

RTR Net Neutrality Report

2026



RTR Net Neutrality Report

2026

Report pursuant to Art. 5(1) of Regulation (EU) 2015/2120
laying down measures concerning open internet access

June 2026



Rundfunk und Telekom Regulierungs-GmbH

Mariahilfer Straße 77–79 | A-1060 Vienna | Austria
Phone: +43 1 58058-0 | Mail: rtr@rtr.at

www.rtr.at

Contents

1	Preface and executive summary	4
2	Introduction: stakeholders and institutions in enforcement	7
3	Timeline of regulatory authority activities	10
4	Net neutrality and 5G network slicing	13
5	Internet blocking	17
5.1	Overview of activities	18
5.2	Internet blocks to protect copyright	18
5.3	Internet blocking pursuant to the Consumer Protection Cooperation Act	19
5.4	Internet blocking pursuant to the EU Market Surveillance Regulation	19
5.5	War in Ukraine: internet blocking pursuant to the EU Sanctions Regulation	20
5.6	Internet blocking pursuant to MiCA	20
5.7	Previous general decisions by the TKK on IP blocks	21
6	Potential breaches of net neutrality and procedures	25
6.1	Blocking of TCP/UDP ports or protocols	27
6.2	Private IP addresses and services	29
6.3	Disconnection of IP connections	29
6.4	Internet blocking	30
6.5	Measures in accordance with Art. 5(1) TSM Regulation	31
6.6	Ensuring legally compliant terms of contract	39
6.7	RTR conciliation procedures	40
6.8	General enquiries	41
7	Indicators of continuous availability of non-discriminatory internet access services	42
8	Outlook on further activities	53
9	Appendix	57
9.1	Mapping	58
9.2	Index of Figures and Tables	59
9.3	Abbreviations	60
	Publishing information	62

01

Preface and
executive summary

01 Preface and executive summary

Dear Reader,

In today's world, rapidly developing technologies pose a unique challenge for communications networks. This is truer than ever in the case of AI. The requirements placed on network capacities are in themselves challenging enough, as the volumes of data needing to be transported across infrastructures consistently grow. Added to this are the various applications used in industry, mobility, healthcare, and public safety that increasingly require guaranteed quality standards for availability, reliability, or latency. At the same time, the open internet remains the fundamental basis for innovation, competition, and free access to information. Harmonising all of these needs is the main challenge.

As the competent body, we are pleased to present you with the tenth Net Neutrality Report, once again providing a retrospective overview of the previous reporting year. At the same time, it represents the product of a full decade's efforts in monitoring the implementation of EU net neutrality rules as a regulator. During this timespan, issues have shifted significantly. In the initial years, discussions focused mainly on transparency issues or business practices, including zero-rating. Since then, matters such as differentiating quality, virtual network architectures, and new digital services are increasingly occupying regulators, market participants, and policymakers alike.

Once again at the top of the agenda, the issue of 5G network slicing is clearly a main topic of this year's report as well. The potential to make network resources available specifically for various designated applications is opening up new opportunities for innovative services and business models. Yet at the same time, we need to ask: how are such advances to be reconciled with the fundamental principle of an open internet? Obviously, ensuring both innovation and open access will remain a key regulatory challenge in the future.

Net neutrality has been a European project from the very beginning. Only in a European context can we successfully move this undertaking forward. Today, net neutrality is raising issues that do not respect international borders. European policymakers are discussing the implications of advancing technologies and thinking beyond. Close cooperation among regulators thus remains crucial if we are to maintain a common interpretation of existing rules while ensuring the free space needed for technical innovation. The Digital Networks Act (DNA) is currently being negotiated by the European Commission, Council, and Parliament. One of the central goals here is to incorporate the principle of net neutrality into the regulatory framework for digital networks, thereby ensuring a harmonised European response. Indeed, this will be crucial for Europe's future ability to compete internationally.

More and more social and business interactions are moving into the digital space, posing new challenges for enforcing laws and legal claims. Increasingly often, legislators, courts, and regulators face the dilemma of having to effectively safeguard legitimate public interests without overly restricting the openness of the internet. Internet blocking sits at the very centre of this conflict. This underscores the importance of a clear legal framework, transparency, and carefully weighing affected interests. In this context, safeguarding legal certainty will always be key to maintaining trust among all parties participating in the common digital space.

