastructure.

— *Rights of way*
Rights of way and planning permissions are essentially land-use and civil infrastructure approvals that apply to both terrestrial and non-terrestrial networks. Satellite networks require rights of way and planning permissions primarily to deploy gateway stations.

International connectivity and routing requirements

To safeguard national security, sovereignty and lawful access, telecommunications regulators usually impose requirements relating to controls on the establishment of international connectivity and traffic routing. For mobile networks, requirements to route traffic through national infrastructure can form an important part of national security policy. Mobile terrestrial licences commonly require switching, core network functions and lawful interception capabilities to be located domestically. These requirements ensure that authorities retain effective control over communications and can enforce security and public safety.

On the other hand, satellite operators inherently operate cross-border systems, with international connectivity being a fundamental architectural feature of satellite networks. It is necessary for regulators to consider requirements to ensure authorities retain effective control over communications. Nevertheless, market-access authorisations and landing rights can still be used to apply routing requirements. National regulators may also require user traffic originating within the country to be routed through domestic gateways or approved facilities, especially where public broadband or direct-to-device satellite services are offered to the public. Noting that there may not be a gateway in every country and that it could sometimes be shared between countries.

Despite international satellite connectivity being technically permissible, regulators may choose to prohibit or limit the use of foreign gateways to serve domestic users, especially where sensitive data, government communications or critical services are involved. Such conditions may be applied to satellite broadband and direct-to-device services to address concerns relating to lawful interception, data sovereignty and reliance on foreign infrastructure.

Restrictions on cross-border gateways

Cross-border gateway restrictions are primarily driven by national security, data localisation, data protection and lawful interception requirements. Countries may prefer domestically generated traffic to be routed exclusively through in-country gateways to ensure regulatory control, surveillance capabilities and compliance with security rules, effectively prohibiting the use of foreign gateways.

In some jurisdictions, access to international networks is permitted only through sanctioned or 'official' gateways, with alternative cross-border routing explicitly prohibited. If required for satellite LEO connectivity services, these requirements can typically be embedded in telecommunications licensing frameworks, under which gateways are treated as regulated network facilities subject to national authorisation and location requirements.

Co-location requirements

In mobile networks, co-location typically involves voluntary sharing of towers, power supply and shelters for the radiofrequency equipment, and is generally encouraged as a policy objective rather than mandated. Co-location helps reduce duplication, lower CAPEX requirements and minimise environmental impact.

For satellite networks, gateway infrastructure may be shared at the site or facilities level.

Multiple satellite operators may co-locate gateways at a common site and share passive infrastructure such as land, buildings, power supply, security and backhaul connectivity. However, active RF gateway equipment — including antennas, RF chains and network systems — is generally specific to each operator and individually controlled. Co-location of active infrastructure is typically feasible only where operators are using different frequencies, reflecting technical requirements related to interference management, network control and security.

End user terminal deployment

Policy recommendation

Regulators should ensure that satellite user terminals used in direct-to-user services meet common technical standards in order to protect consumers, prevent harmful interference and maintain the integrity of shared spectrum resources. This includes compliance with national type approval and certification frameworks and equipment labelling requirements, aligned with existing telecommunications equipment standards, to ensure safety, electromagnetic compatibility and effective interference management.

Regulators should also establish clear and proportionate licensing or authorisation regimes for the use of satellite terminals, taking into account evolving certification requirements, particularly for emerging use cases such as direct-to-device services. In addition, regulators are encouraged to implement appropriate installation rules for fixed or outdoor terminals, covering aspects such as antenna placement and local planning requirements, to ensure safe deployment and protect both users and surrounding communications infrastructure.

Overview

Satellite terminals constitute the primary interface between satellite networks and end users of satellite services. Accordingly, the deployment and use of satellite terminals need to be regulated through frameworks closely aligned with existing telecommunications equipment.

Across jurisdictions, regulatory requirements for satellite user terminals generally involve a combination of type approval and installation rules.

Type approval or certification

Under this process, satellite terminals should be certified or self-certified as compliant with national technical standards before being placed on the market or connected to networks. These processes are designed to ensure equipment compliance with national technical standards to protect health and safety and ensure adequate levels of electromagnetic compatibility.

