# A SIMPLIFICATION AGENDA FOR EUROPEAN TELECOMS

Regulatory evolution to improve the Customer journey for a competitive & stronger Digital Single Market

*REPORT*

July 2025

ELISABETTA CAFFORIO
Partner, TIME
Rome

GREGORY PANKERT
Managing Partner, TIME
Brussels

PAUL DUMOULIN
Manager, TIME
Paris

PATRICK VERMAAK
Manager, TIME
Brussels

NICOLAS MENNIG
Business Analyst
Brussels

# TABLE OF CONTENTS

# LIST OF FIGURES AND TABLES

## Figures



## Tables

# EXECUTIVE SUMMARY

***The European digital economy is at a turning point. The ability of citizens and economies to innovate, improve productivity and create more opportunities for sustainable growth relies on significantly upgrading the digital infrastructure. As citizens and businesses demand high-performance and resilient connectivity, Europe's telecom regulation must evolve in line with the ambitions. This study specifically focuses on regulation impacting the customer journey highlighting some key policy adaptations to restore the overall competitiveness of the EU and digital ambitions in the telecom sector, whilst safeguarding the end-user protection.***

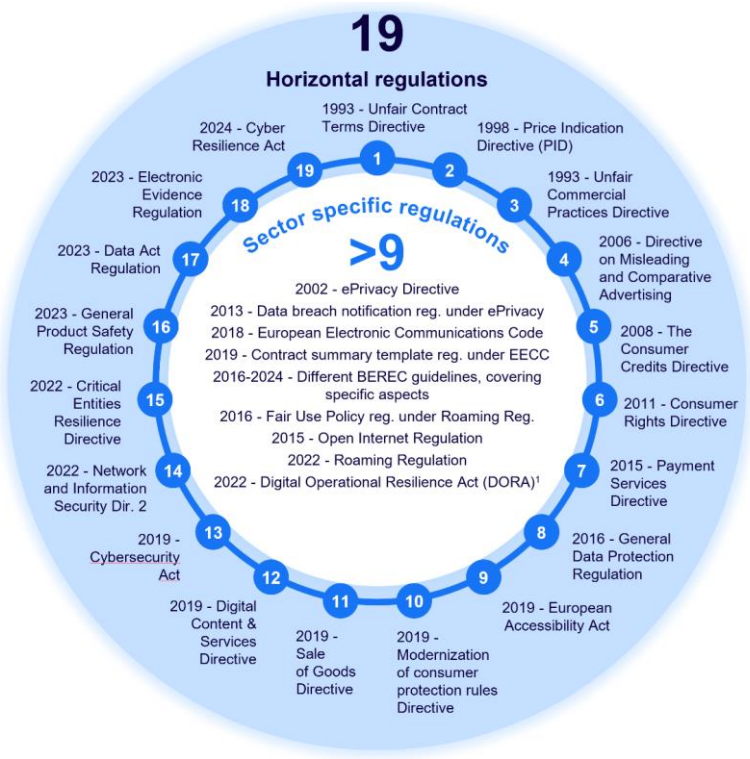
The targets for the 'Digital Decade' – complemented by the ambitions laid out in the Reports by Enrico Letta, Mario Draghi and in the more recent 'Competitiveness Compass' of the EU Commission – are aimed to drive the European Union towards a new era of innovation and competitiveness and are based on four pillars: i) digital skills, ii) developing secure digital infrastructures, iii) digitizing business and iv) transforming public services. Advanced connectivity networks and services are at the centre of this policy framework, and they will be essential to the achievement of the related goals.

Telecom operators play a central role in enabling digital participation by providing reliable, secure, and affordable connectivity to millions of citizens and businesses. Over time, European consumers have benefited from tremendous value creation delivered by and enabled by telecom operators, through greater service access, unlimited usage, much faster (x10) speeds, enriched quality, TV and entertainment options. However, European telecom operators are experiencing the lowest growth among 'digital players' despite relatively higher investment (CAPEX) and value given to the sector. Compared to global peers – particularly in North America and Asia – European telecom operators have underperformed across key performance metrics. Revenue growth of European telecom operators has for instance been flat from 2014 till 2023, whilst other markets grew their revenue >3% p.a.. Furthermore, the market capitalization of non-European telecom operators grew by 1-2% p.a., while the European telecom operators' market cap declined by almost 2% p.a.

Today's regulatory framework, built up over decades through both sector-specific and horizontal legislation, is no longer fit for purpose in many aspects considering the dynamic and increasingly digital ecosystem and the telecom sector' high level of maturity. While regulatory simplification is required in many areas this study offers a concrete simplification agenda for rules affecting the customer journey and security regulation.

Telecom operators are subject to a complex mix of over 28 European horizontal and telecom specific regulations (notwithstanding national laws), see Figure 1, stem from a mix of sector-specific and horizontal legislation, with nearly half overlapping.

**Figure 1: Overview of European horizontal and sectoral regulation affecting the end-user journey**




Telecom providers must comply with a patchwork of 34 sets of regulatory obligations that affect the whole end-user journey (see Figure 2) – from customer acquisition to service delivery and ultimately disconnection.

**Figure 2: 34 sets of obligations along the customer journey**


Source: Arthur D. Little

This results in complex, redundant information requirements, inconsistent rights across Member States, and constraints on offering innovative or tailored services – especially in fast-evolving areas like 5G and cross-border services – affecting both the way digital connectivity services are delivered and how they are ultimately experienced. This report explores why reform is urgently needed to support a more competitive, simplified, and harmonized framework for EU telecoms while maintaining a high level of consumer protection.

[1] DORA is a sector-specific regulation to the financial sector. Telecommunications providers may fall within the definition of ICT third-party service providers to the extent that they deliver network, data, or hosting services to financial entities.

Based on the operational burden created for telecom operators and their value to end-users, the report identifies **nine high-impact regulatory dimensions** that require review due to their impact on the end-user (see Table 1).

**Table 1: Overview of identified high-impact regulatory areas**

| | Regulatory issues | High level description |
|---|---|---|
| Prospect phase | 1. Outdated universal service obligations | Universal service obligations are outdated as market coverage and affordability are now near universal. Current obligations create significant costs and administrative burden that are difficult to recover, whilst targeted public funding (e.g. vouchers) would be more efficient for customers |
| | 2. Excessive customer protection under telecom specific law | Information transparency exceeds general consumer law. Information and transparency provisions are also subject to national gold-plating, leading to information overload for consumers while increasing compliance costs for telecom operators |
| During contract duration | 3. Restrictive net neutrality rules that ignore the extended digital ecosystem | Restrictive and divergent interpretations across Member States of "specialized services" generate regulatory uncertainty, hindering the launch of advanced or differentiated services ultimately preventing end-users from accessing innovative offerings and services like low-latency gaming or telemedicine; In parallel, big tech can freely manage traffic within their platforms, deteriorate quality of service etc. |
| | 4. Dual and stringent data protection and privacy rules apply only to telecoms | Telecoms face dual breach notification obligations under GDPR and ePrivacy, resulting in higher compliance costs. Inconsistent protection of confidentiality of communication compared to digital platforms and more stringent data processing grounds for traffic and location data lead to confusion on customer protection levels expectations, whilst limiting telecom's ability to deliver innovative services. |
| | 5. Fragmented national customer service & call center obligations | National customer service rules vary significantly and contain sometimes excessive obligations (e.g. response time or human interaction) raising costs for telecom operators. Rigid metrics may reduce service quality for users as telecom operators could prioritize form over meaningful support. |
| Customer churn | 6. Excessive telecom specific contract duration and termination rules | Sector-specific rules and gold-plating in some Member States add extra complexities. In the absence of a demonstrated market failure that would justify a purely sectorial approach, horizontal customer protection rules are sufficient (as long as contract duration rules do not act as a de facto lock-in) |
| | 7. Disparity in provider switching and number portability obligations that do not apply to big tech | Telecom users benefit from regulated switching and number portability, but equivalent protections are missing for messengers, email, or storage services. This regulatory gap reinforces user lock-in and fails to reflect functional equivalence across the digital ecosystem. |
| Transversal: Security | 8. Nationally-driven security restrictions fragment telecom operations | National rules on asset localization, remote access, and security clearance of personnel prevent cross-border operations and resilient service deployment (e.g. through hindrances to cross-border fail-over mechanisms during outages); Cybersecurity risk management obligations under NIS2 are being implemented inconsistently, leading to duplicated assessments and reporting requirements that divert resources from real threat response. |
| | 9. Compliance heavy incident reporting for security incidents | National fragmentation in NIS2 incident reporting creates diverging thresholds, timelines, and formats, forcing operators to duplicate efforts across jurisdictions. This diverts resources away from threat response, implementation of cybersecurity risk management measures etc., and weakens overall user protection. |

Source: Arthur D. Little

From the deep-dive analyses, several examples illustrate how current regulation consolidates into the undermining of the initial customer protection regulation ambition as well as unbalanced extra costs for telcos, due to three core structural challenges:

- **Overregulation** – Redundant, outdated and overlapping sector-specific and horizontal obligations reduce transparency and clarity for consumers while increasing costs for telecom operators. It can lead to inconsistency (e.g. notifications and confusion during data breaches) or additional rules being imposed to protect customers but ultimately creating confusion (e.g. contract information overload due to multiple transparency requirements)
- **An uneven playing field with big tech** - Functionally equivalent services face different obligations and consumer protection experience depending on who delivers them - telecom operators or big tech. Different customer protection regulations on similar services provided by different players might leave consumers without the expected protections (e.g. provider switching)
- **Fragmentation among European countries** - National variations of EU directives result in inconsistent consumer rights and experience across Member States, leading to different rights and service levels for consumers depending on their location, ultimately undermining the Single Market[2].

[2] 'Over 270 regulators active in digital networks across all Member States ("The future of European Competitiveness" Report, Draghi, September 2024)

To support Europe's strategic objectives under the Digital Decade, to achieve European competitiveness and a Single Market, this report proposes a reform package structured around **three priorities**:

**1. Simplify and align regulations to reflect modern consumer needs**

- Streamline overlapping obligations by relying on horizontal consumer protection rules (e.g., GDPR, CRD) instead of duplicative sector-specific ones
- Focus contract rules on information that enables meaningful comparisons, not technical details
- Eliminate sector specific data protection rules by repealing the ePrivacy Directive and consolidating the principle of confidentiality of communications, as the only remaining sector-specific element, under harmonizing legislation (e.g. GDPR or DNA).
- Abolish outdated USOs and replace them with targeted public support (e.g., broadband vouchers)
- Exclude B2B offers from consumer protection obligations under the EECC, recognizing their distinct nature and needs

**2. Ensure a level playing field across equivalent services**

- Extend key obligations, such as switching rights and confidentiality of communications, to other digital providers offering functionally equivalent services
- Clarify net neutrality to enable innovation:
    - Allow a more flexible framework, in line with pro-innovation regulators (i.e. Ofcom)
    - Create a whitelist of permitted specialized services to offer legal certainty
- Reflect the broader digital value chain, ensuring that obligations apply fairly to all key actors like operating systems for an even consumer experience across digital value chain and players.

**3. Harmonize implementation and reduce fragmentation across the EU**

- Use a regulation rather than a directive to ensure consistent application of customer protection rules across Member States and avoid national gold-plating
- Strengthen EU-level coordination and institutional support to align enforcement practices and reduce divergence and additional obligations by Member States
- Accelerate and streamline the enforcement of harmonized rules to support consistent consumer experiences and efficient cross-border services

Europe's telecom regulatory framework has helped deliver connectivity, protection, and competition. Telecoms markets have fiercely evolved since its entry into force. It is therefore time to reassess the patchwork of rules applying to operators to improve harmonization and simplify them wherever possible to ensure they are future-proofed, and innovation-enabling, while delivering consistent rights to users across the EU.

# INTRODUCTION

The liberalization of telecommunications in Europe, launched in the late 1980s and culminating in full market opening by 1998, represented a milestone in European integration. Through successive legislative packages - such as the 2002 Regulatory Framework, the Telecoms Single Market Regulation, and the European Electronic Communications Code (EECC) - the EU progressively combined competition policy with social and strategic objectives: consumer protection and infrastructure investment.

In a drastically changing market environment, the regulatory framework has struggled to keep pace. Telecom operators face growing regulatory complexity due to overlapping sector-specific and horizontal obligations, outdated regulations, and divergent national implementations in some Member States, sometimes more stringent than required by the European framework. Furthermore, big tech have gained a dominant position in the digital ecosystem, offering functionally equivalent services to those offered by telecom operators but without following the same regulatory obligations.

Telecommunications remain a cornerstone of the European digital economy and the backbone of all EU industries. The sector provides the essential infrastructure and connectivity that supports innovation, growth and digital inclusion. In order to ensure that telecom markets remain competitive, investment-ready, and capable of consistently delivering value to end-users and society as a whole, there is a pressing need to reform EU's regulatory framework to foster a competitive and secure European telecommunication networks, echoed by the Draghi and Letta reports, both of which emphasize the importance of strategic coordination, simplification, and investment in critical infrastructure.[3]

In 2024 the commission published a 3-pillar White Paper[4], of which the second pillar aims to complete the Digital Single Market with considerations around i) equal rights and obligations for all actors and end-users of digital network, ii) copper switch-off and full-fiber acceleration policies, iii) more integrated governance at European Union level, for spectrum and authorizations and iv) 'greening' of digital networks.

At the beginning of this year the European Commission has published the "European Competitiveness Compass[5]" a roadmap to restore Europe's dynamism and economic growth, introducing five horizontal enablers to increase European competitiveness, assessing innovation gaps, reducing regulatory burdens, and fostering a more integrated Single Market.

In this context, the European Commission is currently working on the re-evaluation of the European Electronic Communications Code (EECC) with a view to proposing a new Digital Networks Act (DNA), aimed to drive the European Union towards a new era of innovation and competitiveness.

After all, Europe's ability to meet its Digital Decade targets - including universal gigabit connectivity, secure digital infrastructure - depends on more than just investment or innovation alone. It also requires a regulatory framework that is coherent, proportionate, and aligned with market realities. Without the needed reforms, the complexity,

[3] Mario Draghi, The Future of European Competitiveness, September 2024; Enrico Letta, Much More than a Market, April 2024.

[4] European Commission, White paper: How to master Europe's digital infrastructure needs? February 2024

[5] A Competitiveness Compass for the EU, January 2025.

asymmetry, and fragmentation challenges currently observed risk becoming structural barriers to progress. Regulatory clarity, fairness, and consistency are not only administrative concerns - they are critical enablers of the EU's digital competitiveness and strategic autonomy.

**Purpose and scope of this report**

While regulatory simplification and deregulation (e.g. network access) is needed across a wide range of areas, this study specifically focuses on regulation impacting the customer journey (among others, consumer protection, data and privacy requirements, universal service mandates and net neutrality) and security regulation.

The analysis is grounded in a mapping of 34 end-user related obligations drawn from 28 EU legislation and national transpositions, and analyzing the burden on telecom operators highlighting the effect of regulation on the quality, clarity, and consistency of the end-user experience across the customer journey. This is done with a detailed analysis including case studies and benchmarks illustrating how current rules operate in practice. The objective of the report is to highlight key policy adaptations that are required to restore EU's overall competitiveness and digital ambitions in the telecom sector, whilst safeguarding and or improving the end-user journey.