High-quality internet access services continue to become increasingly available to Austrians, as seen in developments during the past reporting year. Powerful communications networks form the basis for competitive businesses, participation in society, and digital innovation. Thus, both in terms of economic and civil democratic policy, maintaining an open internet is not just a technical or regulatory issue. Instead, it is a key incentive for businesses to locate in Europe.

Still, the openness of the internet is not to be taken for granted. It must be continuously monitored and safeguarded, as well as adapted to meet changing technical requirements. RTR will therefore continue to work both at the national level and in the international sphere to ensure a balance between innovation, competition, and end-user rights. With this goal in mind, and in view of how relevant net neutrality is, we will also act within the context of our international activities to ensure that the issue is devoted appropriate attention in the DNA.

I truly hope this report provides you with interesting reading.

**Vienna,
June 2026**

Klaus M. Steinmaurer

*Managing Director
Telecommunications and Postal Services Division
RTR*

Introduction: stakeholders and institutions in enforcement

02 Introduction: stakeholders and institutions in enforcement

This is the tenth Annual Report on Net Neutrality by the Telecommunications and Postal Services Division of the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR). In structure, it reflects the topics covered in last year's report. It is designed to give readers an overview of the regulatory authority's broad range of activities.

How open is the internet in Austria? Which measures had to be adopted by regulators in the reporting year (1 May 2025 to 30 April 2026, inclusive) to ensure the openness of the internet? What new product developments might offer advantages for consumers, at the same time potentially harbouring risks for the future sustainability of the internet?

As in the past, companies providing internet access service, or internet service providers (ISPs), continue to be the group primarily targeted by net neutrality provisions. The EU Regulation is mainly concerned with responding to changing technical capabilities and enabling any new business models developed by ISPs, while not compromising the innovative power behind the internet. The TSM Regulation accordingly identifies business practices, technical measures and obligations (such as ensuring transparency for end users) that are either necessary or to be avoided in order to uphold net neutrality. Besides ISPs, the regulation both empowers and addresses in particular end users with a right to free access to an open internet: private citizens and businesses as well as providers of content, services or applications.

Responsibility for enforcing the TSM Regulation in Austria lies with the Telekom-Control-Kommission (TKK) and RTR. Supervisory procedures are the TKK's responsibility, while the preceding request-for-information procedures are conducted by the RTR's Telecommunications and Postal Services Division. Also related to net neutrality is the requirement for general terms of business and fee provisions to be submitted to RTR before taking up service. The TKK may prohibit general terms of business from being applied if these contravene the Telecommunications Act 2021 (TKG 2021) or specified consumer protection regulations. All relevant changes in contract conditions, including any affecting net neutrality, must be submitted to the regulatory authority. Such changes are reviewed for compliance with the minimum contractual content given in the TSM Regulation. This gives the regulatory authority an efficient early warning mechanism. Despite that, infringements of other provisions of the TSM Regulation can only be prohibited ex post. The regulatory authority can also better assess the impact of specific measures on the market, by imposing reporting requirements on a company.

RTR is a convergent telecoms, postal and media organisation, and its divisions, for Telecommunications and Postal Services and Media, consult both mutually and with the TKK and the Austrian Communications Authority (KommAustria) on all key issues relating to net neutrality. This is significant, not least because certain net neutrality issues (such as specialised services) may also exhibit an overlap with media topics.

The present annual report has its roots in an obligation imposed on the European national regulatory authorities by the TSM Regulation. One aim of this obligation is to achieve a highly consistent, EU-wide approach to applying net neutrality provisions.

In working with ISPs, the regulatory authority consistently adheres to the principle of identifying infringements of the TSM Regulation (monitoring) while at the same time raising awareness for the topic among ISPs, with the ultimate aim of creating a stable environment for entrepreneurial activity and innovation. Where infringements of net neutrality rules occur, the authority allows appropriate transition periods for resolution. This enables businesses to adjust to the new legal standards without experiencing disruptive interventions.

