GSMA

Position Paper on the European Union Digital Networks Act proposal

April 2026

GSMA

Executive Summary

Europe's connectivity infrastructure lags behind global 5G leaders in the Gulf, East Asia and North America and the European regulatory framework for telecommunications needs urgent and extensive reform. Without significant and rapid change, Europe will be unable to deliver the best-in-class networks on which its competitiveness, security and resilience aspirations depend.

The proposed European Union Digital Networks Act ("DNA") represents a welcome acknowledgement of this situation, but in its current form it does not yet deliver the step change required to strengthen investment, innovation and competitiveness. The DNA contains positive elements, such as the legal form of the proposal, and most notably on spectrum, but it needs to do much more to support innovation and regulatory simplification. As it stands, the proposal fails to tackle regulatory asymmetries or to deliver necessary incentives for essential network investments. The draft lacks the ambition required to deliver European competitiveness and technological leadership.

New spectrum framework should take effect as soon as possible

The DNA proposals on spectrum reform offer Europe an opportunity to secure long-term connectivity goals. Indefinite licences (or very long licences of at least 40 years) together with automatic licence renewal can immediately tackle investment uncertainty. This will foster industry incentives to accelerate 5G standalone rollout and create the right conditions for early 6G planning. Moreover, it is essential that these principles apply to existing 3G and 4G licences without delay, allowing Europe to keep pace at a global scale and build a resilient digital future.

Need for greater simplification and focus on horizontal rules

The DNA proposal does not achieve genuine simplification. Consolidating several legislative instruments into a single Regulation, alone, does not reduce complexity if substantive obligations remain in place, new sector-specific requirements are added, and a large volume of secondary legislation, guidance and review mechanisms is introduced. In practice, the proposal risks increasing reporting, compliance and governance burdens on operators, contrary to the European Commission's wider simplification agenda. A more credible simplification effort would require the removal of duplicative and outdated rules, in particular in areas such as privacy, consumer protection, universal service and other end-user provisions that are already covered by horizontal legislation or no longer justified by market realities.

Similarly, the EU's resilience objectives should be addressed through the existing horizontal frameworks, rather than sector-specific rules. It is also misguided to link General Authorisation to expanded and as-yet undefined cybersecurity obligations, and risks introducing parallel enforcement tracks, duplicative assessments, and uncertainty as to regulatory competence. By adding yet another layer of sector-specific rules, this proposal undermines simplification and further exacerbates the uneven playing field.

Aim for consistent rules across the digital ecosystem

The DNA correctly identifies structural imbalances in the wider digital ecosystem, but it does not translate this diagnosis into meaningful corrective measures and does not apply the "same services, same rules" principle. Telecom operators would continue to face the most extensive regulatory, security, data protection and compliance obligations, while other digital actors with comparable services remain largely outside the scope of these obligations. This is particularly visible in the areas of General Authorisation, satellites, interconnection, ePrivacy and Open Internet rules in the DNA. For example, the core Open Internet principles should be modernised, simplified and extended to all key actors to reflect the evolution of networks and the growing provision of innovative and more customized services. At the same time, these principles should explicitly carve out B2B services to allow for bespoke contractual services for sophisticated parties and ensure consumers can benefit from innovative technologies like network slicing.

In summary, while the proposed DNA is a necessary step towards Europe achieving a best-in class connectivity ecosystem, it fails to address several major challenges. It needs to be redesigned so that it can revitalise the European telecoms sector, and enable the EU to meet its objectives for high performance connectivity, advanced digitisation, and greater competitiveness.

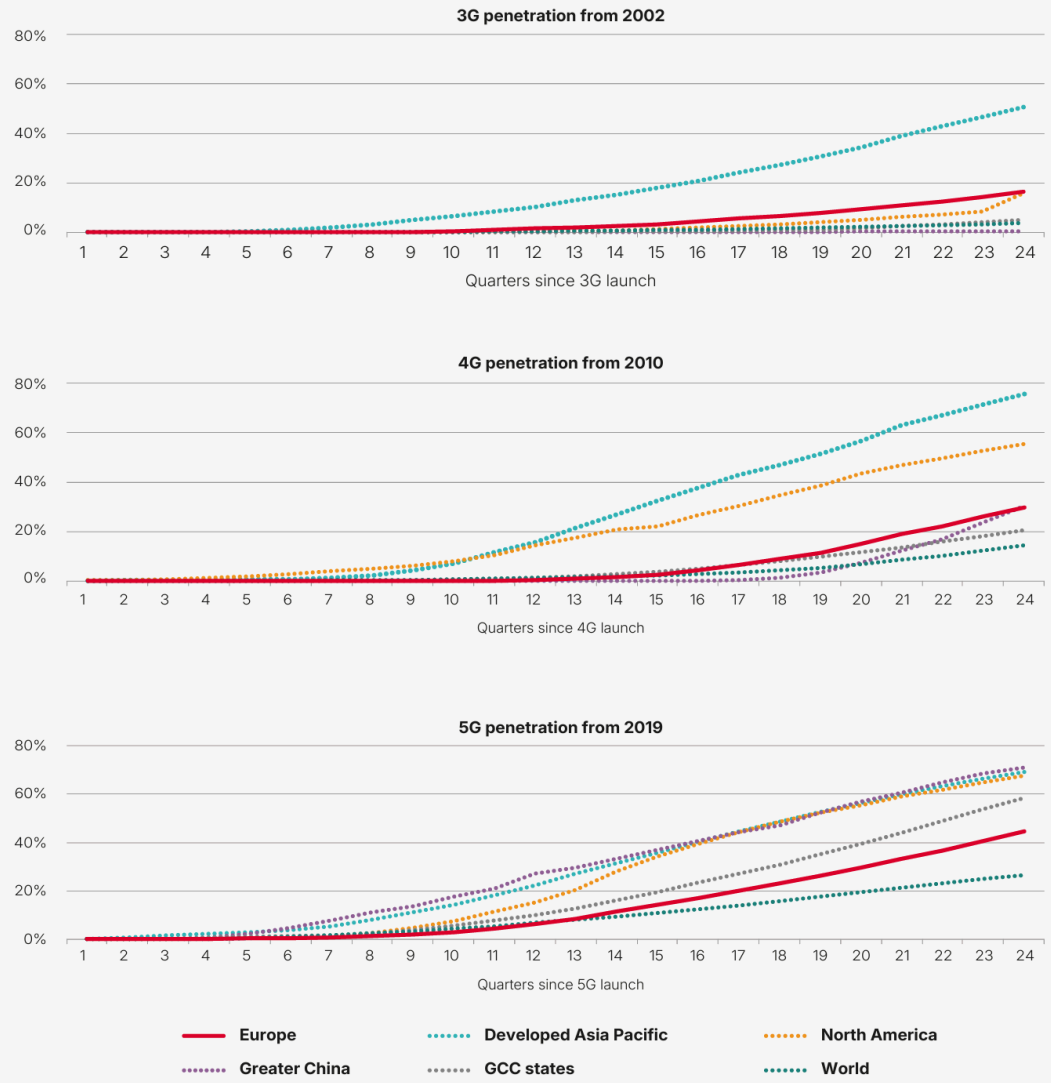
Introduction

Europe is behind the world's 5G leaders

High quality mobile connectivity is a key tenet of the EU's strategy to build a globally competitive digital economy. The EU Commission's 5G Action plan and the EU Digital Decade goals call for uninterrupted 5G broadband coverage for all urban areas and major roads and railways by 2025, and for all populated areas to be covered with 5G by 2030. The Commission has also stated that 5G should be at the core of new products, manufacturing processes and business models by the end of this decade.