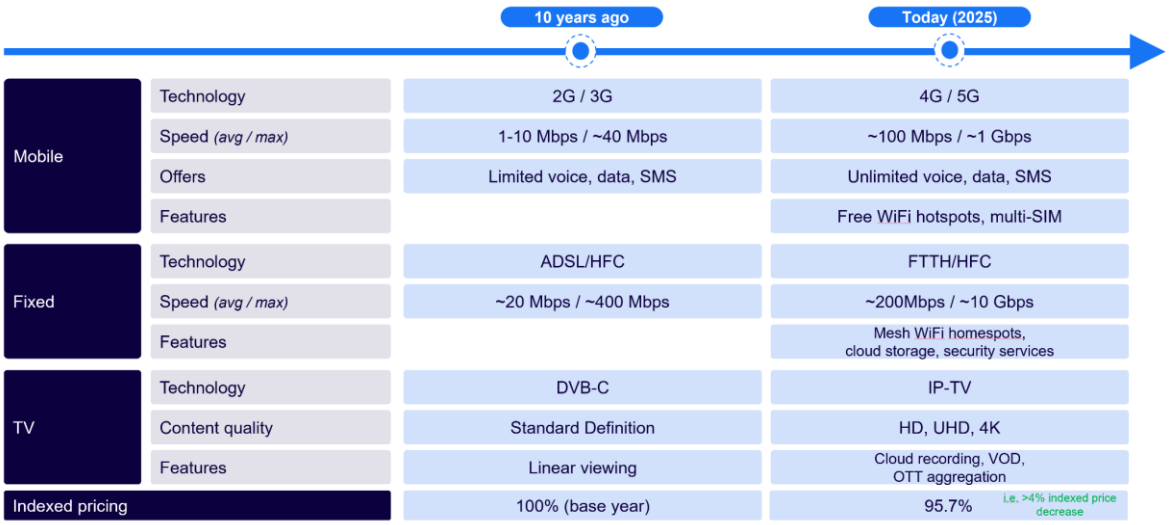
**Structure of the Report**

After giving an overview of the value enabled by telecom operators throughout the last decade and the high-level results across the sector, an overview is provided of the regulatory landscape impacting all steps throughout the end-user journey from prospect to churn. Deep-diving into nine priority areas it is demonstrated how overregulation, uneven playing field and fragmentation impact end-users and burden telecom operators. Based on the preceding analysis, policy recommendations are proposed, aiming for simplification, restoring the level playing field and harmonization whilst safeguarding or enhancing the customer-journey and society as a whole.

# 1. EUROPEAN TELECOM OPERATORS DELIVERED HUGE VALUE FOR THEIR END-USERS, BUT LAGGED PERFORMANCE

European consumers have significantly benefited from the huge value created and enabled by telecom operators. Over the past decade, customers have seen a significant leap in the value they receive from telecom services (see Figure 3). Today, consumers enjoy greater service access, unlimited usage, much faster speeds, quality and richer TV and entertainment options. Although the liberalization policies and pro-competitive regulation at the European level[6] opened up markets to competition, allowing new entrants to challenge former incumbents, the resulting market structure with 34 mobile network operator groups and roughly 500 MVNOs currently active in the EU, is much more fragmented in comparison to other global regions, like the US or China[7]. This fragmentation, while initially fostering competition and end-user value, has also placed sustained financial and operational pressure on telecom operators. Over time, this has hindered their capacity to invest and maintain innovation, potentially threatening the long-term health and competitiveness of the sector.

**Figure 3: Major technology evolutions and customer value increase over 10 years**



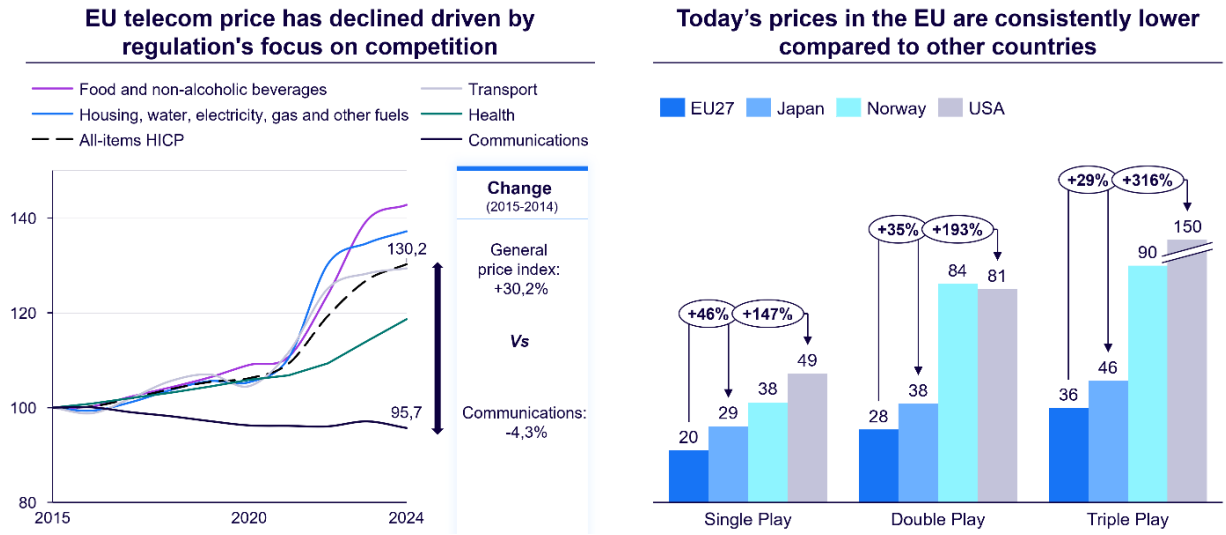

Source: Arthur D. Little, Eurostat

Importantly, this transformation has been accompanied by flat or even lower prices. Compared to a decade ago, consumers today get far more value at a relatively lower cost, ignoring inflation (see Figure 4). Prices for communications services have declined ~4%, versus indexed increases on all other services of ~30%. Also, zooming in on Europe, compared to other countries the European prices are consistently lower than in other developed economies.

[6] Enrico Letta, Much More than a Market, April 2024.

[7] Mario Draghi, The Future of European Competitiveness, September 2024

**Figure 4 : EU telecom prices: evolution and comparison in EUR PPP compared to other countries**




Source: Left - Eurostat data, retrieved April 2025. Right - Publications office of the EU[8]

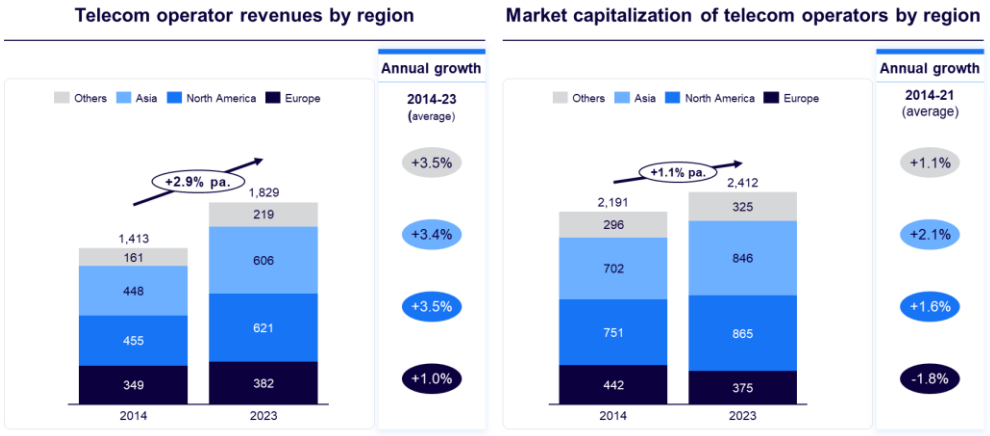
Furthermore, as a cornerstone of the digital society, telecom operators have contributed to broader economic and social value across sectors. Their role as both infrastructure providers and digital enablers has been central to Europe's digital transformation and continues to deliver direct benefits to consumers across the continent. A total of €177billion in potential annual economic gains were identified in 2017 by the European Commission linked to the Digital Single Market Strategy (DSM) initiatives, corresponding to 1.2% of the European GDP (See Figure 13 on page 34 in appendix).

However, over the past decade, European telecom operators have faced growing pressure on their business models due to stagnating revenues, high investment requirements to pursue the best available technology, and increasing regulatory burdens. Compared to global peers - particularly in North America and Asia - European operators have underperformed across key performance metrics, including revenue growth, market capitalization, and capital investment capacity.

A recent Arthur D. Little benchmarking analysis shows that from 2014 to 2023, European telecom operators' revenue grew at a compound annual growth rate (CAGR) of just 1.0%, compared to approximately 3.5% for operators in other regions. In parallel, European telecom operators have experienced a negative market capitalization growth (-1.8% CAGR, - 15% cumulative over the 2014-2023 period) whilst Asia (+2.1% CAGR, +20% cumulative) and North-America (+1.6% CAGR, +15% cumulative) have grown positively (see Figure 5).

[8] European Commission: Directorate-General for Communications Networks, Content and Technology and Empirica, *Mobile and fixed broadband prices in Europe 2022 – Final report and executive summary*, Publications Office of the European Union, 2024.

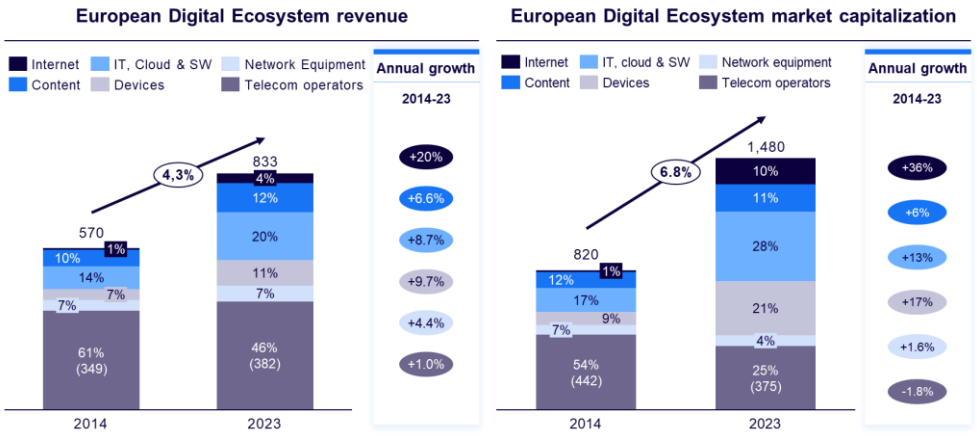
**Figure 5: Telecom operators revenue growth by region, according to headquarters location[9]**




Source: LSEG, Arthur D. Little

In terms of revenue share in the European digital ecosystem, telecom operators represent the majority at roughly 50%, but with the smallest share in terms of revenue growth (1%) on the 2014-2023 period while Internet players stand at the head of the digital ecosystem (+20%), IT, Cloud & software players (+8.7%) and Content providers (+6.6%). Similarly, market capitalization of telecom operators has decreased by 1.8% annually, whilst internet players have experienced the highest growth rates (36%), IT, Cloud & software players (+13%), Content providers( +6%) - see Figure 6.

**Figure 6: Telecom operators' revenue and market capitalization compared to the digital ecosystem for companies headquartered in Europe[10]**




Note: **Internet** refers to platforms providing access to web-based services, marketplaces, and advertising ecosystems; **Content** includes providers of digital media, entertainment, music, and gaming services; **IT/Software/Cloud** includes technology firms offering enterprise software, cloud infrastructure, and business platforms; **Devices** includes manufacturers of end-user hardware such as smartphones, laptops, and connected consumer devices; **Network Equipment** refers to companies supplying physical infrastructure and equipment for telecom networks, including 5G and fiber technologies.

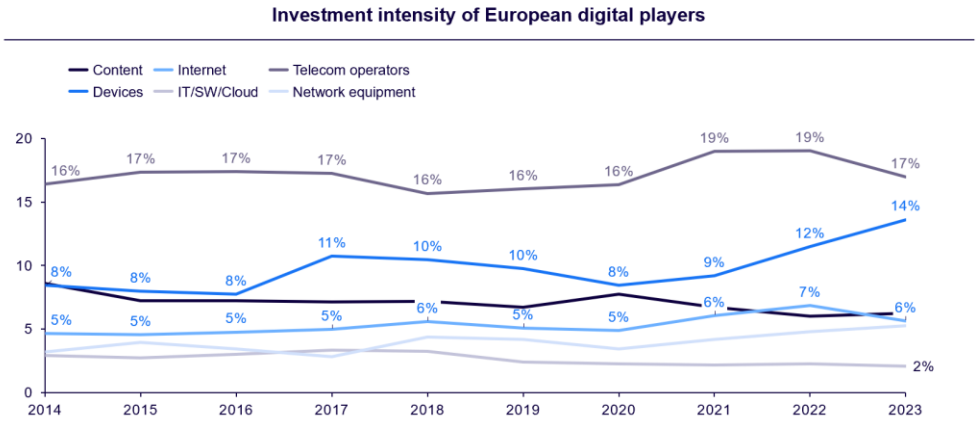
Source: LSEG, Arthur D. Little

[9] World, 2014-2023, In constant billion Euros, top 500 players by category

[10] World, 2014-2023, In constant billion Euros, top 500 players by category

Despite these pressures, European telecom operators have always kept high CAPEX-to-revenue ratios, between 15-20%, indicating sustained but increasingly strained investment levels (see Figure 7). Furthermore, the level of investment is, and structurally has been, approximately two to five percentage points higher than its US peers.

**Figure 7: European telecom operators investment ratio compared to other digital ecosystem players [11]**




Source: LSEG, Arthur D. Little

This economic environment, coupled with fragmented regulatory frameworks and increased competition from Internet, IT, Cloud & software and Content players, raises concerns about the sector's ability to fund next-generation infrastructure and contribute to Europe's Digital Decade targets. The Letta report acknowledges that "*digital technologies drive industrial productivity and citizen well-being"* and *"Unsteady economic sustainability of operators may worsen future consumer welfare by way of lower quality services, as well as security, and uneven distribution of network access, as well as it hinders digitalization of industries and services, leading to lower growth and competitiveness for the whole Europe and for each domestic market*."

*For publisher: quote -* This is highly relevant to society. As Mario Draghi wrote in his report[12] : "The declining profitability of the telecom sector now may represent a risk for industrial companies in Europe, in a phase when state of the art infrastructure is required to digitize manufacturing, supply and distribution chains."

[11] CAPEX/Revenue, World, 2014-2023, in constant billion euros, top 500 players by category

[12] Draghi report on EU competitiveness, Part B, p. 70

# 2. HOW THE CUSTOMER JOURNEY IS IMPACTED BY THE CURRENT REGULATORY FRAMEWORK

*For publisher: Side quote -* ”A complex landscape of 28 regulations, resulting in 34 sets of obligations along the customer journey”

On top of the beforementioned stagnating revenues and unsustainably high investment requirements for providing the best available technology, the regulatory burden on European telecom providers has significantly increased over time. With the progressive addition of regulatory instruments at European level, and their transposition into national laws, telecom operators in the EU are subject to a complicated regulatory environment, which is a complex mix of 28 European horizontal and telecom specific regulations (notwithstanding national laws), see Figure 8, which translate into 34 distinct regulatory obligations related to the different steps of the customer journey (see Figure 9).