A key distinction concerns responsibility for satellite terminal certification. For example, in the European Union, responsibility lies with the equipment manufacturer, which must ensure that radio equipment complies with applicable technical and regulatory requirements. Compliance is demonstrated through manufacturer self-assessment, with equipment presumed to conform if it meets the relevant ETSI harmonised standards. Importers and distributors of satellite terminals are subjected to the same obligations as for terrestrial equipment, while end users play no role in the certification process.

Satellite operators, unless they also act as equipment manufacturers or importers, do not certify terminals. However, satellite operators should ensure that equipment authorised for use on their networks operates safely, does not cause harmful interference and complies with applicable harmonised standards. National regulators may require a licence for the use of satellite terminals or may permit their deployment under licence-exempt or general authorisation regimes, provided that terminals comply with the relevant standards. This serves to protect consumers from unsafe or malfunctioning equipment and to ensure reliable service performance, while also preventing harmful interference that could disrupt other critical communications services relied upon by society. Some jurisdictions could also impose local importation regulations including Local Content Requirements (LCRs) in telecom manufacturing which mandate that a percentage of goods, labour or investment for network equipment and devices have a minimum domestic component or could have specific custom regulations which may require separate import permits/licences.

In D2D scenarios, smartphones would typically be certified as radio equipment in accordance with existing certification rules. However, as D2D services evolve, regulators will need to assess whether additional testing or certification frameworks are required.

Installation rules

Installation rules typically apply to fixed or semi-fixed outdoor terminals, such as satellite dishes or user antennas, which may be subject to building codes, zoning rules or restrictions related to public safety and interference management.

For LEO satellite broadband services, regulators may apply installation-related rules reflecting the physical characteristics of outdoor terminals, including requirements for antenna placement, mounting, and, in some cases, coordination with local authorities or property owners. These requirements are broadly comparable to those applied to other fixed telecommunications infrastructure and are typically enforced at the point of installation or importation rather than through ongoing monitoring. As set out above, their purpose is to ensure safe deployment and to prevent harmful interference with surrounding communications infrastructure.

Fiscal considerations

Policy recommendation

As satellite operators expand and offer direct-to-user services, ensuring they contribute fairly to public revenues is essential to uphold societal needs and protect consumer interests. However, fiscal obligations often flow automatically from service classification rather than deliberate design. Policymakers should therefore actively review whether existing fiscal regimes apply appropriately to satellite services, ensuring obligations are fit for purpose rather than applied by default.

Satellite operators offering retail services should comply with fiscal obligations similar to terrestrial telecom providers, including licensing fees, regulatory levies, universal service contributions and applicable taxes. These obligations should be applied in a technology-neutral and proportionate manner, preventing regulatory arbitrage while avoiding undue burdens that could constrain investment and service affordability. Where sector-specific taxes are applied to communication services, policymakers should consider whether reducing these charges would better serve consumers and broader socio-economic development.

Overview

As satellite services transition towards retail-facing telecommunications services, fiscal obligations need to be increasingly aligned with those imposed on terrestrial providers. Regulatory frameworks should ensure that these obligations are applied in a technology-neutral and proportionate manner, supporting a level playing field while avoiding undue burdens that may constrain investment and service affordability.

Fiscal obligations directly influence investment incentives, pricing flexibility and service affordability. As LEO satellite services (without partnerships) move from wholesale capacity provision towards retail telecommunications service delivery, regulators in many jurisdictions are extending existing fiscal regimes to these services, either explicitly or by default.

Fiscal obligations applicable to satellite broadband and D2D services may not be tailored specifically to satellite delivery models but instead would flow automatically from the classification of the service as a licensed telecommunications activity. Where satellite-based services are authorised under telecommunications licensing frameworks, they should be subjected to similar categories of fees and financial obligations as terrestrial operators, even where the underlying network architecture and cost structures differ materially.