Since 2015, mobile operators have invested €330 billion in Europe. Much of that has been spent on 5G, which was rolled out faster than any other generation before, and now covers more than 90% of Europe's population. In terms of adoption, 5G penetration in Europe has reached 45%. But most European countries are lagging global 5G leaders in the Gulf, East Asia and North America. The evidence also shows that the utilisation of 5G Standalone (which is needed to unlock 5G use cases) is lower in Europe compared to the leading regions, which means lower network quality and lower data usage.[1]

[1] *Spectrum Pricing and Renewals in Europe*, GSMA, December 2025, https://www.gsma.com/connectivity-for-good/spectrum/gsma_resources/spectrum-pricing-and-renewals-in-europe/

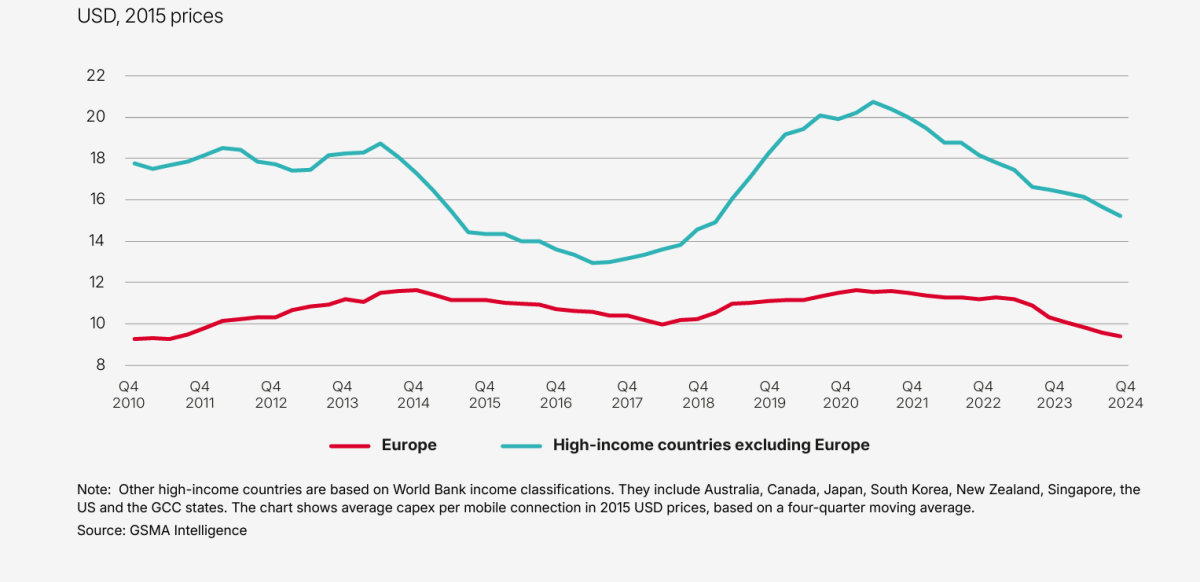


Penetration is calculated by dividing connections by total population. A 3G/4G/5G connection is defined as a 3G/4G/5G SIM card (or phone number, where SIM cards are not used) that has been registered on the mobile network at the end of the period. Connections differ from subscribers in that a unique subscriber can have multiple connections.

Source: GSMA Intelligence

The reasons for this are clear – most of Europe has lower network investment per subscriber than in other high-income countries. This is caused by a vicious cycle – ARPUs in Europe are much lower, which means lower returns on investment and therefore lower investment per user. Breaking out of this will require policy reforms that allows operators to improve their ability and incentive to invest and innovate, as well as enabling them to more effectively monetise their investments.

The DNA provides Europe with an opportunity to address the aspects of policy and regulation that have inhibited greater investment and innovation and hampered the continent's digital progress.



Note: Other high-income countries are based on World Bank income classifications. They include Australia, Canada, Japan, South Korea, New Zealand, Singapore, the US and the GCC states. The chart shows average capex per mobile connection in 2015 USD prices, based on a four-quarter moving average.

Source: GSMA Intelligence

Spectrum

The DNA proposals on spectrum are welcome and should be implemented without delay. If adopted in their current form with minor improvements, the DNA provisions on spectrum can support investment predictability, encourage direct investment, and strengthen the region's connectivity infrastructure, supporting industry efforts to make mobile networks more robust, secure and sustainable.

License duration and renewals

The spectrum proposals set out in the DNA can help reset licensing practices to support long-term mobile connectivity outcomes. The move towards indefinite-by-default or minimum 40-year licences across the EU, as detailed in Article 24, would significantly benefit the continent's digital infrastructure and economic competitiveness.

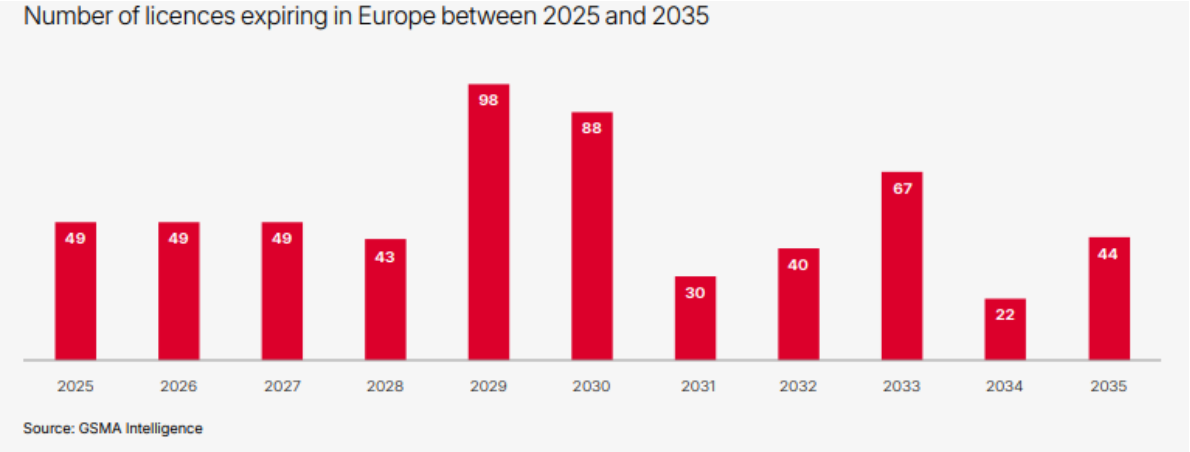
Mobile networks need constant upgrades and investment to support new services and use cases, and to continue to deliver high quality performance for consumers. Indefinite (or 40-year minimum) licence terms give operators the legal certainty and regulatory predictability they need to invest and innovate over time, which helps to meet growing consumer and business demand. Increased predictability across spectrum holdings allows operators to plan and make investments based on what their networks really need, instead of being constrained by artificial rules driven by the expiry dates of licences.