**Figure 8: Overview of European horizontal and sectoral regulation affecting the end-user journey[13]**


Source: Arthur D. Little

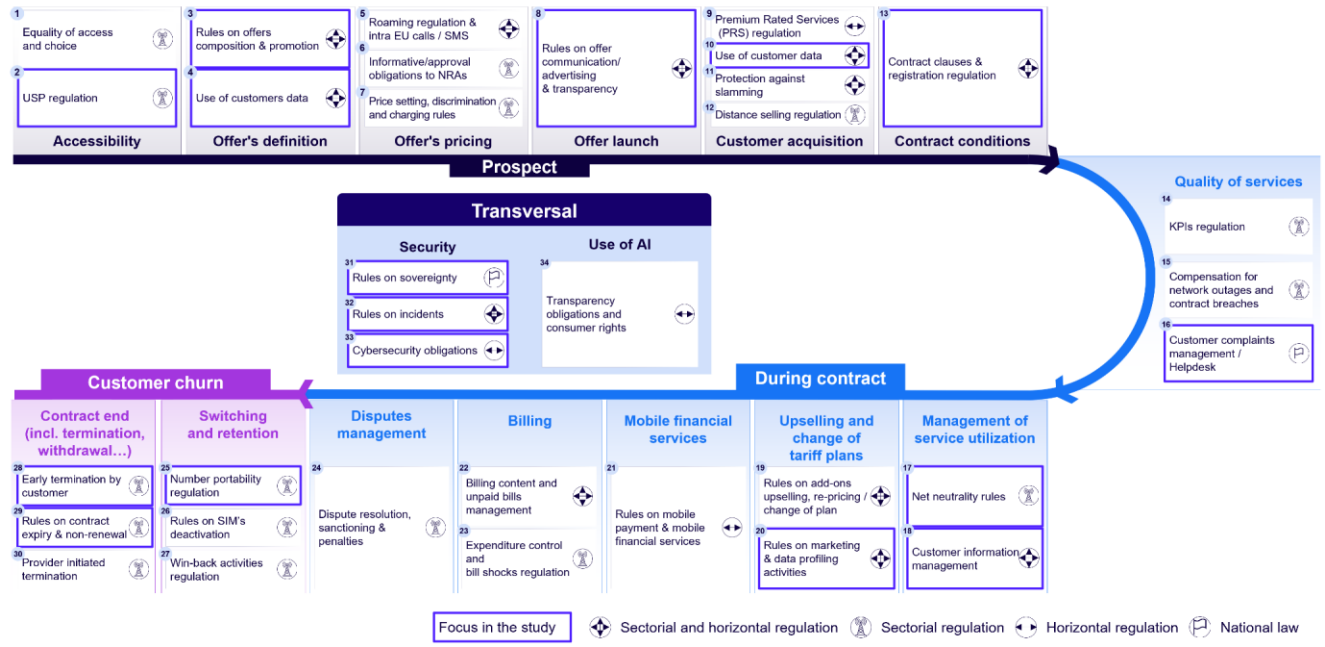
Figure 9 shows that among these 34 sets of obligations:

- 16 are governed by sector-specific rules only (e.g., Roaming Regulation, EECC, net neutrality rules).

[13] DORA is a sector-specific regulation to the financial sector. Telecommunications providers may fall within the definition of ICT third-party service providers to the extent that they deliver network, data, or hosting services to financial entities.

- 12 are governed by both sectoral and horizontal rules, often leading to overlap (e.g., customer protection under EECC and horizontal customer protection laws, data protection under GDPR and ePrivacy).

**Figure 9: End-user related obligations applicable to European telecom operators**




Source: Arthur D. Little

Whilst regulation enabled the benefits for end-users throughout the last decades, several of them have led to obligations that undermine the initial customer protection regulation ambition, as well as creating unbalanced extra burden and costs for telcos (these are marked in Figure 9 as *'focus in the study'*). These obligations have been assessed based on the operational burden they create for telecom operators and their value to end-users, and regrouped in nine regulatory dimensions, ordered along the end-user journey, rather than importance:

1. Outdated universal service obligations
2. Excessive customer protections under telecom specific law
3. Restrictive net neutrality rules that ignore the extended digital ecosystem
4. Dual and stringent data protection and privacy rules apply only to telecoms
5. Fragmented national customer service & call center helpdesks obligations
6. Unnecessary telecom specific contract duration and termination rules
7. Disparity in provider switching and number portability obligations that do not apply to big tech
8. Nationally-driven security restrictions fragment telecom operations
9. Compliance heavy incident reporting for security incidents undermines user protection

This chapter follows the end-user through their interaction with telecom services, starting from first contact (prospect phase), to contract execution and usage, through to contract termination and churn. In addition, it covers transversal considerations related to security and AI. Through a regulatory analysis and concrete operational examples the report questions existing obligations and analyses areas where reform would be beneficial.

It provides i) deep dives into the nine regulatory dimensions as they appear along the customer journey, and then ii) draws out three broader patterns linked to those regulations.

## Following the customer journey - Phase I: Prospect phase

Before users subscribe to a telecom service, they engage with offers, compare prices, and make decisions about which plan to choose. In this early phase, they are already exposed to a broad range of regulatory obligations related to basic service accessibility, the definition and promotion of offers, pricing, offer communications, contract conditions and contract setup.

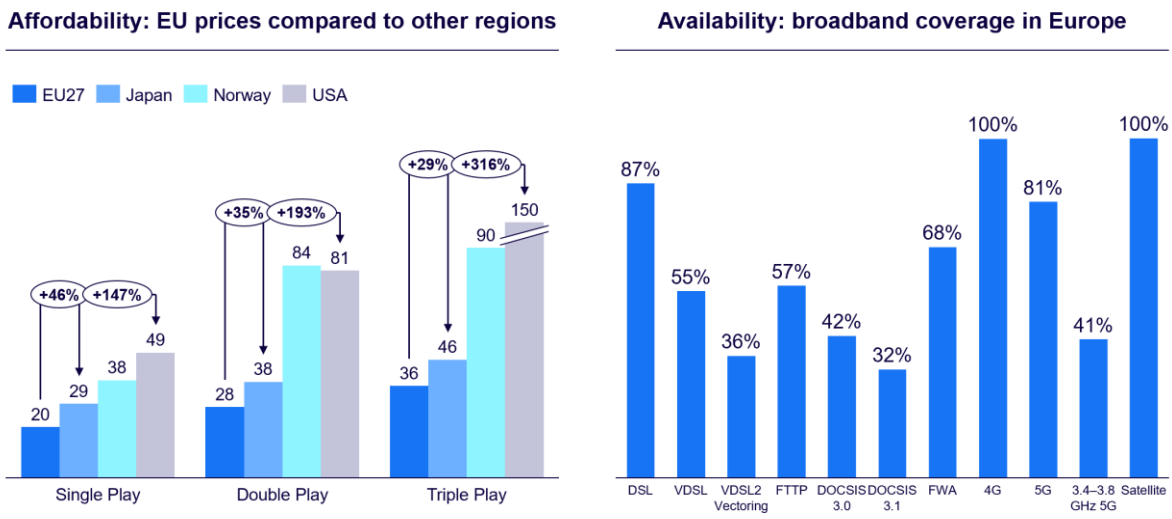
Two regulatory areas have been identified as problematic through their impact on consumers as well as telecom operators: i) universal service obligations and ii) customer protection rules on information and transparency.

### *i. Outdated universal service obligations*

Even before an end-users begins considering a subscription, obligations related to accessibility apply to ensure universal availability of broadband services for potential future customers under the Universal Service Obligation. The articles 84 to 92 of the EECC force Member States to ensure that all consumers have access to adequate broadband at affordable prices to ensure universal provision of internet services. While this was critical in the past to overcome infrastructure gaps and promote digital inclusion, current market conditions have made USOs outdated.

Affordability is no longer a systemic issue: competition and innovation have significantly lowered telecom prices EU-wide. Availability has also improved, 98% of households are covered by fixed broadband[14], and mobile and satellite technologies fill most remaining gaps, especially in rural areas.[15] As a result, internet take-up in households now stands at 94%, compared to 80% in 2014.[16]

**Figure 10: EU telecom prices (comparison in EUR PPP compared to other countries) and broadband coverage**




[14] European Commission, Broadband Coverage in Europe 2022

[15] BEREC Report on Member States' best practices to support the defining of adequate broadband internet access service, Draft version, 5 October 2023. 7 March 2024.

[16] Eurostat

Source: Left - Publications office of the EU[17], Right - Study by Omdia and Point Topic for the European Commission

Only nine Member States have designated universal service providers, which suggests that the market is mostly expected to ensure universal access to the basic services (e.g. the Belgium NRA (BIPT) has not designated any USP as it did not receive any complaint within the scope of USO in 2020). In parallel, industrial policy objectives are more forward-looking and ambitious compared to the "adequate" broadband definition under the universal services rules[18]. Adequate broadband internet access services as defined by Member States under universal service mostly revolve around 10Mbps, whilst EU industrial policy ambitions aim for universal Gigabit connectivity and 5G-equivalent wireless coverage by 2030.

Compensation for USO has proved to be inefficient in reality. When telecom providers seek compensation demonstrating for the net cost of meeting USOs, they often face complex, lengthy, and uncertain processes.[19]

Given that any remaining affordability/coverage issues are limited to small, vulnerable groups, targeted public subsidies (e.g. vouchers) could be more effective, justified (public policy) and less burdensome than blanket obligations.

Legacy USOs impose disproportionate burdens on telecom operators, including administrative complexity and incomplete and uncertain cost compensations, as well as legal uncertainty on national interpretation. On the customer side, universal service can be addressed more efficiently through targeted public subsidies (e.g. public vouchers), ensuring that the customer protection does not get undermined.

### *ii. Excessive customer protections under telecom specific law*

**Transparency and information requirements that overwhelm rather than informs customers**

From the moment a consumer begins exploring internet or telecom offers, telecom operators are subject to strict information and transparency requirements under the EECC, that are exceeding horizontal customer protection applicable to big tech. National divergences exacerbate the issue. These obligations aim to empower consumers, but in practice often overwhelm them with legalistic and technical detail, making it difficult to focus on what truly matters. Research demonstrates that information overload leads to worse decision quality and experience.[20] End-users may also be misled by different levels of protection depending on the provider and the country. From the operators' perspective, the obligation results in increased compliance costs, due to product-specific data integration into IT and CRM systems, and the additional need for internal coordination across legal, regulatory, IT, and customer support teams. Sector-specific consumer rules should only be applicable when justified by

[17] European Commission: Directorate-General for Communications Networks, Content and Technology and Empirica, *Mobile and fixed broadband prices in Europe 2022 – Final report and executive summary*, Publications Office of the European Union, 2024.

[18] In Europe, ambitious EU connectivity targets were set by the 2010 Digital Agenda for Europe (DAE) and the 2016 Gigabit Society objectives

[19] Example: - In Ireland, incumbent operator Eircom submitted a claim for compensation covering the 2009–2010 period, citing a positive net cost of €5.1 million. However, after an extended assessment process lasting several years, the national regulator ComReg rejected the claim, arguing that the burden did not meet the legal threshold of being "unfair." The rejection was upheld despite formal recognition that the services were provided at a loss.

[20] M. Peng, Z. Xu and H. Huang, *Does Information Overload Affect Consumers' Online Decision Process? An Event-Related Potentials Study*, 2021; G. Kusi, G. Rumki, F. Quarcoo, E. Otchere et. Al., *The Role of Information Overload on Consumers' Online Shopping Behavior*, 2022.

specific needs of the market. Contract information and transparency requirements can be effectively addressed through horizontal consumer protection rules.

Article 102 and 103 of the EECC mandates highly detailed pre-contractual information and transparency, including internet speeds, remedies, and performance commitments, alongside a standardized contract summary (Regulation 2019/2243). This goes beyond the basic information required under general consumer law, which focuses on price, duration, and key contractual term. See Annex 1: Overlapping consumer protection rules: EECC vs. horizontal customer protection law**.**

National divergences exacerbate this issue. Germany requires communication providers to issue a product information sheet with key contractual details prior to contract conclusion.[21] This goes beyond EECC which requires precontractual information in the form of a contract summary. In Italy, all end-user information has to be provided in accessible formats to users with disabilities by default, not just on request as foreseen in the EECC.[22] See Annex 4: Divergent consumer protection implementation.

## Following the customer journey - Phase II: In-contract

Once a contract is signed, the end-user enters the service phase during which telecom operators face 11 obligations related to quality of services, management of service utilization, billing, disputes management.
The following regulatory areas have been identified as problematic through their impact on end-users as well as telecom operators: i) net neutrality rules, ii) data protection and privacy rules and iii) national customer service & call center helpdesks.

### *i. Restrictive net neutrality rules that ignore the extended digital ecosystem*

Once a customer is subscribed to an internet access service, net neutrality[23] rules govern how their respective traffic is managed, ensuring that all online content and applications are treated equally. Net neutrality rules were introduced to ensure that internet access providers do not discriminate between online services or content or end-users, but overly restrictive interpretations now hinder innovation, while true neutrality is not guaranteed, as the rules do not apply across the entire digital ecosystem.

**Restrictive and fragmentation interpretation of specialized services limits innovative services**

Today's reading and implementation of the Open Internet Regulation has become preventive and risk-averse in many countries, which is limiting traffic differentiation. While specialized services are theoretically permitted, the restrictive interpretations leave operators hesitating in launching such offers, ultimately deterring innovation. For example, low-latency offers for gamers, temporary quality boosts during live events, or guaranteed service levels for enterprises face legal risk if implemented under current interpretations.

[21] §§1–2 of the Telecoms Transparency Regulation

[22] Article 98 of the transposing law (Legislative Decree No. 207/2021)

[23] Regulation (EU) 2015/2120 and BEREC Guidelines

Research acknowledges that overly rigid neutrality rules can restrict beneficial service innovation and deter network investment, leading to long-term welfare losses for society.[24] In its 2023 review, Ofcom stated that rules are impacting telecom operators and therefore also consumers: Net neutrality rules "*may be restricting their ability to innovate, develop new services and manage their networks. This could lead to poor consumer outcomes, including higher costs, or consumers not benefiting from new services as quickly as they should, or at all. These potential downsides might become more pronounced in the future, as people's use of online services expands, traffic increases, and more demands are placed on networks.*"[25] The European Commission also acknowledged this challenge in its 2023 review of the Open Internet Regulation, stating that greater legal certainty could benefit both innovators and consumers.

In addition, the enforcement of net neutrality rules varies across the Union, adding complexity and regulatory uncertainty for operators. National regulatory authorities (NRAs) apply differing interpretations of the net neutrality principles, particularly in areas such as specialized services, traffic management practices, and the relationship between innovation and non-discrimination. This variation in implementation creates differences in compliance requirements across Member States and may contribute to uncertainty and a chilling effect for launching innovative service offerings, as ISPs often pre-emptively align with the strictest national interpretation to mitigate regulatory risk, even when more flexible solutions would be permissible elsewhere. An overview of divergent positioning of NRAs and concrete examples can be found in Annex 5: Inconsistent application of net neutrality rules.