Applicable fees

Across jurisdictions, fiscal obligations imposed on telecommunications service providers typically comprise a mix of one-time charges, recurring fees and variable levies, administered by telecommunications regulators, ministries or other public bodies. These may include:

— *Licensing and application fees*, payable upon submission or grant of a telecommunications licence, authorisation or permit. These fees are generally intended to recover administrative costs and may also apply to licence renewals or amendments;

— *Annual regulatory fees or administrative levies*, commonly calculated as a percentage of relevant turnover or licensed revenues, and are meant to be used to fund the ongoing operations of the regulator or supervisory authority;

- *Contributions to Universal Service Funds (USFs) or equivalent mechanisms*, which are commonly imposed on licensed telecommunications service providers to support connectivity objectives in rural, remote or underserved areas
- *Spectrum-related fees*, where applicable, including administrative charges associated with spectrum authorisations or permits;
- *Type approval or homologation fees for end-user terminals*, covering testing, certification and market-entry approval processes;
- *Other telecommunications-specific fees*, such as numbering charges, inspection or audit fees, or contributions linked to sector development funds; and
- *National corporate and income taxes*, imposed under generally applicable tax legislation on taxable profits or income derived from telecommunications activities and typically applied uniformly across the sector.

Individually, these charges may appear modest; however, in aggregate they can represent a material financial burden. Best practice calls for uniformly lowering sector-specific taxes on communication services to allow the benefits to be passed on to consumers and businesses to boost socio-economic development.

In summary, the application of such fiscal obligations raises important questions of competitive neutrality and proportionality. Where satellite-based retail services compete directly with mobile or fixed wireless access services, applying comparable fiscal obligations would support a level playing field. Conversely, exemptions or preferential treatment risk creating competitive distortions. Governments seeking to stimulate greater investment in communications infrastructure and services may reassess the continued value of such fees and, accordingly, consider reducing them across the whole sector.

Emergency services and public safety

Policy recommendation

All users (where relevant), regardless of whether they connect via terrestrial or satellite services, should be able to access emergency services and receive public safety alerts. Emergency services and public safety frameworks should be updated to reflect the growing role of satellite and direct-to-device (D2D) communications, which are not fully covered by existing terrestrial-focused regulations. Governments should ensure that relevant satellite services, where offered directly to users, can support access to emergency calling, including reliable location information and, where feasible, minimum service availability as applicable to terrestrial providers offering similar services.

Regulators should also consider extending public warning system requirements to satellite-enabled devices to improve emergency alert coverage, especially in remote or underserved areas. In addition, appropriate disaster resilience and service continuity obligations should apply to satellite operators providing critical connectivity, with appropriate coordination with public authorities and alignment with national emergency response objectives.

Overview

Current legal frameworks for emergency services were developed primarily for terrestrial network architectures and may not yet provide a coherent or harmonised approach for satellite-enabled direct-to-device emergency services.

Emergency services and public safety obligations are a critical component of telecommunications regulation. They ensure timely access to emergency assistance, the dissemination of public warnings and the continuity of communications during crises. As LEO satellite and direct-to-device services evolve to provide wider coverage in remote areas and consumer-facing connectivity, their potential role in supporting emergency communications is becoming increasingly significant. This section outlines key regulatory considerations relating to emergency calling, public warning systems and disaster resilience, and examines how existing frameworks, largely designed for terrestrial networks, may need to adapt to accommodate satellite-enabled services.

Emergency calling

Emergency calling obligations, including access to emergency numbers and localisation information, represent a core component of public safety regulation in the telecommunications sector.

For terrestrial networks, regulators typically require uninterrupted access to emergency services, accurate and timely caller location information, and defined levels of network availability and reliability.[11] Internet service providers that do not offer voice services are generally not subject to obligations to provide access to emergency services.

When D2D services evolve and are offered as a standalone connectivity solution (without partnerships with mobile network operators), regulators will need to consider how emergency calling requirements should apply to non-terrestrial networks. Key issues include the technical feasibility of supporting emergency calls/messages from satellite-enabled devices, the availability of reliable location information where terrestrial positioning methods may be unavailable or degraded, and the ability of satellite networks to meet minimum service availability standards under emergency conditions.

11. In many countries, mobile network operators are required to provide access to emergency services even if the caller is not a subscriber to their network.

Public warning systems

Public warning systems, such as cell broadcast or emergency alert frameworks, are increasingly relied upon by authorities to disseminate time-sensitive information during emergencies. Terrestrial mobile networks are commonly required to support such systems as part of their licensing conditions.

The applicability of public warning obligations to satellite-broadband and D2D services is less clearly defined. Regulators are considering whether satellite-enabled devices should be capable of receiving public warning messages, particularly in areas with limited or no terrestrial coverage. Satellite services may play an important role in extending the reach of public warning systems to these remote or underserved populations.