The DNA provides a robust framework to ensure indefinite or very long-term spectrum licences remain responsive to evolving market dynamics and technological changes over time, safeguarding the efficient use of spectrum as a scarce resource, and innovation by all players in the ecosystem. This is achieved through a combination of:

- Market-based mechanisms, notably the strengthening of the secondary market (Article 26), where the redistribution of spectrum is enabled through commercial agreements;

- Regulatory measures, including periodic reviews; the possibility to revoke licences; and "use-it or share-it" requirements. Although regulatory safeguards are necessary, these must be proportionate in order to avoid undermining the positive effects of the proposals. In particular, any grounds for licence revocation and any competition-related obligations must be designed so as not to undermine legal certainty. Spectrum sharing requirements must remain market-driven, and based on operators' strategies and market demand, rather than being strictly prescribed in regulation; and
- The possibility to meet social connectivity goals by exchanging annual fees for commitments, upon request of the licence holder, based on a reimbursement rate set by National Competent Authorities.

The DNA proposal on automatic renewals detailed in Article 25 is also welcome. Nevertheless, the timing of such measures will be decisive; the DNA must not prolong the unpredictability impacting those expiring licenses, to avoid undermining the effectiveness of the reform.



At a time when Europe must accelerate 5G standalone deployment and prepare for 6G, preserving predictability and security of licence tenure is essential. The principles set out in the DNA (including indefinite or 40-year minimum, automatically-renewable licences) should therefore apply immediately upon the adoption, in a proportionate and legally secure manner, to all existing licences.

The transitional provision under Article 25(5), which would exclude licences expiring within seven years from the new renewal framework, risks significantly undermining the effectiveness of the reform – as it could leave over 50% of licences outside the enhanced renewal certainty introduced by the DNA.

Automatic low-cost renewals (in which renewal fees are set at zero instead of being tied to historic prices) could save up to €30 billion in spectrum costs over the next 10 years, improving the viability of further network investment.[2] This could increase network speeds by up to 23% and increase Europe's GDP by up to €75 billion in by 2035.

[2] Ibid.

Harnessing the Single Market

Under the DNA, spectrum management competencies will remain with Member States, with national administrations retaining primary decision-making authority to reflect local market conditions and policy priorities. In parallel, the DNA introduces targeted, pro-investment measures to support greater policy alignment, harnessing the effective functioning of the Single Market.

Firstly, recognising that high spectrum costs have constrained 5G rollouts in Europe, the European Commission will adopt a Recommendation on a common pricing methodology (covering both annual fees and reserve prices). Provided it is appropriately designed, in consultation with industry, this proposal has the potential to address high spectrum costs and to spur investment in Europe. Total spectrum costs in Europe have tripled over the past decade as a proportion of operator revenues, reaching around 8%.[3] In the same timeframe, since 2014, the revenue generated from each MHz unit of spectrum has declined by 54%. Prices paid by mobile operators have often been driven by non-market factors, including high reserve prices, excessive annual fees and auction designs that artificially restrict spectrum supply. A common methodology should therefore be designed to avoid any inflationary effects, prioritise pro-investment pricing, including enabling replacement of recurring spectrum fees with long-term commitments to support digital objectives.

Secondly, the DNA introduces a helpful mandatory review mechanism through a binding Single Market spectrum procedure (Article 31), covering both new assignments and renewals and replacing the existing peer review process. Under this framework, the European Commission, BEREC, and the RSPB (formerly RSPG) would be able to review and intervene where assignments conflict with internal market principles, including in relation to licence durations and certain market-shaping measures. This ex-ante review is a welcome step that can help address sub-optimal assignment approaches, which have hindered 5G rollouts in some countries.

Thirdly, the European Commission is potentially empowered to assign radio spectrum at Union level (Article 22), to promote pan-European services (this may include satellite and terrestrial services). However, such EU-wide assignment beyond satellite spectrum should be avoided. This proposal risks artificially increasing scarcity, leading to decreasing service quality in existing networks. It also risks discriminating against operators that are willing to enhance their existing networks by investing in a subset of EU markets. This would undermine investment predictability, drive up spectrum prices, and thus decrease mobile service quality.

Finally, the DNA strengthens spectrum governance by upgrading the Radio Spectrum Policy Group (“RSPG”) to the Radio Spectrum Policy Body (“RSPB”), supported by a secretariat within the Office for Digital Networks (“ODN”) which replaces the BEREC office. This change may be positive for overall spectrum policy, supported by increased expertise and resources.

[3] Ibid.

Spectrum roadmaps

Article 17 of the DNA (which we support) will introduce long-term spectrum roadmaps that are designed to be updated following each World Radiocommunication Conference ("WRC"). Importantly, these roadmaps will carry a binding status and the first of these roadmaps is anticipated to focus on the development and deployment of 6G technology.

GSMA's Vision 2040 study projects that mobile data usage per connection in Europe will further increase, while countries will require an average of 2-3 GHz of mid-band spectrum by 2035-2040.[4] Early clarity on future bands, including those relevant for 6G, such as upper 6 GHz, 7-8 GHz, and sub-700 MHz, enables operators to plan investment, develop ecosystems and engage in international harmonisation efforts, while providing clear direction on timing and policy objectives, consequently supporting predictability for investments.

Spectrum sharing

There is a strong shift towards spectrum sharing, with shared used of spectrum established as principle of spectrum management, as reflected in Articles 15 and 27. While sharing can be beneficial in specific circumstances, exclusive rights are key to maintaining spectrum value, giving operators the legal certainty they need to invest in long-term assets.

Voluntary sharing should therefore be the primary tool relied upon to promote the efficient use of spectrum. Market-based mechanisms enable targeted, voluntary sharing where it is technically feasible and economically justified. Mandatory sharing, by contrast, is insufficiently nuanced and, moreover, can oblige licence holders to disclose commercially sensitive information (such as re-farming plans, capacity forecasts and investment strategies) simply to demonstrate why sharing is not feasible.

Consequently, any sharing framework should be proportionate, based on clear and objective criteria, and grounded in commercial agreements. It should be limited to situations of clear and lasting underuse, where there is a proven risk of inefficient use and increased opportunity cost. Sharing frameworks must also preserve the rights of the primary licence holder, granting mobile operators protection against interference from secondary users and allowing them to deploy whenever and wherever needed.