A whitelist of use cases that are considered as specialized services by the European Commission would highly improve legal certainty.

**Net neutrality limits operator flexibility in a big tech platform-dominated market**

The current net neutrality framework creates a structural imbalance in the digital value chain. Internet access providers remain subject to stringent obligations under the Open Internet Regulation (TSM), while large technology companies, who deliver the vast majority of traffic and exert increasing control over content delivery, application behavior, routing, and Quality of Service, are not subject to equivalent rules. This asymmetry means users are no longer enjoying a "neutral net" with regards to the broader digital ecosystem.

The environment that net neutrality regulations sought to control (i.e. ISPs as primary bottlenecks) significantly evolved. On the one side, fierce competition and end-user empowerment has advanced significantly through switching rights, reducing the market power of ISPs compared to end-users. On the other side, the market power ISPs once had compared to big tech, also shifted in favor of the latter: a handful of global big tech dominate traffic flows and end-user experiences:

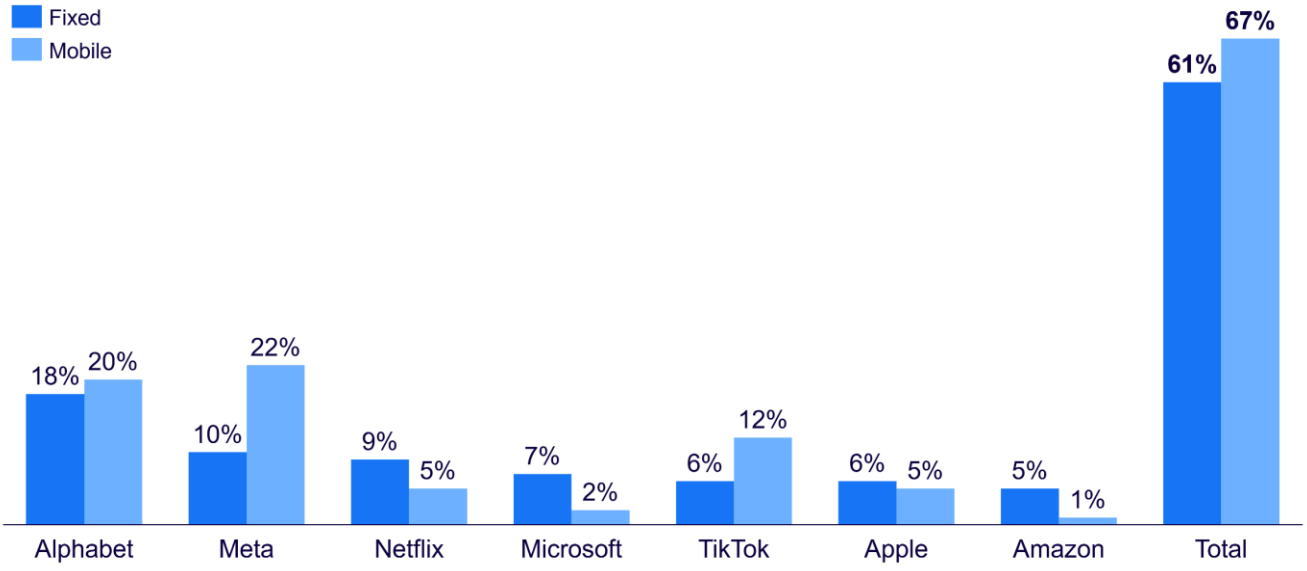
- Big tech has gained significant importance in defining the content for end-users, creating virtual lock-ins the net neutrality regulation was trying to avoid, with practices restricted to ISPs such as blocking or paid prioritization.

[24] Briglauer, Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector: Relevant Developments and State of the Empirical Literature, 2024

[25] Ofcom, 2023, Net Neutrality Review.

- 60% of global network traffic now originates from just 8 big tech[26], a number that keeps increasing while data traffic is expected to triple by 2030.[27]

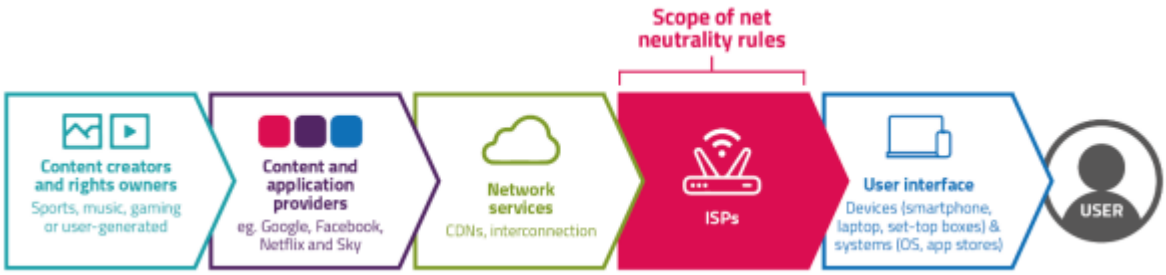
**Figure 11: Data traffic generated (fixed and mobile) by the seven major big tech service providers**




Source: Sandvine 2024 Global Internet Phenomena Support

These players, manage operating systems, and increasingly control private backbones, CDNs, and cloud services, influencing quality and routing far beyond the reach of ISP management.[28] As a consequence, an increasing volume of traffic is being managed outside the scope of the OIR, and by market actors who are not subject to those rules.[29] In its net neutrality review of 2023, Ofcom indeed concludes that *"net neutrality rules limit the actions ISPs can take, but do not restrict other parties in the value chain. Since the rules were put in place, players with strong market positions have developed throughout the internet value chain and are not constrained in the same way as ISPs by the net neutrality rules."*[30]

**Figure 12: Scope of net neutrality rules in the Digital Ecosystem value chain**




Source: Ofcom, 2023, Net Neutrality Review

[26] Sandvine's 2024 Global Internet Phenomena Report

[27] Ericsson Mobility Report, 2024

[28] BEREC Draft Report on the entry of large content and application providers into the markets for electronic communications networks and services - BoR (24) 51; Stocker et al. 2017).

[29] Briglauer, Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector: Relevant Developments and State of the Empirical Literature, 2024.

[30] Ofcom, 2023, Net Neutrality Review.

**Deep dive on big tech practices that would be prohibited through the OIR**

Across the digital ecosystem, big tech increasingly exercise control over traffic delivery and service quality, engaging in practices that are functionally similar to those prohibited for ISPs under the EU's Open Internet Regulation. While these practices are often implemented in the name of user experience optimization or operational flexibility, they create significant asymmetries in regulatory treatment at the detriment of end-users.

- Service availability blocking and self-preferencing on platforms: Google's blocking of YouTube on Amazon devices, and Apple's rejection of cloud gaming apps, illustrate their ability to restrict content access on rival platforms (even tough, relying on horizontal competition law or on the DMA, some practices have been regulated).
- Freely rerouting traffic, while additionally encrypting it and fully anonymizing traffic through the use of Privacy Relays, limiting the access of third parties to traffic information they keep for themselves
- Imposition of network architecture requirements: as 5G Standalone networks enable slicing, operating system providers like Apple (iOS 17+) and Google (Android Enterprise) are introducing features that depend on dedicated network slices to guarantee performance for specific applications (e.g. enterprise apps, AR/VR, critical messaging). To support these features, telecom operators must meet several technical and operational requirements (such as enabling per-application slice mapping through Mobile Device Management (MDM) or Android APIs, or configuring real-time policy control for device-triggered QoS settings). Yet, telecom operators are prohibited from offering similar differentiated treatment for their own services or customers

### *ii. Dual and stringent data protection and privacy rules apply only to telecoms*

From the moment a user begins interacting with a telecom service, by requesting information, browsing plans, or registering interest, telecom providers are subject to a dual data protection regime. This burden intensifies during the contract phase, where telecom operators face two particularly problematic obligations: dual breach notification duties, and narrow data processing rules for traffic and location data. Unlike big technology platforms that operate solely under the General Data Protection Regulation (GDPR), telecom operators must also comply with the ePrivacy Directive of 2002, revised in 2009, which imposes additional, outdated, and often more restrictive obligations

This results in overlapping, fragmented, and inconsistent protection levels for end-users.

- Dual breach notification reporting leads to parallel incident reporting duties, legal uncertainty, duplication of efforts and unnecessary compliance costs. For each incident, operators must determine which rules apply, assess risk under two different legal thresholds, and prepare reports for different authorities, often using separate templates, submission systems, and deadlines. For end-users, the overlapping frameworks can result in inconsistent and sometimes excessive communication. In the absence of a unified threshold for notification, providers may send breach notices to consumers even when the actual risk is low, simply to avoid potential sanctions. This can contribute to notification fatigue, where users stop paying attention to security alerts, potentially undermining the original intent of protecting consumer trust and privacy.[31]

[31] EDPB Guidelines on Breach Notification (2018).

- Inconsistent protection regarding confidentiality of communications and data processing grounds erode user trust and creates confusion for consumers about privacy rights and data handling, and more difficulties for operators to innovate in the data economy. Users may assume their communication and location data are treated equally across apps and networks, but in practice, their rights and protections depend on which type of provider they interact with. The disparity also has competitive effects that indirectly impact users as for example the fragmented implementation of ePrivacy has so far created delays and legal uncertainty for the adoption by fixed and mobile operators of anti-fraud techniques. Stricter rules on ECSs constrain their ability to innovate, personalize services, or use analytics, unlike digital-native companies.

Therefore, the ePrivacy Directive should be repealed considering that:

- its core provisions (e.g. art. 4 on breach notifications and art. 6 and 9 on traffic and location data) are partially overlapping and can be covered by the GDPR
- other provisions (for instance on itemized billing, presentation and restrictions of calling identification, public directories, etc.) are not relevant compared to current state of technology and service offerings, and can be deleted
- with regards to the principle of confidentiality of communications (art. 5), specific provisions could be integrated in upcoming or existing horizontal legislations to ensure consistent application of the rules across the digital ecosystem

**Overlapping breach notification rules**

For example, breach notification rules differ across frameworks. Telecom providers must alert national telecom regulators within 24 hours under ePrivacy rules (Article 4 ePrivacy Directive, Regulation (EU) No 611/2013) , even for minor incidents, while GDPR requires reporting to data protection authorities within 72 hours only if the breach poses a high risk to individual rights (Articles 32, 33 GDPR). These parallel requirements involve different authorities, timelines, and thresholds. As a result, providers frequently duplicate their efforts, especially when an incident involves both communication-related data and other personal information. The European Data Protection Board has issued guidance clarifying that a second notification under the General Data Protection Regulation may not be needed when the ePrivacy rules have been followed. In practice, telecoms often duplicate reporting due to legal uncertainty and inconsistent national interpretations. See Annex 2: Overlapping data protection obligations

**Uneven protection of confidentiality of communications**

Under article 5 of the ePrivacy Directive, public Electronic Communications Services (ECS) must keep communications and the related traffic data confidential, banning any listening, storage, or tapping unless users explicitly consent or national security laws create exceptions[32]. While the confidentiality of communications is a core element of digital privacy and should be preserved, it is currently limited to ECSs. Its scope should be extended to all interpersonal communications services. This would better reflect Article 7 of the EU Charter of Fundamental Rights, which protects private and family life.

**More restrictive traffic and location data processing grounds for telecom operators compared to big tech**

Under articles 6 and 9 of the ePrivacy Directive, traffic and location data must be erased or made anonymous when it is no longer required for communication or billing purposes, and cannot be used for any other purpose, unless the user has provided his consent for another use. Both impose stricter limitations compared to the broader

[32] In accordance with art. 15(1) E-Privacy Directive.

grounds for data processing available under the GDPR. For example, location data is defined as “any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.”

While highly precise GPS-based location data collected by apps falls only under the GDPR, network-derived mobile location data (e.g., Cell-ID) collected by telecom providers is additionally subject to the ePrivacy framework. The current Directive hinders innovation by making it too complex to process location data and to compete with technology companies that are not subject to the same sectoral rules. Additionally, the Directive imposes limitations on the adoption by electronic communication service providers of anti-fraud measures that would protect customers from impersonation fraud. Network operators would currently require an exemption at (each) Member State level in order to deploy such solutions.

### *iii. Fragmented national customer service & call center helpdesks obligations*

Telecom operators in the EU are subject to a patchwork of fragmented customer service obligations, creating far-reaching requirements. These national requirements increase operational complexity and costs for telecom operators. In particular, the strict response times combined with the limitation of the automation of call center responses / obligation of a “personal, human interaction” may significantly drive-up staffing costs for operators, whilst the difference in national interpretations add compliance costs for telecom players operating cross-border. Strict obligations may also have unintended consequences for end-users: service quality can be affected when providers need to prioritize compliance with formal metrics (e.g. response times) over delivering meaningful support. Some countries such as Ireland, Netherlands, Italy force call-centers to be completely free of charge, and increased costs may ultimately affect service quality or pricing.

The Italian NRA (AGCOM), with the Resolution 255/2024[33], has updated the telecom providers[34] call center regulation requiring to offer customers free-of-charge call center services (as already provided by the current regulation) with a human operator available throughout extended daily hours (i.e. from 8:30 AM to 9:30 PM). The average operator response time is set at 150 seconds, whilst at least 40% of the calls should be answered within 20 seconds. [35]

Other countries use cross-sectoral regulations for call-centers. In Portugal[36], a cross-sectoral regulation forces the response time to be lower than 60 seconds once the call has been answered, and forces the availability of a personalized service during a number of pre-established hours.[37] Similarly in Spain, customer service via telephone channels must guarantee direct, personal attention at all times.[38] In France, the law requires waiting time on hold to be free of charge.[39] In Belgium, when the waiting time exceeds 2.5 minutes, the operator must

[33] Delibera 255/24/CONS, Adoption of discipline and quality indicators of customer service in the electronic communications and audiovisual media services sector.

[34] Resolution only applied to authorized communication and audiovisual services providers.

[35] In Italy, there is also a current law proposal under discussion for a cross-sectoral regulation on call-centres which includes obligations in terms of SLA even higher than the sectoral specific Agcom 255/2024 Resolution.

[36] Decree-law 134/2009, of 2 June 2009, establishes the legal framework applicable to the provision of marketing, information and support services for consumers and users through call centres; Law nº 134/2009; Decree-Law nº 59/2021, Provision and publicizing telephone lines for consumer contact.

[37] Art. 6 (2), Decree-law 134/2009 of 2 June 2009.

[38] Law 11/2022, of June 28, General Telecommunications Law (Spain).

[39] Law n°2008-3 of 3 January 2008 on competition and consumer protection (Loi Châtel)

offer the user the option to leave contact details and a short message. The helpline must call back by the end of the next working day, preferably at the time requested by the user. [40]

## Following the customer journey - Phase III: Customer churn

When users leave their provider, by switching or terminating the contract, they enter a regulatory zone shaped by contract duration rules, switching rights, and portability. The process is framed through at least six obligations, of which those related to i) contract duration & termination as well as ii) switching/portability have negative impact on both consumers and telecom operators.

### *i. Telecom specific contract duration and termination rules are not responding to a specific market failure and drive fragmentation*

The ending of a contract is ruled through contract duration and termination rules (art. 105 EECC). Contract duration and termination rules are being subject to detailed sector specific obligations for telecom operators, whilst big tech falls under the scope of horizontal law. (See Annex 1: Overlapping consumer protection rules: EECC vs. horizontal customer protection law**.)** Fragmentated implementations, whereby end-users are experiencing uneven protection across Member States, and gold-plating come on top, adding significantly more complexity for telecom operators.