Disaster resilience and continuity requirements

Satellite operators may also be considered for disaster resilience and service continuity obligations comparable to those imposed on mobile network operators, particularly where their services support critical communications. These obligations include continuity planning, operational readiness during emergencies and effective coordination with relevant public authorities.

Enforcement

Policy recommendation

Effective enforcement is essential to the credibility of any telecommunications regulatory regime. Without it, consumer protections, security safeguards and competition rules have little practical impact. Users should not face weaker protections simply because their service provider operates across borders or is located outside national jurisdiction.

Satellite operators providing services equivalent to those offered by terrestrial networks should be subject to comparable penalties and enforceable obligations within each market in which they operate.

Given the inherently cross-border nature of LEO satellite systems, enforcement may be more complex where operators are headquartered or technically managed outside the national jurisdiction. Governments should therefore require a meaningful local legal presence, enabling regulators to investigate non-compliance, compel remedial action and impose sanctions effectively.

Where direct technical control over satellite networks is limited, regulators could focus enforcement on market access measures, including restrictions on terminal sales and activation. Stronger international cooperation and information-sharing between regulators would also be critical to address cross-border non-compliance and ensure consistent enforcement outcomes.

Overview

For telecommunications regulation to be effective, regulatory obligations must be enforceable to protect users, safeguard national security and preserve fair competition for all communication providers. Without credible enforcement mechanisms, even the most well-designed rules risk becoming ineffective, undermining trust in the regulatory framework. Strong enforcement also ensures accountability, deters non-compliance and promotes a level playing field across the sector. Where satellite network operators provide services equivalent to terrestrial providers, they must be subject to comparable penalties and enforcement mechanisms to ensure consistent consumer protection and regulatory outcomes.

The rapid expansion of large LEO constellations has intensified debate around regulatory oversight and enforcement. Their continuous, cross-border operation can complicate compliance with national licensing, spectrum and security requirements and could expose limits in regulators' ability to address conduct occurring outside their territory. Unlike terrestrial networks, satellite systems are often controlled, monitored and technically managed from foreign jurisdictions, making it more difficult for national authorities to investigate violations, compel remedial action or impose sanctions directly on an SO that may not have a legal presence in their jurisdiction.

Effective enforcement in this context depends on the existence of a meaningful legal presence within the jurisdiction. A purely nominal or limited local presence may constrain the ability of regulators to impose sanctions, compel compliance or ensure accountability. Regulatory frameworks should therefore ensure that operators providing services directly to end users are subject to enforceable obligations within the markets in which they operate, particularly where issues of harmful interference, security concerns or persistent non-compliance arise.

In serious cases, regulators may suspend or revoke licences from SOs and, where necessary, withdraw market access. While satellite transmissions cannot be switched off on a national basis, enforcement can be effectively exercised through market access controls, including restrictions on the sale, activation and use of user terminals, as well as obligations imposed on operators and intermediaries within the jurisdiction. Stronger international cooperation, mutual assistance and information-sharing between regulators will be essential to effectively addressing cross-border non-compliance.

Annex

This annex provides supplementary reference material supporting the Playbook, including an overview of international space regulatory obligations applicable to satellite operators and illustrative network architecture.

Space regulatory obligations

The rapid deployment of large constellations of LEO satellites has renewed attention on space-related regulatory obligations applicable to satellite operators. These considerations exist independently of telecommunications regulation and are specifically designed to address legal, safety and sustainability considerations related to activities in outer space. They reflect the specific risks, responsibilities and international legal considerations associated with the operation of objects in outer space.

International space law, developed under the United Nations system, provides the international legal foundation, which is complemented by national regulation of space activities. These frameworks establish core principles relating to state responsibility, liability, registration and supervision of space objects, and directly influence the design of national space regulatory regimes applicable to satellite operators. Although the content and implementation of national space laws vary, they are generally aligned with these international principles and apply to all space activities conducted under a state's jurisdiction or control, including the operation of commercial satellite services.

Detailed space regulatory obligations are mainly applied in a relatively small group of advanced space-faring nations, while many other countries have not yet begun to focus seriously on these aspects of satellite oversight. Where comprehensive regimes do exist, they typically address a common set of domains derived from international space law and established best practices, including:

- Registration and notification of space objects, enabling transparency, jurisdiction and the allocation of international responsibility and liability;
- Space sustainability obligations aimed at preserving the long-term usability of the orbital environment;
- Space debris mitigation requirements addressing debris generation and collision risks;
- End-of-life disposal and deorbiting rules governing the removal of satellites from operational orbits; and
- Space traffic management and conjunction avoidance measures, which are becoming increasingly important as orbital congestion increases.