Moreover, the sharing requirement is understood to be predicated on the move towards indefinite licences. If the provisions on licence duration are weakened during the course of the legislative process, the sharing requirements should also be reconsidered.

Finally, the EU-level database to support spectrum sharing will need to be amended to better consider privacy, confidentiality and national security aspects linked to mobile networks. The EU-level database to support spectrum sharing will need to consider privacy, confidentiality and national security aspects linked to mobile networks.

---

[4] *Vision 2040: Future Spectrum Needs*, GSMA, November 2025, https://www.gsma.com/connectivity-for-good/spectrum/gsma_resources/vision-2040-future-spectrum-needs/

Spectrum-related market shaping measures

The proposed clarification of conditions for wholesale obligations and set-asides for new entrants are to be welcomed. Market-shaping measures must nevertheless be strictly limited to exceptional cases and subject to effective scrutiny. In the past, national measures have been imposed despite strong competition, adding unnecessary burdens and, at times, leading to unsustainable outcomes. Clearer guidance from the European Commission is therefore needed.

Policy recommendations:

- Co-legislators should embrace the European Commission proposals on spectrum management, especially on licence duration and renewal, which are balanced and investment-friendly.
- The proposed principles on automatic renewal should apply to existing licences to avoid a situation in which hundreds of licences expire across Europe during the negotiation and implementation period for the DNA.
- A more proportionate approach must be taken to spectrum sharing. Spectrum sharing should only be mandated in the DNA to the extent that indefinite licences are also mandated.

Simplification

Complexity instead of simplification

The DNA represents an important step in telecommunications policy, by proposing a directly applicable Regulation and aiming to reduce fragmentation and so-called "gold-plating" across Member States. Unfortunately, it falls short of delivering genuine simplification of the regulatory framework. Combining four laws into one without noticeable reduction of regulatory obligations is not simplification. Additionally, through the DNA the European Commission introduces numerous pieces of secondary legislation or guidance, which will add additional layers of regulation on top of the DNA framework after adoption. This creates legal uncertainty in the meanwhile.

The proposed DNA is therefore at odds with the European Commission's stated target to cut red tape in the 2024-2029 legislative mandate by a value measure of €37 billion (25% at EU level). It conflicts with the intention expressed in the June 2025 Call for Evidence on the Digital Networks Act to "reduce existing reporting obligations (up to 50%) and to remove unnecessary regulatory burdens",[5] as well as the stated objective of limiting the use of implementing and delegated acts to technical definitions.[6]

[5] See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14709-Digital-Networks-Act_en

[6] Statement by President von der Leyen with President Costa following the informal EU leaders' retreat, 12 February 2026, https://ec.europa.eu/commission/presscorner/detail/en/statement_26_405

Operators need legally and economically viable conditions if they want to offer cross border services without undermining investment incentives for infrastructure (i.e., 5G and fibre networks). Regulatory interventions that would force providers into offering cross-border services or would *de facto* result in a form of access regulation would have the opposite effect to incentives for investment. Consequently, the EU should refrain from introducing new obligations or measures such as "Harmonised access products" which, we believe, would be unjustified and disproportionate, and could also create more favourable conditions for non-EU providers, to the detriment of European investing operators.

Although the European Commission signals an intention to reduce reporting obligations, this effort is narrow, falls short of the "up to 50%" goal and is clearly offset by new sector-specific requirements, in areas such as sustainability (Article 115), resilience (Article 6), fraud prevention (Article 103) and Open Internet (Article 94) which in fact impose extended reporting, more monitoring, and additional governance layers.

The DNA introduces a significant number of additional requirements, including BEREC guidelines, which is unnecessary where clear regulation is set out in the DNA. Similar approaches have been taken in areas such as voluntary conciliation and Open Internet, and risk introducing additional complexity for operators.

Moreover, in key areas where simplification was expected, such as the removal of duplicative consumer protection and ePrivacy rules already covered by horizontal legislation (e.g. data protection, incident reporting, requirements towards contracts), phase out of the Universal Service Obligations ("USO"), the reassessment of obligations ill-suited to business markets, and a more material streamlining of end-user provisions (in Articles 95 to 102, for example, the DNA still applies consumer-related provisions to the B2B market), remain largely unaddressed. These are described in detail in the relevant sections below.

Overall, the DNA will increase complexity and bureaucracy rather than reduce it, missing the opportunity to make a balanced framework supporting investment, innovation and competitiveness at a time when regulatory burden is heavily constraining Europe's connectivity sector.

Level playing field considerations

The DNA proposal recognises the fundamental evolution of the communications ecosystem and the resulting and the structural imbalance in today's connectivity ecosystem, where EU telecom operators are subject to significantly stricter regulatory, security and compliance obligations than other digital actors offering equivalent or competing communications services. At the level of Objectives (in Article 3) and Recitals (in particular in Recitals 2 and 16), the proposal acknowledges the need for a fairer and more balanced relationship across the digital value chain, as well as the growing role of large content and application providers ("CAPs"), cloud providers and related intermediaries in shaping traffic flows, network usage and user experience.

However, this approach is not translated into binding, obligations on other digital players according to the "same service, same rules" principle. In particular, the DNA does not introduce enforceable responsibilities regarding interconnection, traffic generation or the material influence exercised over quality of service and network performance. For example, in Article 9, Number Independent Interpersonal

Communication Services ("NIICS") are explicitly excluded from the scope of the General Authorisation, and the Open internet rules are not extended to other digital players that impact traffic routing. In addition, Articles 191 and 193 propose an ecosystem conciliation mechanism that is voluntary and without binding obligations and which, as described further below, is therefore ineffective.

As a result, a longstanding imbalance persists. Telecom operators continue to face extensive regulatory requirements that are not borne equally by other powerful actors in the ecosystem, and are commercially disadvantaged as a result.

Policy recommendations:

- Streamline duplicative and outdated rules and rely on horizontal frameworks where available to achieve true simplification (e.g., ePrivacy, consumer protection, USO)
- Avoid introducing new reporting requirements (e.g., fraud, resilience, net neutrality)

Open Internet Rules

Modernisation needed

Europe's Open Internet Regulation ("OIR") was adopted in 2015, in a fundamentally different technological and market context compared to the present day. At the time, 5G and fibre networks had not yet been deployed, and advanced use cases requiring guaranteed performance, ultra-low latency or differentiated quality of service were largely theoretical. The OIR was therefore designed for an earlier world, focused on first generation data connectivity and a relatively simple internet ecosystem.

A decade on, the European Commission has chosen to "copy paste" the existing articles of the OIR within the proposed DNA in Article 93. In doing this, the DNA fails to address the structural misalignment between outdated rules and today's network capabilities. Even worse, it perpetuates these shortcomings for another decade.

