

AIOTI Feedback on the Digital Networks Act

AIOTI welcomes the European Commission's Digital Networks Act and supports its objective of strengthening Europe's competitiveness, resilience and technological sovereignty. AIOTI recognises the strategic importance of a robust, secure and future-proof digital connectivity infrastructure as a fundamental enabler of Europe's economic growth, innovation and digital transformation.

Challenge of trusted suppliers and cybersecurity

AIOTI supports greater harmonisation of cybersecurity requirements across the EU. Security requirements should be based on objective, technology-neutral and risk-based criteria, supported by EU-wide standards, certification, and independent verification.

Trust in technologies and suppliers should be based on verifiable facts and internationally recognised security standards. Any restrictions or exclusion of suppliers should address a genuine, present and sufficiently serious security risk, based on transparent and evidence-based assessments.

A proportionate and harmonised approach would strengthen security while avoiding unnecessary barriers to innovation, competition and investment. Measures should also remain consistent with applicable EU and international legal obligations.

Security standards for end-to-end connectivity

Europe should promote common and interoperable security standards across the full digital connectivity chain, including connectivity between field devices and edge gateways in locally controlled networks using spectrum under general authorisation. These connections should remain fully integrated into end-to-end edge-cloud security, assurance and lifecycle-management frameworks.

We encourage stronger European engagement in international standardisation organisations and greater EU participation in the development of global standards. Building internationally recognised standards will support interoperability, avoid regulatory fragmentation and enable European companies to remain competitive globally.

The Digital Networks Act should therefore promote a risk-based, technology-neutral and standards-driven approach across the full connectivity chain. Any claim concerning security, interoperability or spectrum-resource efficiency that is relied upon for regulatory compliance must be substantiated through a common, transparent and reproducible assessment method set out in a recognised standard or technical specification, or through an equivalent independently verifiable method pending standardisation. Where a claim is relied upon to demonstrate compliance with Article 20(2)(b) or (d), competent authorities should be able to require the underlying evidence and supervise compliance under Article 196.

Architecture neutrality for distributed IoT sensing

AIOTI supports the Digital Networks Act's ambition for advanced 5G and 6G connectivity. A horizontal Digital Networks Act should also operationalise technology and service neutrality across public provider-managed networks, private managed cellular networks and low-power networks using spectrum under general authorisation. These architectures serve different and complementary requirements.

Many industrial, infrastructure, agricultural and environmental applications transmit small, intermittent sensor payloads from long-lived devices and do not inherently require broadband or a public mobile core. A fit-for-purpose architecture may combine low-power field sensing and edge aggregation with 5G/6G, fixed or satellite connectivity for orchestration and backhaul. The Union radio spectrum strategy should recognise this layered model.

Spectrum under general authorisation and locally controlled networks

Harmonised sub-GHz short-range-device spectrum, where made available on a non-exclusive basis under general authorisation and subject to applicable harmonized technical conditions, is a connectivity resource in its own right. It enables distributed sensing and telemetry over locally controlled or provider-managed low-power networks while remaining subject to applicable harmonised conditions on power, duty-cycle[FK2.1], channel-access, interference-mitigation and emission conditions

For non-public deployments, this model supports operational autonomy, local lifecycle control and deployment independent of public-network rollout without requiring a particular provider or subscription model. It complements managed services, public network backhaul and private 5G, which remain appropriate where managed quality of service, mobility, determinism or higher data volumes are required.

Measuring efficient use in shared spectrum

Different waveform designs can use shared spectrum differently for the same communication task. In managed networks, a central coordinator can schedule transmissions; in non-exclusive spectrum under general authorisation, independent networks share the band without a common scheduler. Duty-cycle compliance is therefore necessary but insufficient: airtime alone shows neither the useful information delivered nor the resource made unavailable to others.

For packet services, a first-order indicator should measure the occupied bandwidth multiplied by the cumulative transmission time required to deliver a defined application payload by a deadline. For waveforms using time and frequency diversity, the bandwidth-time resource should be calculated as the sum of the occupied bandwidth and duration of each individual emission. It should not be calculated from the overall frequency span between emissions, from the nominal spectrum allocation, or from a channel bandwidth that is not simultaneously occupied. It should include signalling, overhead, repetitions, retransmissions and failed attempts and report the result per successfully delivered useful bit or message. Successful delivery should be assessed at application level under a common service profile, without mandating a particular acknowledgement, repetition or retransmission mechanism.