As a general principle of law, sector-specific consumer rules should only be applicable when justified by specific needs of the market. Contract duration rules (as long as they do not act as a de facto “lock-in” or disincentive for change) and termination rules can be effectively addressed through horizontal consumer protection rules.

Under Article 105 of the EECC, telecom contracts are capped at 24 months, during which termination fees are implicitly allowed. After automatic renewal, consumers must be allowed to terminate at any time with a maximum one-month notice, and without incurring any costs except the charges for receiving the service during the notice period. Big tech are not facing similar obligations, whether they are NI-ICS or not, see Table 5 in Annex 3: Asymmetrical consumer protection.

Some Member States have gone beyond the EECC’s harmonized standard for both contract duration and early termination.

- With regards to contract duration, Denmark, for instance, imposes a 6-month limit for consumers[41]. Germany[42], similarly to some other Member States (France[43], Croatia, Italy, the Netherlands, Poland, and the UK) still apply legacy rules, originally introduced under the now-repealed Universal Service Directive, to maintain the availability of at least one 12-month contract option. [44]

[40] Art. 116 of the law of 13 june 2005 concerning electronic communications.

[41] Art. 4, Act on Electronic Communications Networks and Services (Denmark); Art. 7, Executive Order No. 566 of 24 May 2023 on End-User Rights in the Telecommunications Field (Denmark).

[42] Sec 56(1) sentences 1 and 2 Telecommunications Act (Telekommunikationsgesetz, *TKG*).

[43] Law n°2008-3 of 3 January 2008 on competition and consumer protection (*Loi Chatel*).

[44] Feasey, R., Alexiadis, P., Bourreau, M., Cave, M., Godlovitch, I., Manganelli, A., Monti, G., Shortall, T., De Streel, A., & Timmers, P., *Ideas for the future of European telecommunications regulations*. CERRE, 2024.

- With regards to early termination (fees), the Belgian legislator has added an additional layer of consumer protection regarding early termination. After the sixth month following the commencement of the fixed-term contract, telecom operators are not allowed to ask for an early termination fee anymore.[45] In France, when a consumer terminates a 24-month mobile contract early, the law limits the financial penalties that may be imposed. If the cancellation occurs after the 12th month, the consumer is liable for only 25% of the remaining subscription and service fees through the 24th month. Another example of additional obligations on top of the EECC stems from Italy's Decreto Bersani (Law No. 40/2007). The EECC provides that, after an automatic prolongation of a fixed duration contract, end-users are entitled to terminate the contract at any time with a maximum one-month notice. However, Article 1(3) of the Decreto Bersani grants consumers the right to withdraw from telecom contracts or switch providers at any time (notwithstanding any automatic prolongation, i.e. even during the initial fixed contract term), without unjustified delays or costs, and prohibits operators from imposing notice periods longer than 30 days. It also forbids any fees that are not strictly justified by the operator's actual costs. (See deep-dive Decreto Bersani in Annex 4: Divergent consumer protection implementation).

### *ii. Provider switching and number portability obligations do not apply to big tech*

When customers churn and change provider, switching and number portability procedures (art. 106 EECC) apply. Under Article 106 of the EECC, telecom operators are required to ensure seamless provider switching, including number portability, without service interruption. These rights are enforced across the EU to protect consumers from switching barriers and to promote competition.

By contrast, big tech are not subject to these rules and have therefore no equivalent "messenger portability", "email-address portability" or "cloud-storage portability" obligation (see Annex 3: Asymmetrical consumer protection). Users cannot message across platforms, and they cannot take their messaging history, contacts, or identifiers with them when switching. This creates a functional lock-in, even in cases where services are free of monetary cost. While switching fees do not apply, network effects and the absence of technical portability options make it difficult for users to move away from dominant services. While the Data Act and the Digital Markets Act begin to address data and platform portability, their scope is limited, e.g. to gatekeepers, and does not yet create a level playing field with telecoms.

This regulatory asymmetry undermines fair competition and contributes to user inertia. Customers may assume equivalent protections exist across services offering similar communication functions, which is not the case when Telecom operators must comply with strict switching rules.

## Obligations that are transversal to the customer journey

Several obligations have an impact throughout the whole customer journey, concentrated around i) nationally security-driven restrictions on remote access, asset localization and security clearance, cybersecurity risk management measures and ii) incident reporting ensure security.

[45] Art. 111/3, Act of 13 June 2005 on electronic communications (ECA), Belgium.

### *i. Nationally-driven security restrictions that fragment telecom operations*

Nationally imposed security requirements, covering asset localization, restrictions on remote access, and national security clearance create "sovereignty silos" in telecom operations. These rules compel operators to deploy infrastructure and personnel separately in each Member State, blocking the use of centralized or shared systems across borders. The result is increased capital and operational expenditure, reduced flexibility, and duplication of security resources. This fragmentation also has implications for end-users. As network resilience increasingly depends on the ability to reroute traffic and shift operations dynamically during outages or cyberattacks, such restrictions constrain operators' ability to respond effectively. The limitations contradict the EU's ambition for a unified Digital Single Market, as set out in Article 3(2)(c) of the EECC.

**Fragmentation of telecom operations and weakened resilience due to asset localization, remote network access and security clearance**

Telecom operators deploying cross-border infrastructures or seeking to operate distributed network functions face significant obstacles due to divergent national requirements on asset localization and restrictions on remote network access:

- In Sweden, core network functions must be physically located and managed within Swedish territory at all times, even during emergencies. Remote operational access from abroad is prohibited, even for read-only access.
- Norway allows limited cross-border failover, but operators must first secure pre-approval from the National Security Authority, potentially delaying emergency responses.
- Denmark permits failover to data centers elsewhere in the EU but imposes strict limitations on routing traffic through third countries.
- Finland requires that critical communication systems and its control and management must be capable of returning inside national borders without delay if emergency powers are used.
- In Germany, Section 110 TKG requires telecom companies to maintain interfaces for judicially ordered interception and to transmit intercepted data directly to German law enforcement. The detailed Telecommunications Surveillance Ordinance (TKÜV) and Bundesnetzagentur technical guidelines specify the technical and organizational steps operators must take (i.e. essentially pre-installing interception points and interfaces so that German authorities can immediately tap communications when authorized). This means a provider can't rely on a centralized interception system in another country, it must host interception equipment locally in Germany to comply. This also means that the lists of targets of legal interception cannot be shared across jurisdictions in different Member States, hampering the effectiveness of legal interception instruments in cross-border cases.
- In Croatia, telecommunications operators must ensure a permanent and direct access to facilities and technical equipment in order to facilitate lawful intercept for the national state authority .

In addition, telecom operators maintaining cross-border infrastructures, or wanting to use scarce skilled workforce in multiple countries face considerable burdens arising from divergent national security clearance rules. Personnel performing identical operational tasks across borders must often undergo multiple separate national clearance procedures, increasing delays and costs. Critically, this fragmentation weakens crisis preparedness by hindering the rapid deployment of trusted personnel across national borders during emergencies.

- Sweden imposes strict role-specific clearance procedures ("Säkerhetsprövning" and "Registerkontroll"), tying authorizations to particular posts involving classified information. Clearances are not portable across roles or organizations.

- Denmark and Norway recognize foreign clearances but maintain country-specific procedures and requirements for access to critical network elements.
- Finland requires security clearance for personnel having physical or logical access to critical parts of the mobile network or other key communications networks.

**Fragmented transposition of cybersecurity rules turn risk management into compliance overload**

Another growing source of divergence stems from the national transpositions of Article 21 of the NIS2 Directive and DORA, which imposes risk management obligations on essential entities, including telecom operators. While the Directive sets out a common baseline, requiring operators to take appropriate and proportionate technical, operational, and organizational measures to manage cybersecurity risks, the actual interpretation and implementation vary significantly across Member States in scope, prescriptiveness, and oversight mechanisms.

In some jurisdictions, these requirements are being implemented through detailed national guidelines or sector-specific regulations, often adding additional layers of reporting, auditing, or compliance documentation. For example, Germany has introduced highly detailed requirements through its IT-Sicherheitsgesetz 2.0, which applies to “critical infrastructure operators” (KRITIS) and mandates extensive risk documentation, internal audits, and technical certifications, including for telecom entities.

Meanwhile, countries like Italy and France are aligning NIS2 implementation closely with existing national security legislation. France, through ANSSI, maintains sector-specific cybersecurity risk requirements that go beyond NIS2’s minimum - especially for operators of vital importance (OIVs), which often overlap with telecom-related assets and services.

This fragmentation means that telecom operators active in multiple countries face duplicative or conflicting risk assessment methodologies, reporting formats, and technical control baselines. For example, one country may require the cross sectorial global ISO 27001 certification, while another mandates bespoke national frameworks or mandatory registration of security officers and critical suppliers.

Fragmented obligations on cybersecurity risk management obligations lead to a compliance-heavy environment through duplicative or conflicting risk assessment methodologies, reporting formats and technical control baselines. The compliance-heavy regulation leads to risk governance being sometimes reduced to a box-ticking exercise, pulling security teams away from actual threat detection and risk management.

### *ii. Compliance heavy incident reporting for security incidents undermines user protection*

Due to differing national implementations, operators must report security incidents across Member States under different thresholds, timelines, and formats, even when the incidents are the same. Even within Member States, regulatory overlap exists, with reporting obligations to several national authorities. This patchwork of incident reporting measures forces operators to report incidents at different thresholds and timelines through different countries, tailoring the depth, terminology and format of their reports across jurisdictions, even if the core information overlaps. To end-user security is impacted by allocation of scarce time of qualified security personnel, that is being used for compliance due to national fragmentation of incident reporting.

NIS2 requires entities to notify, “without undue delay” any incident that has a “significant impact” on the provision of their services.” (Article 23 NIS2). Whilst the directive has not yet been fully transposed into national law across the EU, current NIS2 transpositions suggest that divergence will persist, with some countries introducing stricter timelines, broader definitions, or additional reporting obligations.

For example, some Member States are already proposing stricter or broader rules: Cyprus requires early warnings within six hours of detection; the Czech draft law expands reporting obligations beyond significant incidents; and Slovakia includes mandatory notifications for prevented threats and unresolved vulnerabilities in publicly accessible systems. These developments echo the same issues of fragmentation seen under Article 40 EECC, particularly around the definition of a reporting threshold (“significant incident”) and timelines. See Annex 6: National Fragmentation in incident reporting for security incidents.

In addition to differences in thresholds and timelines, Member States are also diverging in the level of detail and structure required for the content of incident notifications. While NIS2 defines a shared baseline (i.e. early warning, initial notification, and final report) the practical implementation varies in terms of how prescriptive, standardized, or operationalized these requirements are.

For example, Belgium’s Centre for Cybersecurity (CCB) has published detailed templates that specify what must be included at each reporting stage, including fields such as threat type, cross-border impact, technical indicators, and mitigation status (link). Germany’s draft NIS2 transposition law outlines similar stages (early report, 72-hour update, final report), but with fewer structured guidelines on content format. France’s ANSSI similarly follows the Directive’s reporting logic but relies more on case-by-case interaction with operators than on formal reporting templates.

## Following the customer journey - Conclusions

Based on the aforementioned examples, it can be concluded that the analyzed regulation consolidates into the undermining of the initial customer protection regulation ambition, as well as unbalanced extra costs for telcos.

The current issues can be summarized into three main challenges:

- Overregulation, often stemming from overlapping sector-specific and horizontal rules, can lead to inconsistency or additional rules being imposed to protect customers but ultimately creating confusion or limiting operators' ability to meet customer needs
- An uneven playing field, with asymmetries versus big tech, might leave consumers without equivalent protections, as equivalent services are subject to different obligations depending on whether they are delivered by telecom operators or digital platforms
- Fragmentation arising from various national implementations of EU directives results in inconsistent consumer rights and experience across Member States

# 3. POLICY RECOMMENDATIONS

Previous sections of this report demonstrated how Europe's telecom regulatory framework is marked by the challenges created by regulatory complexity that has an impact throughout the whole end-user journey. This chapter links the regulatory issues to specific recommendations on legislative action and presents a set of priority technical policy recommendations aimed at creating a more competitive Europe while safeguarding the end-user journey and advancing Europe's objectives in digital resilience (see Table 2):

- Overregulation calls for simplification of obligations
- Achieving a level playing field between telecom providers and native digital service providers can be pursued in two ways: (1) reduce or simplify obligations where existing rules have become disproportionate or outdated; and (2) justified, up-to-date, and relevant obligations need to be extended to actors that currently fall outside the regulatory framework
- Fragmentation should be addressed through the realization of the unified Digital Single Market

The revised EU telecom framework must address the recommendations from the Draghi report and the European Competitiveness Compass to reflect and to complement the goal of increasing competitiveness in the set of policy objectives.

**Table 2: Overview of main policy recommendations**

| Priority Area | Simplification | Leveling the playing field | Realization of the DSM | Policy Recommendations |
|---|---|---|---|---|
| 1) Universal Service Obligation (USO) | ✓ | ✓ | | Abolish USO sector specific provisions and shift to targeted public funding when needed (e.g. vouchers) |
| 2) Customer protection (Information & transparency) | ✓ | ✓ | ✓ | Rely on horizontal customer protection rules; restore harmonized implementation and level playing field. |
| 3) Net neutrality | | ✓ | ✓ | Provide by EC clarity for specialized services,<br>Reconsider net neutrality rules to take into account the broader ecosystem |
| 4) Data protection & privacy | ✓ | ✓ | ✓ | Rely on horizontal legislation (the GDPR) for incident reporting and the processing of traffic and location data; Restore level playing field regarding confidentiality of communications |
| 5) Customer complaints management / Helpdesk | | | ✓ | Strengthen harmonization |
| 6) Customer protection (contract duration and termination) | ✓ | | ✓ | Rely on horizontal customer protection rules; harmonize implementation |
| 7) Customer protection (switching and number portability) | | ✓ | | Application based on service-functionality to big tech |
| 8) National security requirements (remote access, asset localization and security clearances; cybersecurity risk management measures) | ✓ | | ✓ | Ensure mutual recognition of security clearances, audits, and certifications across Member States and base implementation of security requirements on international standard to facilitate cross-border operations; Repeal provisions in sector-specific regulations which overlap with similar provisions in horizontal ones, such as NIS2; Ensure that compliance with NIS2 is deemed sufficient where other legislation imposes similar cybersecurity obligations (presumption of conformity |
| 9) Security (Incident reporting) | ✓ | | ✓ | Harmonize and streamline reporting obligations, templates, and interpretation across incident reporting frameworks |

Source: Arthur D. Little

## REGULATORY SIMPLIFICATION

Simplification of regulation is essential wherever consumer protection can be preserved, or even enhanced through horizontal rules, improved coordination, or better-targeted sector-specific measures.

**Address overlaps between sector-specific and horizontal legislation**

The legislator must undertake a comprehensive rationalization of the regulatory framework for electronic communications.