In today's markets, to preserve the aim and the spirit of the original net neutrality rules, while at the same time enjoying new capabilities of advanced 5G and fibre networks changes in their form and extent are necessary. The Open Internet rules should provide enhanced legal certainty for innovative services based on network slicing and allow for differentiated and assured quality of service. Therefore, clear and prompt guidance such as a Recommendation from the European Commission is needed immediately – pre-empting the DNA – presenting a non-exhaustive list of services that should be considered as permitted "specialised services".

The DNA should encourage the broad adoption of advanced technologies such as networking slicing and encourage consumer choice. This requires updating the provisions around traffic management, differentiated quality of services, and services other than internet access services.

As such, Open Internet rules must be modernised, keeping the consumer at its centre, while being adapted to reflect the evolution of networks and the growing provision of innovative and more customised services. Without such operational flexibility, network quality, resilience and innovation will suffer – ultimately harming users. Additionally, in the interests of regulatory simplification, the reporting obligation set out in Article 94 of the DNA should be removed.

Focus on non-discrimination for consumers while acknowledging network evolution

For consumer markets, the Open Internet rules should be simplified and refocused around their core objective: preventing harmful discrimination that undermines user choice or competition. The current framework is overly-prescriptive and complex. It is also based on assumptions that no longer reflect how modern networks operate, either today or in the near future. Electronic communication networks are undergoing major transformation as they rely more and more on software, cloud, network slicing, and AI. All those evolutions impact the way networks are managed, for the benefit of all, as they allow operators to develop more customised offers to meet customer demand. Modern networks must manage exponentially growing traffic volumes, diverse application requirements, and increasingly asymmetric traffic patterns.

The DNA should choose a principles-based approach, centred on non-discrimination, transparency, and user control in the provision of internet access services. This would provide stronger and more durable consumer protection than rigid, technology specific rules. It would also give operators the flexibility required to manage increasingly complex networks efficiently and responsibly. In practical terms, this means granting more choice to consumers via more flexible traffic management rules. Enabling differentiation would deliver better network performance without undermining Open Internet principles; rather, it would help ensure that consumers continue to receive high-quality connectivity as demand grows and use cases diversify.

Exclude B2B services

The OIR was designed first and foremost to protect consumers in retail internet access markets. However, its current scope applies to all “end users”, inadvertently capturing a wide range of business-to-business (“B2B”) services that are fundamentally different in nature and purpose from consumer internet access. This overbroad application has become a significant barrier to innovation and investment in enterprise connectivity.

The DNA should therefore modernise the scope of the Open Internet rules so that they apply explicitly to consumers, but carve out B2B services. This distinction is critical to ensure that consumer focused protections do not unintentionally constrain bespoke contractual services delivered between sophisticated parties. In bespoke B2B contracts, transparency, performance guarantees, and remedies are negotiated commercially. However, smaller businesses or NGOs using standardised contracts would continue to be covered by the Open Internet rules.

Extend the core OIR principles to all key actors

Modernization of the Open Internet principles implies that they apply, not only to traditional providers of Internet Access Services ("IAS"), but also to other relevant digital service providers with influence over the quality of experience and traffic management.

Policy recommendations:

- Allow greater flexibility for traffic management, differentiated quality of service and freedom of choice for B2C services
- Exclude B2B services from scope.
- Extend core OIR principles to relevant actors in the value chain
- Clear and prompt guidance from the European Commission on innovative specialised services

Satellite

Many satellite networks and services are cross-border by nature. Satellite connectivity can offer a useful complement to terrestrial mobile networks and help extend the coverage of mobile networks to areas of low population density and also add resilience.[7] The proposed introduction of harmonised and centralised authorisation of satellite networks, services and spectrum signals an important shift toward EU-level regulatory coordination.

Harmonised processes can reduce fragmentation and lower administrative burdens. They can therefore support pan-European satellite connectivity provision and deliver a more coordinated and comprehensive management of those networks in the EU.

Nevertheless, while the DNA demonstrates a commendable intention to create balanced market conditions between different connectivity providers, it does not fully deliver on the principle of "same service, same rules". Achieving regulatory parity for services being provided directly to end users requires more explicit and consistent provisions than those set out in Article 38, which establishes an EU-level general authorisation framework for satellite systems, to ensure that comparable services are subject to comparable regulatory treatment.

Many of the complex regulatory requirements typically faced by telecom operators, such as obligations related to security or access to data (lawful intercept and data retention), are not fully harmonised under the proposed DNA framework and may therefore not apply in the same way, or at all, to all end-to-end communications service providers across all EU Member States.

[7] *The Limits of D2D,* GSMA, February 2026 https://www.gsma.com/connectivity-for-good/spectrum/gsma_resources/the-limits-of-d2d/

Regulatory parity is essential to ensure that customers receive the same level of protection when they buy the same type of services, and that societal outcomes are not weakened as new communication delivery models emerge. Where satellite and telecom operators provide functionally equivalent, direct-to-user services, obligations should be aligned in effect, support fair competition, clear accountability and long-term investment certainty.

Technical and regulatory measures must guarantee that satellite operations do not cause harmful interference to terrestrial networks, if introducing satellite direct-to-device services in mobile bands.[8] Article 45, which stipulates that shared use of radio spectrum between terrestrial and satellite systems must only be allowed with the explicit agreement of the primary holder of terrestrial rights, is important and must be preserved throughout the legislative process.

This approach supports efficient spectrum use, safeguards current and future mobile network development, and ensures that the licence holder retains accountability for interference management and regulatory compliance.

Finally, it must be noted that Recital 97 raises some concerns. It includes an indication that terrestrial spectrum could be repurposed for satellite use, which raises concerns for the mobile industry, as this could constrain both the continuity and the evolution of mobile services providing essential services to the whole European society. There should be clearer recognition in the DNA of the need to ensure certainty of access to terrestrial spectrum for mobile network operators.

Policy recommendations:

- Secure adoption of European Commission proposal on EU-level authorisation for satellite spectrum and safeguard mobile network operators' access to spectrum
- Ensure "same service, same rules" for satellite providers and mobile networks operators
- Safeguard mobile network operators' access to spectrum, including by requiring the explicit consent of the primary holder of terrestrial rights to the shared use of radio spectrum between terrestrial and satellite systems

Conciliation Mechanism

Addressing imbalances in the connectivity ecosystem

The connectivity ecosystem is characterised by persistent asymmetries in bargaining power and cost allocation. Telecom operators finance, build and operate networks that support continued traffic growth - significant both in mobile and fixed networks. In contrast, the largest traffic generators operate global private backbone and delivery

[8] *Spectrum for D2D,* GSMA, September 2025 https://www.gsma.com/connectivity-for-good/spectrum/gsma_resources/spectrum-for-d2d-public-policy-paper/

networks and account for over 70% of the world's total internet traffic but contribute little or nothing to the costs of data transport.[9] Operators face limited ability to negotiate fair commercial terms for IP interconnection and data transport.