The wider coexistence assessment should then relate successful delivery under common reliability, latency, coverage, density, load and interference conditions to the complete frequency-space-time footprint, including spatial reuse, protection areas, receiver blocking and adjacent-channel effects. This two-stage method would operationalise Article 20(2)(b) for shared bands on a technology-neutral, outcome-based basis.

Reference profiles may include secure lifecycle traffic such as configuration, credential rotation and vulnerability remediation. This can support CRA and NIS2 objectives without implying that either law mandates wireless FOTA or that full firmware images are suitable for every low-throughput use case.

Common assessment principles should guide CEPT and ETSI work and, where appropriate, be reflected in Article 17(3) roadmaps, harmonisation under Decision No 676/2002/EC and Article 22 conditions, with proportionate supervision under Article 196.

R&D and commercial deployment

- Preserve spectrum access for high-risk R&D and experimentation.

The DNA's efforts to harmonise spectrum management and promote more efficient spectrum use are welcome. However, spectrum policy should not be driven exclusively by commercial deployment and short-term economic utilisation. Spectrum is also a strategic resource for high-risk R&D, particularly for emerging technologies such as 6G, integrated sensing and communications, NTN and AI-enabled spectrum management. The DNA should therefore preserve flexible and proportionate mechanisms for experimental spectrum access, including experimental licences, spectrum sharing and regulatory sandboxes accessible to RTOs, universities and SMEs. European competitiveness depends not only on scaling existing technologies, but also on maintaining the capacity to experiment with technologies whose commercial potential is still uncertain.

- Recognise RTOs and technology infrastructures as strategic actors for future networks.

The DNA rightly prioritises investment, deployment and industrial competitiveness, but Europe's connectivity ecosystem should not be considered only through the perspective of operators and commercial technology providers. RTOs, testbeds and Technology Infrastructures provide the bridge between research and industrial deployment, allowing emerging technologies to be developed, integrated and validated under realistic conditions. The DNA should recognise these actors within the European connectivity ecosystem and ensure their participation in relevant governance and consultation mechanisms. Regulatory conditions concerning spectrum, network access and experimentation should facilitate rather than constrain high-risk R&D. Long-term European competitiveness requires both the capacity to scale today's technologies and the research capacity to create tomorrow's.

Regulatory delivery through the DNA

Recital 91. Alongside next-generation 6G wireless broadband, the first Union radio spectrum strategy should cover spectrum under general authorisation, public and non-public networks, user-controlled deployments, and low-power, low-data-rate wide-area M2M and IoT connectivity in rural, remote and industrial environments.

Article 17(2). The existing reference to sensing should be operationalised by requiring the strategy and roadmaps to address low-power distributed sensing and telemetry as a distinct deployment context, including harmonised sub-GHz spectrum under general authorisation and networks operated by end users for their own connectivity needs.

Efficient-use condition. A new Article 20(3) should operationalise Article 20(2)(b) for spectrum used on a non-exclusive basis under general authorisation through common, technology-neutral resource-efficiency and coexistence criteria. Under common service profiles, the framework should measure the occupied bandwidth multiplied by the cumulative transmission time required to complete a defined application or lifecycle task, including signalling, overhead, repetitions, retransmissions and failed attempts, and assess the wider frequency-space-time resource denied or materially impaired for others. For transmission schemes using time and frequency diversity, the relevant resource measure should be the sum of the bandwidth-time occupation of individual emissions, rather than the overall frequency span between emissions or the nominal bandwidth of an available channel.[FK4.1] Successful completion should be determined at application level under common service profiles and should not require a particular acknowledgement, retransmission or network-control mechanism. Airtime alone should not satisfy the assessment. The criteria should govern eligibility to use the relevant spectrum, not access to the product market. Any solution demonstrating the common service outcome within the permissible resource and coexistence envelope, and meeting all other applicable conditions, should remain eligible; among compliant solutions, market participants remain free to choose, including on the basis of greater verified useful effect from the same resource.

Article 22. Common authorisation conditions should preserve the ability of end users to deploy and operate non-public networks for their own connectivity needs, subject to harmonised technical conditions and without prescribing a particular provider or service model.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating AI, IoT and Edge Continuum Innovation in Europe, bringing together small and large companies, academia, researchers, policy makers, end-users and representatives of society in an end-to-end approach. We strive to leverage, share and promote best practices in the AI, IoT and Edge Continuum ecosystems, be a one-stop point of information to our members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of the AI, IoT and Edge Continuum Innovation in society. AIOTI contributions go beyond technology and address horizontal elements across application domains, such as matchmaking and stimulating cooperation by creating joint research roadmaps, defining policies and driving the convergence of standards and interoperability.