Beyond that, net neutrality is a matter always needing to be handled in view of changes over time. Increasingly, new issues are now emerging, such as how to implement net neutrality concepts in the context of the fifth-generation mobile network standard (5G). Other relevant issues include resource distribution across virtual network elements (network slicing) and the classification of such elements within the scope of the TSM Regulation. Another is internet blocks based on various legal provisions. The debate over the potential financial contribution of content providers for their 'use' of ISP networks remains as pertinent as ever. This issue was discussed already back in 2012 during the drafting of the TSM Regulation. On the whole it is safe to say that, as more and more day-to-day activities take place online, the focus shifts ever more strongly to the importance of free access and the openness of the internet—the principle of net neutrality.

In section 3 below, we present a chronological overview of the activities of the national regulatory authority. In section 4, the reader will find a summary of current developments as well as work on net neutrality and 5G network slicing. Section 5 presents the regulatory authority's activities and responsibilities in relation to internet blocks. Section 6 summarises the regulatory measures used to protect net neutrality as well as related procedures. Section 7 provides an overview of key figures on the development of internet access services in Austria. The last part of the report, section 8, presents a brief summary of the projects and events expected in the next reporting year.

Timeline of regulatory authority activities

03 Timeline of regulatory authority activities

Figure 1: Timeline of events in the reporting period

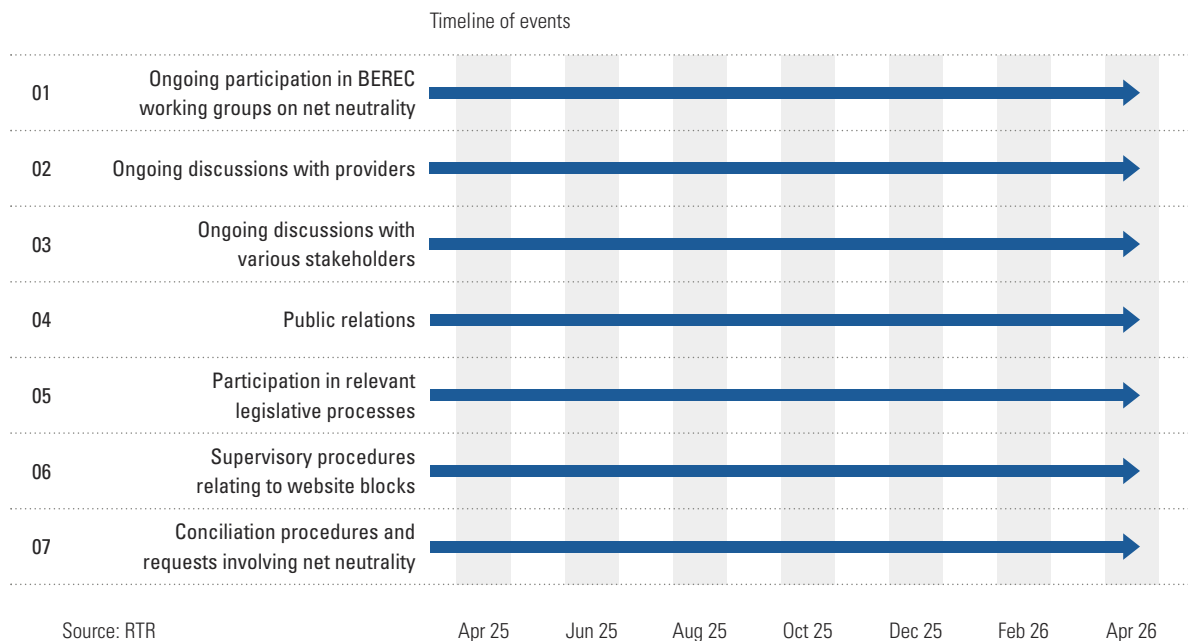


Figure 1 presents in chronological sequence the relevant events during the reporting period (May 2025 – April 2026). The table below gives an overview of these events, with a brief description in each case and giving the time period involved. Further details about these procedures can be found in sections 7.