In many parts of the world, however, these requirements remain limited or absent, with national frameworks focused primarily on basic spectrum and orbital coordination. The result is an uneven global landscape in which only a subset of countries actively impose these obligations as part of satellite licensing regimes and use them to shape the technical design, operational planning and lifecycle management of modern satellite systems.

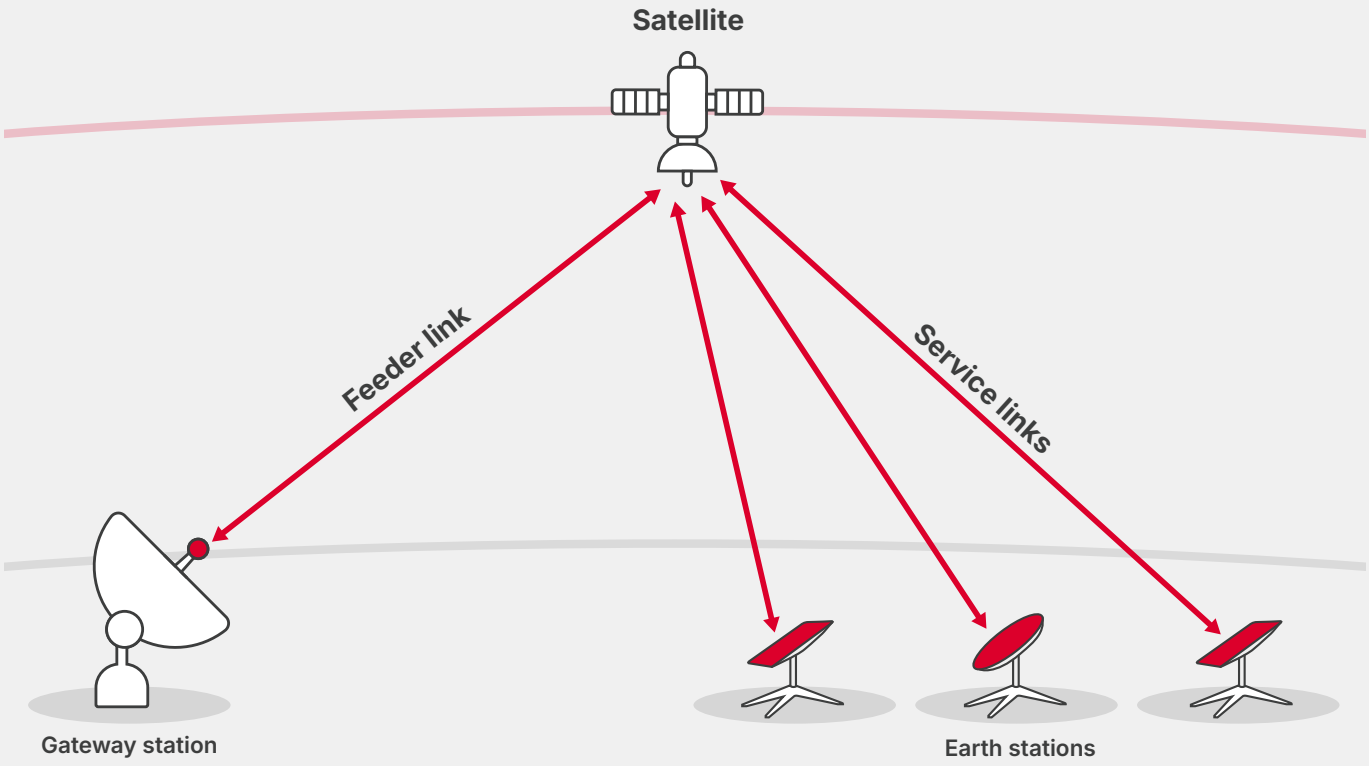
In parallel, satellite networks must comply with mandatory international coordination, notification and governance frameworks under the International Telecommunication Union. Unlike terrestrial telecommunications networks, which are typically subject to limited cross-border coordination confined to border areas, satellite systems operate at a global scale and are subject to ITU processes that apply worldwide and can involve multilateral coordination for both spectrum and orbital resources.