This unjustified imbalance weakens investment incentives, risks undermining network quality and endangers the attainment green transition and resilience goals. It ultimately jeopardises Europe's competitiveness and ability to meet its connectivity, sustainability and industrial policy objectives.

DNA: recognition without a bold correction

The DNA acknowledges the growing role of large traffic generators in driving traffic growth and recognises the resulting pressures on network infrastructure (see Recitals 2 and 15). However, the proposal falls short of establishing binding obligations for these actors.

By leaving the issue of structural bargaining asymmetries unresolved, the proposal risks perpetuating the very investment constraints that threaten Europe's Digital Decade ambitions. This is particularly problematic given the DNA's broader objectives of market integration and competitiveness.

In particular, the DNA does not introduce enforceable responsibilities regarding traffic generation or any duty to negotiate fair and reasonable terms for interconnection and IP data transport. Instead, it relies purely on a voluntary conciliation mechanism (Article 191-193). This mechanism does not correct the underlying imbalance in negotiating power and does not provide the legal certainty needed to support sustained investment.

Therefore, co-legislators should introduce a mandatory, binding regime with obligations for large traffic generators to negotiate with telecom operators backed up with an efficient dispute resolution mechanism.

Moreover, the proposal in Article 191 that BEREC will issue guidance on facilitating ecosystem cooperation (covering matters such as the provision of economically sustainable and innovative products and services) should be abolished. It will further complexify the regime and increase uncertainty, without addressing the persistent underlying asymmetry. The role of a conciliation mechanism should be limited to asymmetric negotiations on interconnection, IP data transport and data traffic optimisation.

Policy recommendations:

- Obligation for large traffic generators to negotiate with operators, backed up by a mandatory, binding dispute resolution mechanism
- European Commission to be preferred over BEREC as the body designated to issue any guidance on dispute resolution related to interconnection and IP data transport

[9] *The State of the Network*, Karlson, 2024

End-user Rights and Universal Service Obligations

As noted above, the simplification goals of the European Commission in 2024-2029 demand that additional changes be made to the proposed DNA, as regards end-user rights, USO, and privacy. In addition, changes are strongly desirable in fields such as fraud and emergency calls.

Connectivity and End-Users

Connectivity plays a vital role in enabling European consumers and businesses to participate fully in the digital economy, stay informed, and access essential services - contributing directly to the continent's economic growth and social inclusion.

The horizontal EU consumer and end-user policy framework already establishes the conditions that allow end-users to make informed choices, drive demand for high-quality and sustainable services, and support innovation. It is one of the strongest horizontal frameworks in the world in terms of protecting end-users and consumers. End-users would benefit from the abolition of duplicative sector-specific rules in favour of one simplified, horizontal framework that ensures fairness, transparency, and legal certainty across all digital services and across all EU Member States.

Strong end-user rights and regulatory reform can coexist

The current regulatory framework for telecommunications in the EU requires significant reform to better serve end-users and providers alike. While we commend the European Commission decision to propose a Regulation with a view to strengthening the Single Market and improving harmonisation by preventing fragmentation and national gold plating, the end-user provisions proposed in the draft DNA fall significantly short of the European Commission's political ambitions to improve the EU's competitiveness through simplification and harmonisation.

End-user rights (Article 95-102)

The consumer protection framework for telecommunications services at EU level is a complex mix of horizontal, sector-specific and national rules. In order to reduce unnecessary complexity and bureaucracy, the DNA should only maintain end-user rights that are fully justified and truly have an impact (the so-called "effect-based approach"). Unnecessary end-user rights without added value should be deleted from the DNA (the so-called "functional approach"). Thus, only a limited number of truly sector-specific and objectively justifiable provisions of the European Electronic Communications Code ("EECC") should remain in the DNA: namely, provider switching and number portability, and conditions related to the sale of bundles (Articles 98 and 100).[10] The DNA misses an opportunity to reduce decisively the excessive information obligations in the context of transparency of contracts (Articles 95-96), which overlaps with horizontal consumer directives.

[10] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

Similarly, the European Accessibility Act provisions on accessibility provide for sufficient coverage, which makes some of the proposed DNA provisions duplicative (Article 102).[11] In those cases, the draft DNA increases complexity and bureaucracy for providers without delivering clear added value for consumers. Furthermore, Member States are still allowed great discretion for gold-plating across the different provisions, which is contradictory to the overall harmonisation objective of the DNA.

In addition, the provisions of the EECC intended for the protection of consumers and small and medium-sized enterprises ("SMEs") should be strictly limited in scope. This is currently not the case, given some obligations apply to all B2B users. As such, the DNA should shift to a consumer protection framework that protects consumers by definition, with greater delineation between the rules applying to "end users" and those applying solely to "consumers". To support this, the European Commission should refine the definition of "end user" in accordance with these principles, focusing on truly sector specific provisions.

Universal service obligations (Articles 87-92)

Based on the current level of deployment and coverage of fixed, mobile and satellite networks, the USO mechanism is no longer justified to the extent it was more than 20 years ago. This is the case from the perspective of both availability and affordability. Today's markets feature a huge variety of offers that match the needs of consumers and ensure sufficiently wide connectivity to ensure social and economic participation in society. In addition to this, telecommunication prices in Europe have massively decreased over the last 20 years due to competition and technological progress.

To protect vulnerable citizens across the EU who struggle with affordability concerns or with closing remaining connectivity gaps, we consider that the most efficient way to address these issues is by targeted public intervention through the provision of direct subsidies such as vouchers, rather than an unclear mechanism like the USO in order to avoid unnecessary administrative effort and create only short-term and geographically isolated solutions.

Allowing Member States to introduce mandatory social tariffs would shift responsibility for social policy from governments to telecom providers. This would place disproportionate financial and administrative costs upon telecom operators whilst only delivering limited take-up of these tariffs. Moreover, the changes introduced in Articles 87-92, which allow Member States to impose obligations on availability, raise serious and proportionality concerns; they do not adequately address concerns of due process nor mention compensation to undertakings leading to significant legal uncertainty.

Emergency communications

Europe's operators will continue to enable citizens to reach emergency services across the EU. It is, however, long overdue that emergency calling obligations should be extended equally to so-called over-the-top players, in order to future-proof the 112-emergency calling system. Moreover, new obligations (such as Article 106) appear to lead to additional regulatory burdens and costs falling solely on the telecom sector.

[11] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services

Fraud (Article 103)

While the GSMA fully supports the objective of protecting end-users against fraudulent activities, the measures proposed in the DNA fail to provide the most effective protection for end-users and a sufficiently targeted approach. Constantly evolving fraud risks cannot be effectively fought with rigid and overly prescriptive regulatory requirements. Instead, service providers should be empowered to address impersonation fraud with the most effective technical solutions available at a given point in time. In this regard, we commend making use of the platform approved in the newly agreed-upon Payment Services Regulation, which gathers all relevant stakeholders together to exchange on the most efficient ways to combat fraud.[12]

Importantly, the DNA should address long standing constraints in the ePrivacy Directive that limit operators' ability to deploy effective anti-fraud tools, as described further below.[13] Greater clarity on the General Data Protection Regulation ("GDPR") notion of "legitimate interest" and its interaction with the ePrivacy regime would be particularly helpful in this context (see below).[14] This will serve end-users best and drive innovative solutions.

ePrivacy

While the draft DNA (Article 207) rightly proposes the deletion of Articles 7, 8, 10, 11 and 12 of the ePrivacy Directive, it fails to put an end to the discriminatory situation faced by European telecom operators for the management of their traffic and location data.