- **Rely on horizontal consumer information & transparency obligations and contract duration and termination** by removing sector specific requirements under the EECC and rely on horizontal consumer protection. (Pre)-contractual information and transparency rules should focus on information that directly enables consumer decision-making, rather than overly technical disclosures.
- **Simplify breach notification frameworks** through the suppression of incident reporting obligations and repeal the e-Privacy directive. Introducing a single, consistent standard for telecom providers could help reduce duplication and inconsistencies in thresholds and reporting requirements.
- **Clarify the relationship between sector-specific and horizontal rules, and abrogate sector specific redundant rules.** For matters already addressed by GDPR, the horizontal consumer protection regulation, or by NIS2 for security, horizontal regulation should serve as the primary framework and sector specific rules should be withdrawn. The adoption of new sector-specific rules should be reserved for cases of demonstrated necessity, only when sectoral risk profiles or market failures justify them. More specifically, only the principle of confidentiality of communications would remain unaddressed under current horizontal law; specific provisions on this matter could be incorporated in upcoming legislations to ensure consistent application among Member States and across the digital ecosystem.

A unified, streamlined regulatory framework would reduce compliance costs, lower legal uncertainty and increase transparency versus consumers.

**Abolish universal service obligations**

The Universal Service regime should be eliminated to reflect market realities and technological developments.

- **Abolish USOs** because market conditions ensure coverage and affordability, and r**eplace operator-funded USOs with targeted public funding models when needed**, through the use of broadband vouchers or targeted state aid to support connectivity.[46] This approach would ensure that public policy focuses on actual affordability challenges without penalizing telecom operators, and safeguarding the benefits for the customer to decide what operator to use the voucher with.

## ENSURE A LEVEL PLAYING FIELD

The principle of functional equivalence should be applied thoughtfully to ensure that users benefit from consistent levels of protection across services that are substitutable in practice, while avoiding unnecessary extension of legacy obligations. Rather than replicating telecom-specific rules across all actors, the priority should be to re-evaluate whether existing sector-specific obligations remain proportionate and necessary considering modern, horizontally applicable regulations. A more balanced and future-oriented regulatory approach would seek to strengthen competitive neutrality by simplifying the regulatory landscape, addressing gaps where they exist, and aligning obligations to reflect the converged nature of services.

[46] Voucher schemes have already been successfully implemented in some Member States to connect remote communities using satellite digital connectivity. Under such a scheme, a public authority provides financial aid (a voucher) to eligible end users with which they can 'pay' a registered service provider of their choice for the purchase, installation and activation of satellite user equipment. The service provider seeks reimbursement of his costs from the public authority implementing the scheme.

**Extend "necessary" customer protection and privacy protection obligations to big tech offering functionally equivalent services**

The following rules should be extended to big tech:

- Provider switching rules
- Principle of confidentiality of communications

**Clarify net neutrality to create a pro-investment regulation and assess the need to extend its principles to the broader digital value chain**

Europe's regulatory framework must actively enable innovation in network technology, business models, and consumer offerings.

- **Provide by EC clear regulatory guidelines for specialized services**, incl. a whitelist of use cases that are considered as "specialized services". Clear guidance would support the development of new services while maintaining compliance with net neutrality principles
- **Extend the principles of the OIR to** the broader digital value chain, especially operating systems

Leveling the playing field removes unjustified advantages and restores fair competition based on innovation, quality, and trust.

## HARMONIZE IMPLEMENTATION, STRENGTHEN COORDINATED ENFORCEMENT AND REDUCE FRAGMENTATION OF THE DIGITAL SINGLE MARKET

Next to simplification and elimination of unnecessary obligations, fragmentation of rule interpretation and application across Member States must be addressed to realize the Digital Single Market's full potential.

- **Prioritize the use of directly applicable EU regulations** over directives in future telecom and digital legislation .
- **Reassess the institutional framework** to improve regulatory consistency across Member States.
- Ensure **mutual recognition of requirements across Member States**, and promote **international standards** to ease compliance.

Uniform interpretation and enforcement would help operators to design cross-border offers efficiently, fostering consumer trust and promoting competition, preserving the integrity of the Digital Single Market and maintain regulatory consistency.

# 4. CONCLUSION: TOWARDS A SIMPLIFIED, COMPETITIVE AND HARMONIZED EUROPEAN FRAMEWORK

The European Union’s telecom regulatory framework, which supported liberalization, competition, and consumer choice over past decades, is increasingly misaligned with today’s market and technological realities. Layered, fragmented, and asymmetrical obligations have created a complex compliance environment that limits operators' flexibility, slows down innovation, and undermines their ability to invest at scale.

But this is not just an industry issue: the regulatory status quo directly shapes the quality, accessibility, and consistency of the digital experience for millions of European end-users. From onboarding to switching, outdated and inconsistent rules are making connectivity services harder to understand, compare, and trust. A modernized and leaner framework must therefore place the user journey at its core - empowering end-users through simpler protections, more innovation, and consistent rights across the Single Market.

At the same time, the EU’s Digital Decade targets based on four pillars (digital skills, developing secure digital infrastructures, digitizing business, transforming public services) - cannot be achieved without a strong, agile, and investment-ready telecom sector at their foundation.

In light of the evidence and case studies presented in this report, a comprehensive review of the current framework is urgently needed. This review should focus on five core areas:

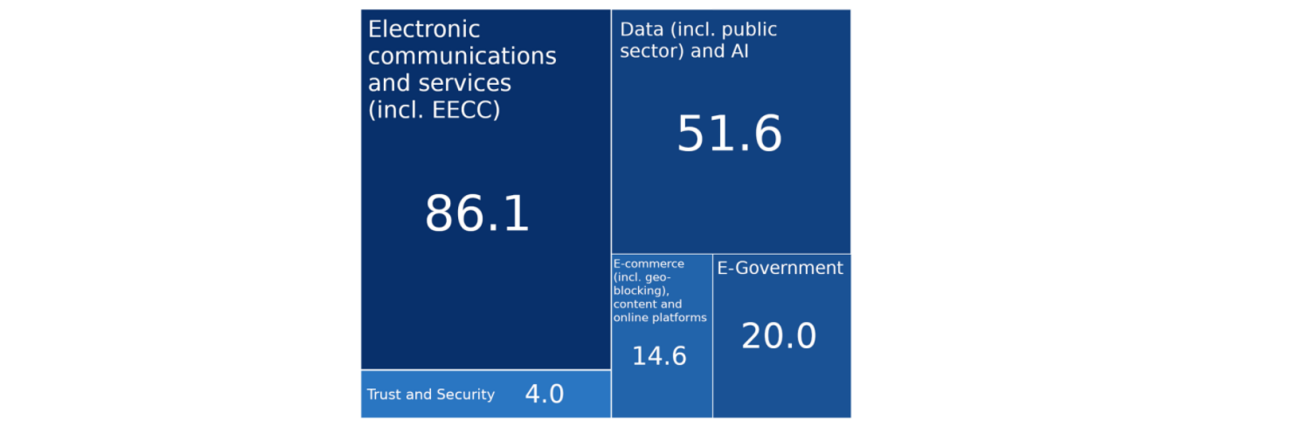
- Rationalizing and aligning obligations to eliminate duplication and legal uncertainty
- Ensuring competitive neutrality across functionally equivalent services
- Harmonizing implementation and enforcement across Member States to reduce fragmentation
- Repealing outdated obligations, no more required in an evolved digital context
- Enabling innovation and investment through a future-proof and proportionate regulatory approach

A coordinated update to the rules is essential to unlock innovation, enabling scale, and restoring competitiveness in Europe’s currently challenged connectivity sector more coherent, user-centric, and future-ready telecom framework will not only support the Digital Decade but will also ensure that end-users across Europe benefit from trusted, high-quality, and resilient digital services - regardless of where they live or which provider they choose.

As Telecoms markets have fiercely evolved since the many regulations entered into force, it has become urgent to reassess the patchwork of obligations applying to operators, to improve harmonization and simplify them wherever possible to ensure they allow the sector to meet the next decade's challenges - especially 5G rollout, and cross-border service scaling – it must be simplified and harmonized. A streamlined, future-proofed, and innovation-enabling framework would support investment, ensure fair competition, and deliver consistent rights to users across the European Union.

# 5. APPENDIX

**Figure 13: Annual benefits (billion €) of Digital Single Market for the European Union**




Source: Bruegel, based primarily on European Commission Impact Assessment reports (2017)

# ANNEX 1: OVERLAPPING CONSUMER PROTECTION RULES: EECC VS. HORIZONTAL CUSTOMER PROTECTION LAW

**Table 3: Comparison of consumer protection obligations: EECC vs horizontal customer protection**

| Obligations | Horizontal customer protection | EECC |
|---|---|---|
| Contractual Information | Required (Art. 5–6 CRD): basic service description, price, terms… | Required (Art. 102)[47]: very detailed, including internet speeds, remedies[48] |
| Transparency obligations and comparison tools | General principle, no comparison of offers required | Specific disclosures about speed, restrictions, minimum QoS, and comparison tools (Art. 103-104 EECC). |
| Provision of a Contract Summary | Not required | Mandatory standard template (per Implementing Regulation (EU) 2019/2243) |
| Contract duration and termination | Does not specify maximum contract durations but ensures consumers are informed about the duration and termination conditions of the contract. | Maximum contract duration of 24 months. After automatic prolongation, end-users can terminate at any time with up to one month's notice, incurring no costs beyond service charges during the notice period. |
| Switching Provider | General right to freedom of choice implied | Detailed rules: deadlines, no service interruption, number portability (Art. 106) |

Source: Arthur D. Little

[47] Incl. annexes VIII & IX of the EECC.

[48] The Open Internet Regulation adds additional transparency requirements on top, related to specific quality of service KPIs.

## ANNEX 2: OVERLAPPING DATA PROTECTION OBLIGATIONS

To implement Article 4 of the ePrivacy Directive, the Commission adopted Regulation (EU) No 611/2013, which standardizes the breach notification process for telecom providers. Under this regulation, providers of public electronic communications services must notify the competent national authority of any personal data breach within 24 hours of detection, using a common format. In case information is not available immediately, a staged reporting process allows for a complete notification within three days.

Additionally, providers must notify affected users without undue delay if the breach is likely to affect their privacy. Article 4 of the Regulation also introduces an exemption from user notification when robust encryption or other protective measures are in place.

However, telecom operators must also comply with Article 33 of the GDPR, which applies to all sectors and mandates notification to the Data Protection Authority (DPA) within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms. Article 34 further requires notifying individuals if that risk is deemed "high."

**Table 4: Comparison of GDPR vs e-Privacy breach notification obligations**

| Aspect | GDPR | ePrivacy + Regulation 611/2013 |
|---|---|---|
| Sectoral scope | All sectors | Telecom operators only |
| Threshold for notification | High risk to rights and freedoms | Any personal data breach |
| Authority notified | Data Protection Authority | National telecom regulator |
| Notification deadline | 72 hours | 24 hours (initial), +72 hours if staged |
| Individual notification trigger | “High risk” | “Likely to affect privacy or data” |
| Notification format | DPA-specific | Standard format (Annex I/II) |
| Encryption-based exemption | Considered case-by-case | Explicit exemption under Article 4 |

Source: Arthur D. Little

## ANNEX 3: ASYMMETRICAL CONSUMER PROTECTION

Traditional telecom operators must comply with robust consumer protection obligations codified in the European Electronic Communications Code (EECC). Whilst the EECC has brought NI-ICS under its general scope, NI-ICS are mostly exempted of EECC demand side rules:

- Telecom operators remain fully bound by the EECC's suite of consumer-protection rules, from mandatory contract information (Art. 102) through transparency and comparison-tool obligations (Arts. 103.2 & 103.4), contract duration and termination limits (Art. 105), seamless switching and number-portability (Art. 106), emergency-call access (Art. 109), and cell-broadcast public warnings (Art. 110).
- By contrast, NI-ICS providers (e.g. Messenger, WhatsApp) only answer to the Art. 102 contract-information requirement, 103.1 on transparency & publication of information and information on QoS (art. 104 EECC). Interoperability or switching rules should also apply to NI-ICS, because these rules are necessary from a consumer perspective regardless of the use of a number.
- Big tech that are not NI-ICS (e.g. Netflix, Spotify, TikTok) only need to comply with horizontal customer protection regulation.

**Table 5: Telecom operators and big tech consumer protection obligations**

| Main consumer protection obligation (EECC Reference) | ISP & NB-ICS | Big tech (NI-ICS)[49] | Big tech (non-NI-ICS) |
|---|---|---|---|
| Art. 102 - Contract Information | ✓ | ✓ | |
| Art. 103.1 – Transparency & Publication of information | ✓ | ✓ | |
| Arts. 103.2 & 103.4 – Comparison Tools | ✓ | | |
| Art. 104 – Quality of Service | ✓ | ✓ | |
| Art. 105 – Contract Duration & Termination | ✓ | | |
| Art. 106 – Provider Switching and Number Portability | ✓ | | |
| Art. 109 – Emergency Communications Access | ✓ | | |
| Art. 110 – Public Warning Systems | ✓ | | |

Source: Arthur D. Little

[49] If offered for free. When NI-ICS are on payment, they are included under the scope of the comparison tools.

## ANNEX 4: DIVERGENT CONSUMER PROTECTION IMPLEMENTATION

The EECC follows the principle of "maximum harmonization" for consumer protection rights (Article 101 EECC), meaning Member States generally cannot impose rules that are either stricter or more lenient than what the directive prescribes. However, the directive allows for certain exceptions. Some adjustments reflect local market conditions, while others may introduce additional requirements beyond the harmonized framework. Divergences should be assessed to ensure they address genuine national needs, as they risk fragmenting Single-Market consistency.[50]

**Maximum contract duration and termination fees**

**Case study #1 – The *Decreto Bersani* in Italy**

**Italy's 2007 Decreto Bersani (Law No. 40/2007)** introduced some of the EU's earliest and strongest telecom consumer protections. It granted consumers the right to cancel telecom contracts at any time without penalties, limited fees for early termination to actual operator costs, and banned disconnection fees unless objectively justified. It also ensured prepaid SIM credit could not expire and mandated its transferability when switching providers. Finally, it prohibited commission fees on prepaid top-ups, making Italy the first EU country to eliminate such charges completely.

Some of these provisions have since been mirrored by the EECC (Articles 105 and 106), which harmonizes early termination, switching, and credit refund rights across the EU.

However, Italian consumer rights continue to shape a national regime that is more protective than the EU framework. The EECC provides that, **after** an automatic prolongation of a fixed duration contract, end-users are entitled to terminate the contract at any time with a maximum one-month notice (art 105(3) EECC). Article 1(3) of the *Decreto Bersani* grants consumers the right to "withdraw from the contract or to transfer the utilities to another operator without time constraints or unjustified delays and without expenses not justified by the operator's costs (...).", therefore including the right to terminate the contract **at any point**, even during the initial fixed contract term. The *Decreto Bersani* further states that "the costs relating to the withdrawal or transfer of the user to another operator are commensurate with the value of the contract and the real costs borne by the company (...) and in any case made known to the consumer at the time of advertising the offer and during the signing of the contract." This represents a stricter consumer protection standard than the EECC, which allows providers to claim fees reflecting the remaining value of the contract during the initial fixed contract term.