Network architecture

Satellite broadband

In current LEO satellite networks delivering broadband to premises, end-user earth stations take the form of consumer or enterprise kits that receive signals from the satellite and generate a Wi-Fi connection, enabling user devices to access broadband services. Signals are transmitted from the earth station to the satellite and then onward to a gateway.

Figure 4
Basic satellite communication architecture: uplink and downlink links

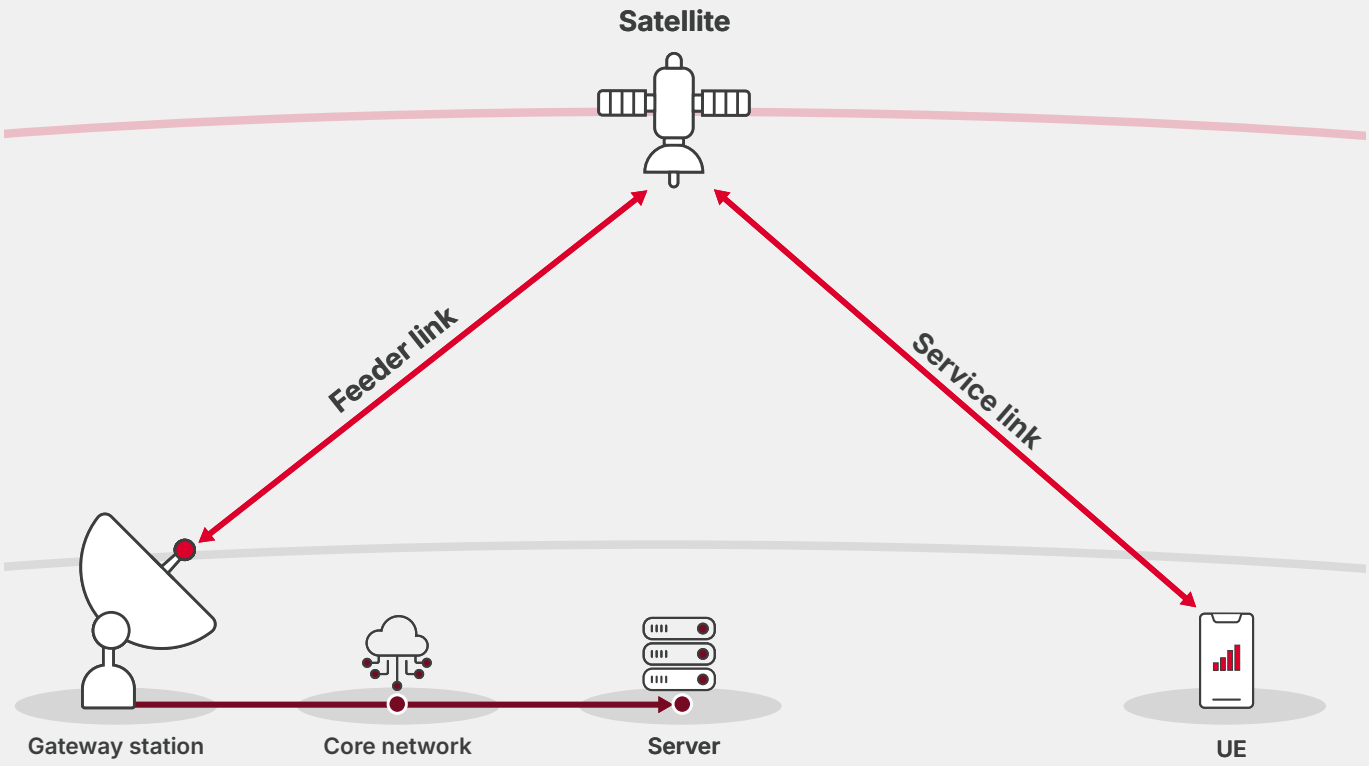


Source: Access Partnership

D2D

In a D2D setup, the earth stations are the mobile devices themselves. The figure below illustrates a typical satellite direct-to-device network architecture.

Figure 5
D2D architecture



Source: Access Partnership

GSMA

GSMA Head Office
1 Angel Lane,
London,
EC4R 3AB,
United Kingdom