Table 1: Timeline of events in the reporting period

Work in EU bodies		
01	Ongoing	Participation in the BEREC Open Internet Working Group on net neutrality (open internet) Topics in 2025: Implementation of the Open Internet Regulation and the BEREC Open Internet Guidelines; BEREC contribution to the implementation of the Digital Markets Act; Report on switching and termination of contracts; BEREC contribution on the impact of Artificial Intelligence on the competition dynamics, internet openness and end-users rights; Collaboration on internet access service measurement tools; Workshop on the consideration of 5G differentiated services and network slicing. Topics in 2026: Implementation of the Open Internet Regulation and the BEREC Open Internet Guidelines; BEREC contribution to the implementation of the Digital Markets Act; Report on switching and termination of contracts (carry over); BEREC-BEUC joint workshop on end-user rights; Ad hoc work on reinforcing end-user rights and empowerment; BEREC report on the impact of artificial intelligence on competition dynamics, internet openness and end-user rights; Collaboration on internet access service measurement tools; Further guidance on the consideration of 5G network slicing.
National status quo analysis/discussion with ISPs		
02	Ongoing	Net neutrality discussions with providers
03	Ongoing	Discussions with various stakeholders
04	Ongoing	Public relations
05	Ongoing	Participation in relevant legislative processes
Enforcement of TSM Regulation		
06	January 2025 to August 2025	In the preceding reporting year, one procedure pursuant to Regulation (EU) 2019/1020 (Market Surveillance Regulation) was initiated at the request of the Federal Office of Metrology and Surveying (<i>Bundesamt für Eich- und Vermessungswesen</i> , BEV) with the aim of securing an order from the TKK to prevent access to a website listing a dangerous product. As the request was subsequently withdrawn, the procedure was terminated in August 2025.
07	March 2025 to April 2025	Notification of internet blocks affecting the standardingold.com website by four ISPs based on the EU Markets in Crypto-Assets Regulation (MiCA), set in response to decisions by the competent Financial Market Authority (FMA). These blocks were lawfully set and therefore not in breach of the TSM Regulation.
08	Ongoing	Conciliation procedures and enquiries relating to net neutrality (for further details, see section 6.7).

Net neutrality and 5G network slicing

04 Net neutrality and 5G network slicing

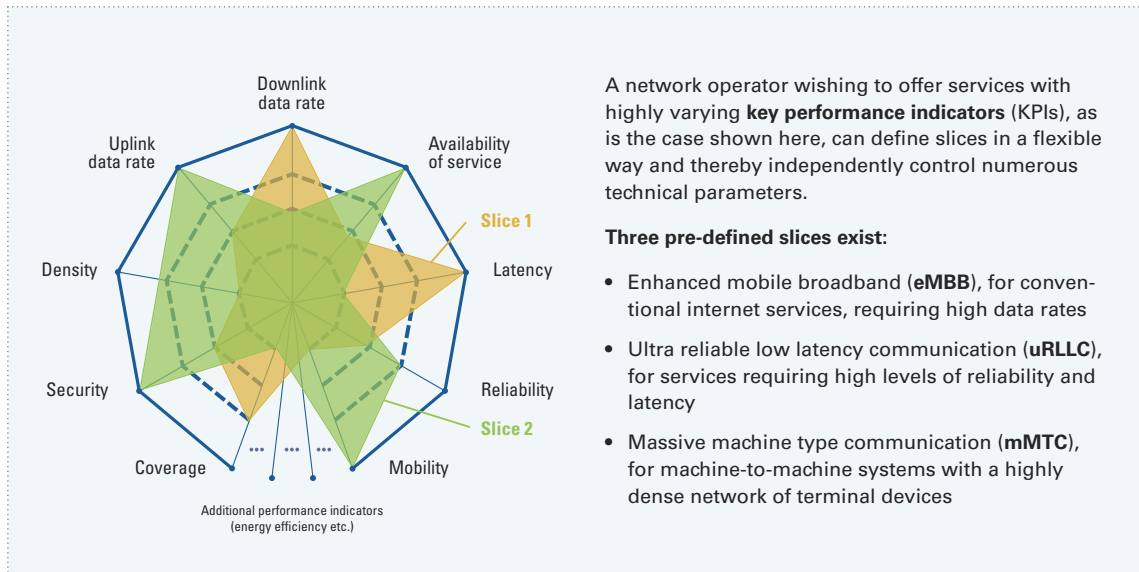
With the European and international rollout of 5G technology, mobile telecoms providers have been awarded additional spectrum. Together with the advances in spectral efficiency achieved by the latest multi-antenna systems, these supplementary frequency ranges will make it possible to achieve increasingly higher capacities and performance levels. These developments also go hand in hand with increasing demand for high-quality communications services. In this context, mobile telecoms providers must take steps to utilise these more extensive resources both profitably and cost-effectively, while adapting them to the quality requirements of the various categories of mobile connectivity solutions. Apart from ensuring the fair distribution of network resources, providers must also adjust quality parameters to prevent the wasteful deployment of network resources in areas where they are not needed. At the same time, providers must meet the stringent and wide-ranging performance requirements posed by the various services. This can be seen as a further refinement of the delineation, successfully achieved during the 4G rollout, between internet data services and voice services. Voice services are now very clearly demarcated: traffic prioritisation is used to prevent unacceptable delays to voice calls, even though the underlying voice service uses the same IP data network as data services. The discrete categories and assignable quality of service levels within a 5G network can be extended almost indefinitely, and these can be added to or removed from an end-user device dynamically. These traffic or service categories can be used simultaneously by one user device, such as a smartphone, and can be activated selectively based on criteria such as temporary use, use in certain locations or use by specified authorised applications. Technical tools are also available that can be used for quality assurance and to ensure the complete separation of data traffic for specific or private services.