Additionally, the Bersani ban on top-up recharge fees remains a uniquely Italian rule, as the EECC does not regulate prepaid pricing structures. Today, these consumer rights remain in force in Italy and continue to shape a national regime that is more protective than the harmonized EU framework.

**Transparency obligations**

Another example of persistent national divergence relates to several transparency rules.

[50] Feasey, R., Alexiadis, P., Bourreau, M., Cave, M., Godlovitch, I., Manganelli, A., Monti, G., Shortall, T., De Streel, A., & Timmers, P., *Ideas for the future of European telecommunications regulations*. CERRE, 2024.

- **Publication of contractual information:** In Austria, the law obliges providers with fewer than 350,000 end-users to notify their general terms and conditions to the regulator[51]. Additionally, transparency rules require providers to notify changes to terms and conditions two months in advance, unless the changes clearly benefit users. This exceeds the one-month period required by EECC Article 102. Germany requires communication providers to issue a product information sheet with key contractual details prior to contract conclusion.[52] This goes beyond EECC which requires precontractual information in the form of a contract summary. In Germany both documents have to be provided. In Italy, all end-user information has to be provided in accessible formats to users with disabilities by default, not just on request as foreseen in the EECC.[53]

- **Publication of QoS information:** Article 104 EECC limits quality of service (QoS) obligations to publicly available interpersonal communications services (ICS) only if they control some network elements, directly or via a service-level agreement. However, France, Germany, and Italy do not apply this exemption, imposing QoS obligations on ICS providers regardless of network control. This contradicts the EECC's approach, which recognizes that providers without network control cannot guarantee or remedy QoS issues, making such obligations impractical.[54] Under §§ 52–54 TKG, operators must provide consumers not only with standardized contract summaries, but also with detailed information regarding actual, maximum, and minimum internet speeds for broadband services. Consumers have the right to independent speed measurement tools and can demand contract termination or price reductions if promised speeds are not achieved. Platforms such as Breitbandmessung.de are officially recognized for these purposes.

[51] Sec 6 Abs 1 TKG 2021

[52] §§1–2 of the Telecoms Transparency Regulation

[53] Article 98 of the transposing law (Legislative Decree No. 207/2021)

[54] *Improving Member States' approaches to number-independent services in light of the EECC*, Digital Europe, 2022

## ANNEX 5: INCONSISTENT APPLICATION OF NET NEUTRALITY RULES

The enforcement of net neutrality rules varies across the Union, adding complexity and regulatory uncertainty for operators.

While the Open Internet Regulation establishes a set of common principles, national regulatory authorities (NRAs) apply differing interpretations, particularly in areas such as specialized services, traffic management practices, and the relationship between innovation and non-discrimination.

This variation in implementation creates differences in compliance requirements across Member States and may contribute to uncertainty and a chilling effect for launching innovative service offerings.

To assess the extent and nature of this fragmentation, the table below compares NRA positions across three key dimensions:

- The “Position on Specialized Services” captures the general attitude of the regulator – whether it tends to be restrictive, moderate, or flexible in its interpretation of what services may qualify as specialized. A restrictive position implies a narrow reading of the regulation, where few differentiated services are allowed. A moderate stance indicates conditional acceptance or reliance on case-by-case assessments. A flexible position suggests a more innovation-friendly approach, where regulators actively engage with operators to enable such services.
- The “Traffic Management Rules” column describes the extent to which regulators allow operators to differentiate traffic – for example, offering low-latency services – and under what conditions. The language used in this column is harmonized to clarify whether such differentiation is permitted only when specific safeguards are met (e.g., no degradation of the open internet).
- In “Ex-Ante Guidance from NRA,” we assess whether operators can obtain advance clarity before launching a service. Some regulators provide formal, transparent procedures; others operate on a case-by-case basis without formal frameworks. In some countries, the absence of clear guidance leads to significant legal uncertainty and risk aversion by operators.
- The “Notes” column provides brief qualitative insight into how the regulatory stance is applied in practice – drawing on known examples such as the treatment of 5G slicing or the practical hurdles encountered in launching differentiated B2B services.

**Table 6: Overview on diverging positionings of NRAs concerning Net Neutrality**

| Country | Position on Specialized Services | Traffic Management Rules | Ex-Ante Guidance from NRA | Notes |
|---|---|---|---|---|
| Italy | Restrictive | Allows limited exceptions under strict interpretation | Minimal guidance published | Raises uncertainty over 5G slicing compliance; operators act cautiously. |
| Germany | Restrictive | Strict/narrow interpretation of OIR rules | Not known | Strong reluctance among ISPs due to legal and economic risks (fines and lost development costs) |
| Belgium | Moderate | Applies BEREC-aligned guidance with cautious flexibility | Some guidance provided by BIPT | Follows EU baseline; NRAs intervene conservatively. |
| France | Moderate | Allows managed services if technically separated | Case-by-case basis via ARCEP | Enables B2B slicing where isolation is demonstrated. |
| Spain | Moderate | Does not apply flexible interpretation of permitted exceptions | No formal ex-ante mechanism | Does not foster new offers due to perceived legal uncertainty. |
| Portugal | Moderate | Allows differentiation for services with specific QoS needs | Some NRA interaction possible | Limited public information on enforcement stance. |
| Austria | Restrictive | Allows on case-by-case basis; slicing flagged for future review | Regulatory caution advised by RTR | Airport 5G slicing under review; risk-averse stance persists. |
| Sweden | Restrictive | Enforces neutrality strictly, with minimal allowances | Little ex-ante clarity | Operators avoid managed service offers due to stringent neutrality enforcement. |
| Finland | Moderate | Allows differentiation for enterprise services if transparent | Cooperative NRA approach | Favors innovation where open internet is not degraded. |
| Denmark | Restrictive | Enforces neutrality conservatively | Minimal public guidance | Operators avoid specialized service models due to enforcement ambiguity. |
| Norway | Moderate | Applies neutral but pragmatic case-by-case enforcement | Some NRA interaction possible | Case-by-case flexibility when requested supports tailored innovation. |

Source: Comparative national law analysis, Arthur D. Little

### Divergent approaches to specialized services

In Austria, the regulator (RTR) has adopted a cautious interpretation of the European framework. For instance, an Austrian airport deployed a 5G network slice dedicated to secure staff communications. Because the same infrastructure also provided limited internet access for passengers, the NRA initiated a review of the deployment. While the service was temporarily tolerated, RTR indicated that offering general internet access alongside prioritized services could raise neutrality compliance concerns.

In the Netherlands, the regulator (ACM) applies a particularly restrictive approach to net neutrality. Any form of differentiated traffic management, even when technically justified, such as for low-latency applications like gaming or telemedicine, is examined closely. Specialized services are generally accepted only under narrow conditions, and bundling risks being interpreted as discriminatory.

In France, ARCEP has acknowledged the potential of 5G slicing and sector-specific applications. It has stated that network slicing could be compatible with neutrality rules if functionally separated and if the general quality of internet access is preserved. However, operators report that procedures to obtain regulatory clarity remain complex and time-consuming.

In parallel, a few regulators – notably in France and Finland – have demonstrated a pragmatic openness toward more flexible treatment of B2B connectivity services. While not formally exempting business users from net neutrality rules, these NRAs acknowledge that certain enterprise use cases (e.g., 5G slicing for hospitals, manufacturing, or transport hubs) may require differentiated treatment that does not compromise the open

internet. Such services are often non-public, technically isolated, and tailored to mission-critical needs, making them candidates for a lighter regulatory approach. This de facto flexibility has encouraged early deployment of advanced B2B services, even though legal uncertainty remains in the absence of explicit exemptions.

**Divergent approaches to traffic management**

The Swedish regulator (PTS) applies a strict interpretation of what qualifies as “reasonable” traffic management. Measures such as application-aware optimization, e.g., prioritizing video streams under network congestion, are examined closely, even when intended to improve user experience.

In contrast, the Finnish regulator (Traficom) has shown more openness toward allowing intelligent traffic management practices, provided they remain transparent and maintain non-discriminatory access conditions.

# ANNEX 6: NATIONAL FRAGMENTATION IN INCIDENT REPORTING FOR SECURITY INCIDENTS

As the NIS2 Directive has not been implemented yet in most countries, an analysis of national interpretations and implementation of art. 40 (2) EEC (which stated very similarly that telecommunication providers must “notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.”) show what might become:

- The thresholds “significant impact”[55] varies in terms of number of impacted users and duration of the incident. In some countries (e.g., Netherlands), no explicit definitions exist, while countries like Italy and Belgium provide detailed thresholds (e.g., number of users and incident duration). Others like France, Austria and Greece rely on general principles or undefined legal terms.

- At the same time, deadlines for incident notification vary. France requires notification "as soon as the provider becomes aware of the breach" (Art. L. 33-1 CPCE), whereas Italy imposes a fixed 24-hour limit (Decree of 12 December 2018), and in some national security-related cases, even within one hour (Decree 81/2021). Germany’s law (§168(1) TKG), interpreted through §121 of the German Civil Code, equates “unverzüglich” with a requirement to act “without intentional or negligent delay.” This diversity in language and underlying legal tradition introduces uncertainty for providers operating in multiple jurisdictions.

[55] Art. 40.2: In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:
(a) the number of users affected by the security incident;
(b) the duration of the security incident;
(c) the geographical spread of the area affected by the security incident;
(d) the extent to which the functioning of the network or service is affected;
(e) the extent of impact on economic and societal activities

**Table 7: Comparative analysis of notification for significant impact on networks or services**

| Country | "Undue delay" | "Significant impact" |
|---|---|---|
| **Italy** | 24h for general incidents; 1–6h for national security | Detailed thresholds: % of users affected and duration (e.g. 15% of national users during >1h, 1% users during >8h) |
| **Belgium** | Immediately upon detection | ≥25,000 users affected >1h; disruption to emergency services or critical infrastructure |
| **Germany** | Without intentional or negligent delay | Criteria-based: number of users, duration, geographic spread, social/economic impact |
| **Austria** | Without culpable hesitation | Impacts on availability, confidentiality, integrity, or authenticity |
| **Denmark** | Without undue delay (not further defined) | Based on availability, confidentiality, and integrity; no specific thresholds |
| **Greece** | Not defined | Broad: "significant impact" or "particular risk"; no measurable thresholds |
| **France** | As soon as provider is aware of the incident | No thresholds; relies on general detection of security breach |
| **Netherlands** | Without undue delay (not further defined) | Not defined; general reference to confidentiality and authenticity |

Source: Digital Europe[56], comparative national law analysis, Arthur D. Little

[56] *Improving Member States' approaches to number-independent services in light of the EECC*, Digital Europe, 2022.

# 6. BIBLIOGRAPHY

## LEGISLATIVE DOCUMENTS

### European regulation

#### *a) Legislative documents that are sector specific to the telecommunications industry*


1. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (EECC), OJ L 321, 17.12.2018.
2. Commission Implementing Regulation (EU) 2019/2243 of 17 December 2019 establishing a contract summary template pursuant to Directive (EU) 2018/1972 of the European Parliament and of the Council.
3. Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (Recast) – known as the Roaming Regulation.
4. Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges.
5. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications (commonly referred to as the Open Internet Regulation or Telecoms Single Market Regulation – TSM).
6. 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 (ePrivacy Directive).
7. Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC (ePrivacy Directive).
8. BEREC. (2023, October 5). Report on Member States' best practices to support the defining of adequate broadband internet access service (Draft). BoR (23) 144.
9. BEREC. (2024). Draft Report on the entry of large content and application providers into the markets for electronic communications networks and services. BoR (24) 51.
10. BEREC. (2016). Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. BoR (16) 127.
11. BEREC. (2022). BEREC Guidelines on the Implementation of the Open Internet Regulation (Updated). BoR (22) 140.


#### *b) Horizontal regulation*


1. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (European Accessibility Act – EAA).
2. Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU as regards the better enforcement and modernization of Union consumer protection rules.
3. Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods.
4. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

5. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights (Consumer Rights Directive – CRD).
6. Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising.
7. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive – UCPD).
8. Directive 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety (General Product Safety Regulation– GPSR).
9. Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers (Price Indication Directive – PID).
10. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (Unfair Contract Terms Directive – UCTD).
11. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Data Act Regulation)
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 7 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR).
13. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 13 March 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act – CRA).
14. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. (Electronic Evidence Regulation)Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act – CSA).
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 (NIS2 Directive).
16. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act – DORA).
17. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (Payment Services Directive – PSD2).
18. European Commission (2010). Communication on A Digital Agenda for Europe
19. European Commission (2016). Communication on Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society

## National legislation

- Austria: Telecommunications Act (TKG), 2021
- Belgium : ECA – Loi du 13 juin 2005 relative aux communications électroniques [Act of 13 June 2005 on Electronic Communications]. (2005). Moniteur belge, 20 June 2005.
- Denmark : Executive Order No. 566/2023 – Bekendtgørelse nr. 566 af 24. maj 2023 om slutbrugerrettigheder på teleområdet [Executive Order No. 566 of 24 May 2023 on End-User Rights in the Telecommunications Field]. (2023). Erhvervsministeriet.

- Denmark : Electronic Communications Act – Lov om elektroniske kommunikationsnet og -tjenester [Act on Electronic Communications Networks and Services]. (Latest consolidation). Erhvervsministeriet.
- France : Loi Châtel – Loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs [Law No. 2008-3 of 3 January 2008 on Competition and Consumer Protection]. (2008). Journal officiel de la République française, 4 January 2008.
- Germany : TKG – Telekommunikationsgesetz vom 23. Juni 2021 [Telecommunications Act of 23 June 2021]. (2021). Bundesgesetzblatt I, p. 1858.
- Italy: AGCOM Delibera 255/24/CONS – Delibera n. 255/24/CONS – Adozione del regolamento recante disciplina e indicatori di qualità dei servizi di assistenza clienti nel settore delle comunicazioni elettroniche e dei servizi di media audiovisivi [Resolution No. 255/24/CONS – Adoption of Regulation and Quality Indicators for Customer Service in the Electronic Communications and Audiovisual Media Services Sector]. (2024). Autorità per le Garanzie nelle Comunicazioni. Decreto Bersani (Law No. 40/2007), Legislative Decree No. 207/2021, , Decree of 12 December 2018, Decree 81/2021.
- Portugal: Decree-Law No. 134/2009 – Decreto-Lei n.º 134/2009 de 2 de junho [Decree-Law No. 134/2009 of 2 June on Call Centre Services]. (2009). Diário da República, 1st series, No. 106.
- Portugal: Decree-Law No. 59/2021 – Decreto-Lei n.º 59/2021 de 14 de julho [Decree-Law No. 59/2021 of 14 July on the Provision and Publicizing of Consumer Contact Telephone Lines]. (2021). Diário da República, 1st series, No. 135.
- Spain: General Telecommunications Law – Ley 11/2022, de 28 de junio, general de telecomunicaciones [Law 11/2022 of 28 June, General Telecommunications Law]. (2022). Boletín Oficial del Estado, No. 154, 29 June 2022.