Instead of repealing the 23-year-old ePrivacy Directive and regulating core principles such as the confidentiality of communications horizontally under the GDPR, many of the existing provisions remain applicable under the DNA. As a result, the telecommunications sector continues to be subject to significantly stricter requirements for the further processing of mobile traffic and location data (Articles 6 and 9) than large parts of the digital economy.

Over-the-Top providers ("OTTs") are able to use comparable data far more flexibly under the GDPR framework than licensed telecom operators can do under the ePrivacy Directive. This regulatory asymmetry is unjustified and entirely outdated in the age of digital communications. Consequently, these provisions should be repealed, to bring about a more level playing field between operators and other digital players, which are solely governed by the GDPR and to enable operators to effectively combat and prevent impersonation fraud.

---

[12] See https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees

[13] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Policy recommendations:

- Prioritise EU-wide horizontal rules, rather than sector-specific rules, to ensure strong and consistent consumer protection across the EU
- Residual and strictly necessary sector-specific rules (portability, switching, bundles) must be harmonised across Member States
- End-user rights should be refocused on consumers
- Withdraw USO and use public support instruments to address affordability issues for vulnerable users, where needed
- Extend the obligation to NIICS / OTTs to support emergency communication services and ensure new obligations remain balanced and proportionate across all actors
- Harmonise and streamline existing rules to fight fraud without adding overlapping or prescriptive measures
- Repeal the ePrivacy Directive, in particular Articles 6 and 9

General Authorisation

Context and policy objective

A genuinely integrated digital Single Market requires simple, predictable, and harmonised market-entry conditions for providers of electronic communications networks and services. We support the objective of reducing fragmentation and enhancing legal certainty and of maintaining light-touch authorisation which has long ensured competitive market entry across the EU.

Legislators should carefully review the minimum conditions attached to the General Authorisation ("GA") regime to ensure they remain targeted, proportionate, and clearly focused on market entry, and do not create undue burdens or asymmetries with functionally comparable providers, including satellite service providers.

Single Passport

The proposed Single Passport might ease the administrative process for operators present in several countries, but also raises questions regarding its enforcement and the possibility for Member States to impose specific obligations (Article 10.6).

In addition, on its own, the proposed Single Passport does not resolve the deeper structural fragmentation that providers continue to face once services are operational. Divergent national approaches to ongoing compliance, lawful interception, data localisation and national autonomy requirements, information requests, reporting obligations, and enforcement practices remain a significant barrier to cross-border operations and genuinely seamless EU-wide provision. These issues sit largely outside the scope of the GA / Single Passport regime and cannot be addressed through notification mechanisms alone.

For this reason, the Single Passport should be positioned as a procedural facilitation tool within the GA framework, rather than as a substitute for wider regulatory convergence in the DNA.

There is a balance to be struck between making the GA framework targeted and light-touch, with a genuine focus on market entry (as opposed to ongoing compliance), without creating incentives for a "race to the bottom" towards the jurisdiction with the lowest enforcement standards. This balance requires making it clear beyond doubt that national regulatory authorities ("NRAs") in the Member State where services are provided retain control over material assessment of legal obligations and effective supervisory and enforcement powers. It should therefore be clear that the GA framework should not result in the notified NRA assuming governance or enforcement competence for activities carried out in other Member States.

Additionally, the Single Passport regime should improve the existing GA regime rather than add complexity. To this end, the DNA should provide clear legal certainty that existing authorisations remain fully valid, are not subject to new or additional qualifying criteria, and allow authorised providers to make use of the General Authorisation or Single Passport without reopening or reassessing market-entry conditions.

The DNA proposal further increases bureaucracy by requiring an explicit confirmation of the responsible NRA before the services launch, which creates a new procedural element instead of removing them.

Link to Revised Cybersecurity Act

The DNA imports a requirement of compliance with the draft Revised Cybersecurity Act ("CSA2") into the GA regime (and also the general authorisation regime for the use of spectrum, Article 20). The proposed CSA2, which is in itself very far-reaching, has not yet been adopted as a legal text. To link two unfinalised legal texts in this way, as the basis of an authorisation regime, creates legal uncertainty for the telecommunications sector.

Moreover, it would expose telecoms operators to cumulative sanctions, including the loss of authorisation rights, in addition to penalties under the relevant horizontal framework. This would result in significantly stricter consequences for one sector, conflicting with the level playing field principles. The proposed link between the DNA and the CSA2 therefore risks duplicating obligations and introducing sector specific enforcement consequences for telecoms operators that do not apply elsewhere in the economy. This would undermine the CSA2's role as a horizontal, risk-based framework and create unnecessary and costly overlap between regulatory regimes. Rather than simplifying the regulatory landscape, this approach risks introducing parallel enforcement tracks, duplicative assessments, and uncertainty as to regulatory competence. The resulting complexity would increase compliance costs and administrative burden and reintroduce fragmentation at the point where greater coherence is most needed.

Level playing field considerations

Last but not least, the DNA is a chance to level the playing field by including the providers of NIICS into the GA scope. The DNA foresees the possibility of NIICS being obliged to comply with the obligations of network resilience, preparedness,

cybersecurity, lawful interception and data retention. From a customer's perspective, the services provided by them are increasingly seen as full substitutes to the traditional electronic communications. Therefore, including NIICS into the GA scope would be a natural step for a future-proof DNA.

Policy recommendations:

- Remove harmful interlinkages with the CSA2 and ensure that minimum conditions genuinely reflect the conditions needed for market entry.
- Include drafting which makes it explicit that nothing in Articles 9 and 10 impacts existing authorised operators across different Member States, and assumes their *de facto* compliance.
- Ensure NRAs in the Member State where services are provided retain effective supervisory and enforcement powers for those obligations.
- Include providers of NIICS into the GA scope.

Connectivity, Security and Resilience

The shared ambition of the telecommunications industry is to provide a trustworthy connectivity ecosystem. Telecom operators ensure strong network security and resilience through comprehensive technical, operational, and organisational measures. Building on evolving requirements, operators have developed comprehensive preparedness, security and resilience concepts and implemented them in coordination with their national authorities. These measures aim to ensure both the physical and digital protection of infrastructure and to reduce supply chain risks and dependences. It is by enabling investment that the DNA can most effectively support operators in further enhancing network resilience, allowing them to adapt to new risks and technological advances, and to maintain robust infrastructure.