The umbrella term ‘5G slicing’ is used as a general designation for such innovations that work to create service differentiation within the 5G network. All of these options are described by standard protocols¹ and are being transitioned to real-world solutions step by step. Broadly speaking, this technology can be described as the capability of a provider to partition their resources and services, and to provide these partitions—also known as ‘slices’—to appropriately authorised end-user devices. The provider can then assign a portion of spectrum, such as the lower range of frequencies in the 900 MHz band, to each of these slices, as a means of providing a specific type of service with improved coverage and less handover.² In more general terms, the provider can also define traffic rulesets with the aim of achieving the levels of performance that are appropriate for a specific service in terms of latency, data transfer rates, security and reliability. Apart from allocating network resources to a service for a specific purpose and specifying the degree to which this service will be isolated from others, the provider can also determine the method used for service marketing and billing. The degree of traffic isolation that is configured for the various slices may also vary widely. Slices that are merely utilised to differentiate between subscription levels for conventional internet data usage may collectively use the resources in full, and their resource access can be subject to different priorities and policies. Meanwhile, a minimum level of resources is guaranteed for the kinds of mission-critical services used by telemedicine, energy grid monitoring or emergency services. This guaranteed level of resource usage is protected by safeguards that prevent a lack of shared resources in one slice impacting a service that is running in another slice.

¹ Definitions for 3GPP 5G system protocol interfaces and slicing functions were finalised in 2019 (Release 15) and completed in 2020 (Release 16). If a 5G mobile telecommunications service also intends to incorporate non-5G network types—such as fixed access networks (optical fibre or copper) or IP transport networks—the various providers and operators need to work together to guarantee the required QoS level. To achieve this goal, other organisations such as the ITU, ETSI, BBF, IETF and GSMA are working jointly or parallel in standardisation activities.

² The term ‘handover’ refers to a device switching to a new radio cell while the device user is moving, as base stations have a limited range (Miao/Zander/Sung/Ben Slimane, Fundamentals of Mobile Data Networks, [2016] 199).

Figure 2: Schematic diagram of quality of service indicators for two slices



This schematic diagram illustrates how key performance indicators are defined for two separate services, which are then provided via two discrete slices.

Apart from the option of allocating resources to specific end-user devices and subscriptions, 5G network slicing is also able to apply a mechanism known as user equipment route selection policy (URSP) to detect the data traffic generated by an application and its assignment to a dedicated slice. URSP is dependent on both the user device and operating system meeting the technical requirements, however, as these must ensure that the correct slice is used when transmitting the data for a specific application. In other words: even if the 5G network operator has the 'final say' on network resources, the manufacturers of the user devices and the operating systems must cooperate in order to ensure that the correct authentication and authorisation mechanism is used for the applications. The open source associations in the mobile telecommunications industry are also working in parallel to standardise software interfaces³ for application developers. Interfaces that allow applications to request specific slices with predefined connectivity requirements will facilitate the development of create mobile telecoms applications with multi-provider compatibility.