## OTHER SOURCES


- Feasey, R., Alexiadis, P., Bourreau, M., Cave, M., Godlovitch, I., Manganelli, A., Monti, G., Shortall, T., De Streel, A., & Timmers, P. (2024). Ideas for the future of European telecommunications regulations. CERRE (Centre on Regulation in Europe).
- Letta, E. (2024). Much more than a market – Speed, Security, Solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens.
- Sandvine (2024). Global Internet Phenomena Report.
- Ofcom (2023). Net Neutrality Review.
- Briglauer, W. (2024). Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector: Relevant Developments and State of the Empirical Literature.
- Digital Europe (2022). Improving Member States' approaches to number-independent services in light of the EECC.
- European Commission. (2023). Report from the Commission to the European Parliament and the Council on the implementation of the open internet access provisions of Regulation (EU) 2015/2120. COM(2023) 233 final.
- European Commission. (2022). Broadband Coverage in Europe 2022
- Eurostat.
- Peng, M., Xu, Z., & Huang, H. (2021). Does Information Overload Affect Consumers' Online Decision Process? An Event-Related Potentials Study.
- Kusi, G., Rumki, G., Quarcoo, F., Otchere, E., et al. (2022). The Role of Information Overload on Consumers' Online Shopping Behavior.
- Stocker, V., et al. (2017).

# GLOSSARY

| Abbreviation | Full Name |
|---|---|
| 4G | Fourth Generation of Mobile Telecommunications |
| 5G | Fifth Generation of Mobile Telecommunications |
| ACM (NRA) | Autoriteit Consument & Markt (Netherlands) |
| AGCOM (NRA) | Autorità per le Garanzie nelle Comunicazioni (Italy) |
| ANACOM (NRA) | Autoridade Nacional de Comunicações (Portugal) |
| ARCEP (NRA) | Autorité de Régulation des Communications Électroniques, des Postes et de la distribution de la presse (France) |
| B2B | Business-to-Business |
| BEREC | Body of European Regulators for Electronic Communications |
| BIPT (NRA) | Belgian Institute for Postal Services and Telecommunications |
| BNetzA (NRA) | Bundesnetzagentur (Germany) |
| CAP | Content and Application Provider |
| CAGR | Compound Annual Growth Rate |
| CDN | Content Delivery Network |
| ComReg (NRA) | Commission for Communications Regulation (Ireland) |
| CPCE | Code des postes et des communications électroniques (France) |
| CRA | Cyber Resilience Act |
| CSA | Cybersecurity Act |
| CRD | Consumer Rights Directive |
| DORA | Digital Operational Resilience Act |
| DMA | Digital Markets Act |
| EAA | European Accessibility Act |
| ECS | Electronic Communications Service |
| EECC | European Electronic Communications Code |
| EDPB | European Data Protection Board |
| ENISA | European Union Agency for Cybersecurity |
| EU | European Union |
| EUR PPP | Euros in Purchasing Power Parity |
| FUP | Fair Use Policy |
| GDPR | General Data Protection Regulation |
| GPSR | General Product Safety Regulation |
| ICS | Interpersonal Communications Service |
| ISP | Internet Service Provider |
| NB-ICS | Number-Based Interpersonal Communications Services |
| NI-ICS | Number-Independent Interpersonal Communications Services |
| NIS2 | Network and Information Security Directive 2 |
| Nkom (NRA) | Norwegian Communications Authority |
| NRA | National Regulatory Authority |
| Ofcom (NRA) | Office of Communications (UK) |
| OIR | Open Internet Access Regulation |
| OTT | Over-the-Top |

| | |
|---|---|
| PID | Price Indication Directive |
| PPP | Purchasing power parity |
| PTS (NRA) | Postoch telestyrelsen (Sweden) |
| PSD2 | Payment Services Directive 2 |
| QoS | Quality of Service |
| RTR (NRA) | Rundfunk und Telekom Regulierungs-GmbH (Austria) |
| SMS | Short Message Service |
| TK-NSiV | Telekom-Netzsicherheitsverordnung (Austria) |
| TKG | Telekommunikationsgesetz (Germany) |
| TKÜV | Telekommunikations-Überwachungsverordnung (Germany) |
| TSM | Telecom Single Market Regulation |
| UCPD | Unfair Commercial Practices Directive |
| UCTD | Unfair Contract Terms Directive |
| URLLC | Ultra-Reliable Low-Latency Communications |
| USO | Universal Service Obligation |
| VHCN | Very High-Capacity Network |

## DETAILED TAXONOMY

| | Areas | Measures | Exemplary elements of regulation |
|---|---|---|---|
| Before acquisition | Accessibility | USP rules | Universal service provider designation |
| | | | Compensation of net cost and funding methods |
| | | | QoS obligations for USO |
| | | | Application of penalties in case of non compliance |
| | | Equality of access and choice | Regulation of beneficiaries (e.g. blind people, low income people, etc.) |
| | | | Specific offers contents and service features for defined categories |
| | | Use of customers data | Rules on customer personal data framework |
| | | | Rules on customer personal data gathering (e.g. opt-in or opt out consent) |
| | | | Rules and limits to customer personal data usage during offer design (e.g. profiling) |
| | Offer's definition | Rules on offers composition & promotion | Limitations to the definition of base contract offer (what's included) |
| | | | Rules on additional services / pre-activated non basic services inclusion, OPT-IN vs OPT-OUT (e.g. voice mails, etc.) |
| | | | Rules and limitations on service bundling with other telco and non telco services |
| | | | Rules on the characteristics of add-ons, such as special family rate, data packages, etc. (e.g. duration, automatic renewal, etc.) |
| | | | Rules & limitations on Handset / product promotions |
| | | | Rules on promotion usage (e.g. consumption limits, timings, etc.) |
| | | | Rules on promotion applicability |
| | | | Rules on promotion notification / approval |
| | | | Rules on promotion duration |
| | Offer's pricing | Price setting, discrimination and charging rules | Imposition of price floor |
| | | | Imposition of price caps |
| | | | Impositions related to the development of replicability test on offers pricing |
| | | | Imposition of a max gap among best and worst offers |
| | | | Prohibition to differentiate on-net vs. off-net prices |
| | | | Imposition of maximum gaps between on-net / off-net prices |
| | | | Prohibition of geographical price differentiation (e.g. regional pricing) |
| | | | Regulation of data prices differentiation (e.g. among applications / content) |
| | | | Cancellation of top-up charges |
| | | | Additional service and Premium Rated Services (PRS) charging rules |
| | | | Regulation of billing increments / rounding regulation (e.g. per second billing, number of days for monthly billing) |
| | | Informative/approval obligations to NRAs | Obligation to notify retail tariffs and promotions |
| | | | Obligation to get NRA approval |
| | | | Perimeter of application of the notification / approval regulation |

| | | | |
|---|---|---|---|
| Time of acquisition | Offer launch | Rules on roaming & intra EU calls / SMS | Powers assigned to the NRAs after tariffs notification/ approval (e.g. suspension, sanctioning, amendment, etc.) |
| | | | Notification & approval process and timings |
| | | | Imposition of roaming price caps |
| | | | Roaming tariffs setting |
| | | | Introduction of alternative roaming providers |
| | | | Price cap regulation vs abolition |
| | | Rules on offer communication/advertising & transparency | Obligation to provide customers and NRAs with a standard set of information |
| | | | Rules on Fair Usage Policies communication |
| | | | Rules on offers and promotion publication |
| | | | Imposition of a standardized format for offers communication |
| | | | NRA's accreditation of tariff comparing tools |
| | | | Obligation to provide specific detailed information (e.g. additional costs / constraints, etc.) |
| | | | Rules on the use of advertising terms (free, unlimited, for life, etc.) |
| | | | Rules on advertised vs. actual BB speed |
| | | | Comparative advertising regulation |
| | Customer acquisition | Distance selling rules | Limitations to the possibility to use distance selling for a specific set of services (e.g. distance selling possible only for add-on and not for tariff plans, etc.) |
| | | | Services' subscriptions process regulation (e.g. request of specific consent) |
| | | | Rules on customer willingness gathering and storing (standard form, storage time, etc.) |
| | | | Introduction of specific terms of cancellation and reimbursement |
| | | | Regulation for inertia selling (longer cancellation period, etc.) |
| | | Protection against slamming | Obligation to gather customer willingness confirmation in case of customer's acquisition from another operator |
| | | | Consent form and storage time |
| | | Use of customer data | Limits to the access and use of customers data for the development of active and targeted selling activities |
| | Contract conditions | Premium Rated Services (PRS) rules | Obligation to provide barring |
| | | | PRS acquisition process regulation |
| | | | Transparency obligations |
| | | | PRS price regulation |
| | | Contract clauses & registration regulation | Limits to commitment period, lock in conditions or other barriers to entry |
| | | | Service cancellation terms and penalties |
| | | | Conditions to apply changes to the contract and for contract renewal |
| | | | Obligation to provide specific detailed information (e.g. on service quality, minimum guaranteed speed, etc. ) |
| | | | Regulation of unfair contract terms |
| | | | Regulation of documentations to be collected for customers registration |
| | | | Regulation of registration methodology and tools (e.g. required face to face identification, etc.) |
| | | | Unregistered SIM management and treatment of registered SIM if more strict rules on customer registrations are introduced |
| During contra | Quality of services | KPIs regulation | Establishment of a mandatory set of QoS KPIs to be monitored (Ping, Packet loss, application layer) |
| | | | Quality of services measurement methods |

| | | | |
|---|---|---|---|
| | | | QoS KPIs publication |
| | | | Target imposition / establishment of minimum QoS KPIs' levels |
| | | | Target enforcement and penalties in case of incompliance |
| | | | Establishment of certified tests on KPIs such as speed, latency, etc.(NRAs' or 3rd parties) |
| | | | Possibility for consumers to have access to certified speed tests |
| | | | Special QoS requirements |
| | | **Compensation for network outages and contract breaches** | Regulation of compensation triggers (e.g. automatic, at customers request, etc.) |
| | | | Regulation of compensation methods (e.g. traffic, cash, etc.) |
| | | | Definition of standard compensation amounts, caps / floors |
| | | | Rules on helpdesk minimum availability |
| | | | Complaint management timings (i.e. time limits for problem solving, including possible technical issues) |
| | | | Rules on helpdesk charges allocation |
| | | **Customer complaints management / Helpdesk** | Customer complaint management organization |
| | | | Rules on helpdesk QoS and answering process (identifiability of operators, traceability of claims) |
| | | | Rules on helpdesk KPIs and activities reporting to the NRAs |
| | | | Call center geographical localization & languages requirements |
| | | | Prohibition to limit on VoIP applications |
| | | | Prohibition to impose charges to VoIP traffic |
| | **Management of service utilization** | **Net neutrality rules** | Limits to the possibility to charge a premium for specific apps |
| | | | Limits to traffic management / web application blocking |
| | | **Customer information management** | Rules / safeguards on the disclosure of customer data and traffic |
| | | | Hide numbers disclosure limitation |
| | | | Rules on options / add-on up-selling procedure |
| | | | Rules / limits on options/ add-ons contracts conditions (e.g. commitment period, cancellation terms and penalties, etc.) |
| | | | Rules on options/add-ons renewal timing and procedure |
| | | **Rules on add-ons upselling, re-pricing / change of plan** | Informative obligation (e.g. on the level of options/ add on consumption) |
| | | | Limits to repricing / change of plans possibility |
| | **Upselling and change of tariff plans** | | Rules on repricing / change of plan communication |
| | | | Rules on re-pricing procedure |
| | | | Rules on customers rights in case of repricing (e.g. right to keep the existing plan, right to switch with no penalties, etc.) |
| | | | Obligation to create a "do not call" register |
| | | **Rules on marketing / data profiling activities** | Data utilization rules (e.g. no profiling, use of geo-localization) |
| | | | Rules on the possibility to contact cust. to offer own/3rd parties offers |
| | | | Rules on customized 3rd party SMS sending (traceability) |
| | | | Limits to the expenditure level and to the range of possible purchasable services using the mobile credit |
| | **Mobile financial services** | **Rules on mobile payment & mobile financial services** | Rules and constraints related to money laundering / fraud |
| | | | Limits to the possibility to transfer credit between SIMs |
| | | | Rules on mobile payment (e.g. authorization process, etc.) |

| | | | |
|---|---|---|---|
| Customer loosing time | Billing | Billing content and unpaid bills management | Specific data protection provisions |
| | | | Limits to operate as a financial entity |
| | | | Limits to the possibility to transfer money from bank account |
| | | | Obligation to provide specific billing format |
| | | | Special billing for disabled people (e.g. braille or voice billing) |
| | | | Minimum set of information to be included in the bills |
| | | | Obligation to separate charges by nature (e.g. voice, data, SMS, PRS, etc.) |
| | | | Rules on itemized billing |
| | | | Limit to the possibility to transfer bill costs to customers (e.g. only in case of detailed paper billing request) |
| | | | Period of minimum service provision before suspension |
| | | Expenditure control and bill shocks regulation | Limits to the possibility to block bad payers during the MNP |
| | | | Right to manage/share bad payers info (TLC register of bad payers) |
| | | | Instant bill verification tools provisions |
| | | | Expenditure alert/ service barring mechanisms |
| | | | Obligation to allow end users to set a limit to their expenditure |
| | Disputes management | Dispute resolution, sanctioning & penalties | Dispute negotiation mechanisms |
| | | | Specific body identification (e.g. mediation and conciliation bodies) |
| | | | Compensation methods |
| | | | Imposition of standard compensation values |
| | | | Number of identified bodies entitled of sanctioning |
| | | | Right for the authority to impose additional compensation to impacted customer base (or OLOs in case of incumbent operators) |
| | | | Inspection power |
| | | | Types of sanctioning (warnings , roll backs or sanctions) |
| | | | Possibility to impose retroactive sanctions |
| | | | Possibility for Telco players to block a sanctioning procedure by proposing / agreeing on commitments |
| | Switching and retention | Number portability regulation | NP process & governance (originator, lead time, capacity management, users experience, technical solution, bad debt / residual credit treatment) |
| | | | Rules on cost allocation |
| | | | Informative obligations regard migration code (e.g. in the bill, at first request) |
| | | | Limitations on retention activity (right to use NP info to make counteroffers during portability time-window) |
| | | Rules on SIM's deactivation | Minimum deactivation period in case of SIM inactivity |
| | | | Obligation to provide unspent credit reimbursement |
| | | | Rules related to the numbering management after SIM deactivation |
| | | | Credit reimbursement process |
| | | | Deactivation procedures/ notification |
| | | | Standstill period |
| | | Win-back activities regulation | Separation obligation (e.g. limits to information sharing between network and commercial departments, Chinese walls, functional separations, etc.) |
| | | | Limitations on the use of lost customers' personal data (e.g. expiration of authorizations in the right to use) |
| | Contract end (incl. | Early termination by customer | Cooling of period |
| | | | Fair termination fees |

| | | | |
|---|---|---|---|
| Transversal | termination, withdrawal…) | Rules on contract expiry & non-renewal | Termination charges |
| | | | Prohibition of lock-in practices |
| | | | Clear termination process |
| | | | Pre-expiration notification |
| | | | Auto-renewal conditions |
| | | Provider initiated termination | Fair grounds for termination |
| | | | Mandatory notice period |
| | | | Fixed contract disconnection |
| | Security | Rules on sovereignty | Rules on asset localization requirements |
| | | | Lawful interception of communication provider data |
| | | Rules on incidents | Incident reporting |
| | | | Data breach notifications |
| | | Cybersecurity obligations | Risk based security measures |
| | Use of AI | Transparency obligations and consumer rights | Rules on AI in customer facing processes |