While the European Commission's objectives of strengthening preparedness, security and resilience in Europe are laudable, the current DNA proposal would undermine this aim by introducing overlapping, top-down, sector-specific mechanisms and additional regulatory layers. In doing so, it disregards operators' expertise and operational realities, further complicating an already complex and burdensome framework. The proposal also establishes new EU-level security competences that overlap with national authorities, adding another layer of confusion.

The current draft DNA (Articles 4 to 8) overlaps with what is already addressed under the horizontal NIS2 Directive ("NIS2")[15] and Critical Entities Resilience Directive ("CER")[16] frameworks, for example anticipation, prevention and response to

[15] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

[16] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

disruptions (Article 4), service continuity obligations (Article 5), and preparedness planning, information gathering and crisis coordination (Articles 6–8) cover areas already addressed under NIS2 and CER. The NIS2 and CER frameworks already ensure a whole-value-chain perspective on security and resilience, preserves operators' autonomy, and allows flexibility in implementing effective measures. Competencies on security matters involving BEREC, ODN, and national authorities should be reviewed to eliminate overlap and confusion.

Moreover, the current proposal departs from the established horizontal frameworks under NIS2 and CER, adding complexity and diverging from their principles-based and cross-sectoral approach further creates significant uncertainty regarding the scope and potential mandate of the proposed *Union Digital Infrastructure Preparedness Plan*, to be developed by BEREC and ODN. The current text further conflicts with existing approaches taken toward the possible involvement of affected stakeholders in defining the most proportional measures to achieve the shared objective.

By increasing reporting obligations to a new security body, in highly sensitive areas, the proposal also signals a shift from the simplification narrative toward a prescriptive, top-down approach to resilience and security, rather than building on horizontal, risk-based, and operator-driven practices and expertise.

The proposal introduces provisions that blur the distinction between cooperation among national and European authorities and potential security obligations imposed on operators under the DNA at the European level. The proposal includes unachievably high standards, for example, with the requirement to ensure continuous or uninterrupted connectivity under any circumstances (Article 5) or to anticipate and prevent any natural disaster, crisis, or man-made disruption, going beyond the established responsibilities of private companies and diverging from the principles established under NIS2 and CER.

Moreover, the security and resilience framework introduces a requirement (Article 5.4) to submit a roadmap two years in advance of migrating from legacy technologies to authorities and end-users. This would add unnecessary documentation which, together with the preparatory measures, would slow down the rollout of next-generation networks and connectivity services.

All of this results in a proposal that is confusing, complex, disproportionate, and uncertain with respect to security and resilience obligations for network operators, disregarding NIS2, CER and national frameworks, network-specific characteristics, operators' views and a horizontal whole-value-chain perspective.

Given the existing security and resilience legal landscape, we question the added value of Articles 4 to 8 and the proposed *Union Preparedness Plan for Digital Infrastructures*, in addition to current cybersecurity and resilience rules. Any preparedness cooperation should remain non-prescriptive, avoid creating unfunded costs or liabilities for operators, and be fully aligned with existing EU and national crisis-management and cybersecurity frameworks, including NIS2 and CER. EU policymakers should engage with telecoms operators to ensure any potential legislative intervention truly fills a gap, preserves stakeholders' autonomy, and allows flexibility in implementing effective measures.

As foreseen in the NIS2 and CER frameworks, effective resilience policies should prioritise measures at critical network sites such as those supporting emergency response, essential public services, and key aggregation functions, rather than

imposing identical obligations across all telecom infrastructure. Not all telecom infrastructures face the same threats, nor do they play the same role in supporting essential services. Over-engineering the entire network diverts resources away from where redundancy is genuinely needed.

Policy recommendations:

- Security and resilience objectives should be addressed through existing horizontal frameworks, rather than sector-specific rules.
- Avoid introducing new reporting obligations for operators.

Cybersecurity

See joint paper "GSMA Europe and Connect Europe's views on the revised Cybersecurity Act (CSA2)", April 2026

Sustainability

The DNA's overall focus on modernisation, competitiveness, investment incentives, and the end-to-end approach to drive energy efficiency and reduce emissions is positive. These levers are essential for telecom networks to support the EU's sustainability goals. Additionally, we believe that data efficiency should be improved via better bandwidth usage, more advanced codecs, and by enabling data-saving mode as the default setting.

Additional sector-specific reporting requirements should be avoided. Telecom operators are already subject to a wide range of sustainability reporting obligations through the Corporate Sustainability Reporting Directive ("CSRD").[17] The CSRD relies on the publication of the transition plan, which is an ambitious exercise that addresses the issue of limiting Greenhouse gas emissions for companies. In addition, CSRD reports are already externally audited, and they will become easier to access and benchmark thanks to a new machine-readable format. The telecom sector has formed an Alliance that works to assess, audit, and improve sustainability performance of telecom operators' supply chains.[18] Concretely, the Alliance conducts joint supplier audits and promotes higher standards on human rights, environmental protection, and responsible sourcing in the ICT sector.

For these reasons, there is no justification for additional reporting. Moreover, adding parallel data-collection requirements to the DNA, for example via NRAs and/or BEREC, would run counter to the EU's simplification ("Omnibus") initiative, risk duplicating existing requirements, without helping operators improve environmental

[17] Directive (EU) 2022/2464

[18] The Joint Alliance for Corporate Social Responsibility (JAC), see https://jointallianceforcsr.org/

outcomes.[19] In addition, heterogenous requirements of NRAs risk inconsistencies between international subsidiaries of multi-national corporations. As a consequence, it will be more complicated for capital markets to benchmark corporate performance, which fully contradicts the intended transparency and may actually hinder carbon-friendly investments.

The DNA should therefore prioritise modernisation rather than expanding its scope into areas already governed by cross sector EU law.

Policy recommendations:

- Remove additional red tape in line with the European Commission's simplification agenda.

Numbering

The DNA has an important focus on coordination processes for the exterritorial use of national numbering resources, with specific awareness on machine-to-machine ("M2M") / Internet of Things ("IoT")-connectivity and M2M/IoT use cases (for example, in the automotive sector). This reflects market realities in which numbering has not historically been a structural bottleneck. It also preserves operators' ability to rely on commercial arrangements, including in the sphere of permanent roaming, without introducing additional regulatory burdens.

There are still opportunities to simplify the framework further, particularly by clearly excluding non-interpersonal M2M and IoT services from consumer-focused obligations and by reducing unnecessary regulatory complexity where numbering is used only for machine connectivity.

In addition, the impact of the proposed shared system for numbering, with the European Commission setting overall strategy and harmonised cross-border number ranges as well as numbering ranges for pan-European services, requires further analysis.

[19] Directive (EU) 2026/470 of the European Parliament and of the Council of 24 February 2026 amending Directives 2006/43/EC, 2013/34/EU, (EU) 2022/2464 and (EU) 2024/1760 as regards certain corporate sustainability reporting requirements and certain corporate sustainability due diligence requirements