5G network slicing is therefore a sophisticated traffic management system. As such, its use is not only governed by the TSM Regulation But must be in compliance with the guidelines issued by the Body of European Regulators for Electronic Communications (BEREC). For its part, BEREC has stated that internet access service (IAS) providers could use network slicing as a method for offering multiple IAS with different levels of quality of service and specialised services (SpS). At the same time, network slicing may also help prevent a deterioration of the quality of IAS in general as a result of providing SpS. The guidelines proposed by BEREC to ensure compliance with European law offer guidance for assessment on a case-by-case basis and therefore constitute a standard reference for related discussions at a European level.⁴

³ The open source association Camara recently launched an API project aimed at providing developers with an interface that allows applications to reserve and manage network slice resources (<https://camaraproject.org/network-slice-booking/>).

⁴ On 7 May 2025, BEREC held an internal workshop on the consideration of 5G differentiated services and network slicing. (<https://www.berec.europa.eu/system/files/2025-01/BEREC%20Work%20Programme%202025%20%28Design%20version%29.pdf>).

Although deployment is by no means as extensive as it is in the United States or a number of Asian countries,⁵ applications that make use of 5G slicing are now becoming more common in the Austrian and European markets. Use cases here range from: safeguarding internet data transmission rates for fixed wireless access (FWA) and providing access to private networks over the public mobile network, to the reservation of resources for emergency or security services.

In conclusion, it can be said that Europe continues to work apace towards making progress on this topic. This is also the reason why RTR is participating in activities, such as those pursued by BEREC, with the aim of discussing best practice for the case-by-case transposition of European standards.

Some market actors have publicly called for greater clarity concerning whether innovative services based on 5G network slicing comply with the provisions of the TSM Regulation. Similarly, in a recent report addressing the enforcement of the TSM Regulation provisions for guaranteeing open internet access, the European Commission has underscored how greater legal certainty in this area would benefit innovators and consumers alike. This view was repeated in the European Commission's call for evidence on its planned Digital Networks Act legislative initiative.

During the past reporting period, BEREC responded by inviting all interested market actors to participate in a "Call for input for further guidance on 5G network slicing" in early 2026. The basic principles of network slicing and service quality differentiation can also be applied in the context of other communications technologies, such as 6G. The results of this more in-depth guidance—which references the general guidelines on net neutrality—are thus to be applied based on a technology-neutral approach. Concrete details will be decided as the work proceeds and the draft will be published for public consultation. The scope has been clearly and narrowly defined as addressing the extent to which network slicing falls within the purview of the TSM Regulation and, specifically, how Art. 3(5) of the TSM Regulation applies to specialised services.

A public consultation on the first draft of the guidance has been tentatively planned for June 2026. The final version of the guidance together with the final report on the consultation is likely to be published towards the end of the year.⁶

⁵ Options for offering services based on 5G network slicing depend on the availability of 5G standalone (5G SA). In contrast to non-standalone, which makes use of the 4G core network, 5G SA means that both the radio network and the core network are based on 5G. Use of the 5G SA deployment mode and compatible end-user devices is more widespread in various Asian countries and the USA than in Europe.

⁶ https://www.berec.europa.eu/system/files/2025-12/BoR%20%2825%29%20186_BEREC_WORK_PROGRAMME_2026.pdf

05

Internet blocking

05 Internet blocking

5.1 Overview of activities

To safeguard net neutrality, the TSM Regulation specifies that providers of internet access services are not to block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof. The Net Neutrality Regulation does also include some exceptions to this basic principle. Thus, the listed measures can be taken insofar and for as long as they are necessary to comply with EU legislative acts or national laws or related implementing measures.

The regulatory authority has been taking a closer look at the issue of network blocking for a number of years now. This stems from concerns that every network block compromises the core principle of net neutrality and potentially affects the right of internet users to freedom of expression, while also forcing providers into the involuntary role of judges. The aim here must be to identify ways and means of maximising the legal protection and certainty enjoyed by all stakeholders. In keeping with this aim, legislative activities at national and European level are closely observed, with the resulting insights actively applied when transposing EU-level provisions into national law.

Accordingly, we have submitted numerous statements in review of draft legislation in recent years. In these reviews we have underscored the importance of free access to the open internet, and the technical challenges raised by network blocking. We as regulatory authority are clearly aware of the completely new challenges arising as more and more daily activities move online, making it even more difficult and tedious for users to assert their rights. Nonetheless, it needs to be emphasised that network blocking is and must always be a last resort. Any excessive use would result in collateral damage and potentially jeopardise freedom of expression in a liberal society. After all, network blocking often entails the risk of 'overblocking'. An ISP only has a certain set of options for blocking online content, and these options often result in the blocking of not only illegal but also legal content. Accordingly, such measures should be used sparingly.

To ensure transparency, RTR publishes all of the currently active blocking measures on its website.⁷ This list is additionally provided in the Open Data format.⁸

5.2 Internet blocks to protect copyright

For more than 20 years, copyright law has included provisions potentially requiring providers of internet access services, alongside the often elusive hosting service providers, to set up internet blocks for websites 'intentionally structured to infringe law'. In the past, this circumstance has led to various court cases involving ISPs and rights holders. Such cases regularly end up before national or European supreme courts. More recently, additional EU legislative instruments have required measures to limit the web content provided by various online agents. Examples include the Consumer Protection Cooperation Regulation⁹ and the Market Surveillance Regulation¹⁰.

⁷ https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/nn_blockings.de.html

⁸ <https://www.data.gv.at/katalog/dataset/f7e9b0f3-60ab-4f53-964a-c6c88c3f681d>

⁹ Regulation (EU) 2017/2394 of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004, OJ 2017 L 345, p. 1

¹⁰ Regulation (EU) 2019/1020 of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ 2019 L 169, p. 1

In the previous reporting period, the relationship between the Net Neutrality Regulation and internet blocks resulting from copyright claims was examined for the first time by the ECJ. This action was prompted by supervisory procedures the Telekom-Control-Kommission had initiated in response to certain IP blocks that some internet access service providers had implemented in their networks. The Telekom-Control-Kommission ruled that the IP blocks set up by the ISPs were excessive and unlawful, and ordered their removal in cases where these blocks were still active. The affected rights holder appealed this decision to the Federal Administrative Court (BVwG), which duly requested the ECJ's interpretation of this and other cases. After the initiation of the written procedure before the ECJ, the rights holder then withdrew their appeal at national level in Austria, causing the ECJ to duly terminate its preliminary ruling procedure. As a result, the TTK's decisions became final.

In addition, between May 2024 and April 2025, six supervisory procedures were conducted pursuant to Art. 5 TSM Regulation to review access blocks for certain websites resulting from injunctions served by copyright holders. The TTK concluded these supervisory procedures with a decision. These procedures concerned DNS access blocks, which in these cases had been lawfully set. No procedures of this kind were conducted during the current reporting year.

5.3 Internet blocking pursuant to the Consumer Protection Cooperation Act

Another legal context allowing, as of March 2021, network blocks to be set is the EU Consumer Protection Cooperation Regulation (CPC)¹¹ and accompanying Austrian legislation, the Consumer Protection Cooperation Act (VBKG). These rules are intended as an effective means of countering cross-border infringements of consumer rights. Numerous European authorities coordinate their efforts in this cause. Authorities can now file injunctions against businesses that infringe upon consumer rights. Sometimes, however, companies cannot be directly prosecuted in an online context. This might be the case where a firm is established outside the EU and does not respond to claims. In such cases, the online intermediaries can be held accountable for remedying infringements at internet level. This could potentially be any information society service, including access providers, host providers, caching providers, search engine providers or even domain registration services. These providers are then ordered to delete the unlawful online content or set a network block. In Austria, the TTK is the authority responsible for taking measures involving intermediary online service providers. Here, network blocks can only be set after review and authorisation by an authority. The corresponding procedure defined by the TTK is aimed at resolving challenges and deficits relating to network blocking arising in the past. The procedure could serve as a model to be applied in other areas as well. Network blocks based on the CPC Regulation were not initiated or required during the reporting period.

5.4 Internet blocking pursuant to the EU Market Surveillance Regulation

The Market Surveillance Regulation¹² creates a pan-European legal framework for responding to novel economic developments and challenges, with a particular focus on international e-commerce and logistics services. One aim for this Regulation was to close previous loopholes that had allowed third-country goods lacking EU conformity to be distributed within the EU market via online platforms, with the economic operators in the EU directly responsible unable to be identified. This Regulation follows the CPC Regulation in extending the potential addressees of orders to take steps to prevent online infringements,

¹¹ Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004

¹² Regulation 2019/1020 of 20 June 2019 on market surveillance and compliance of products

beyond economic operators to potentially include online brokers, meaning those providing information society services, such as access, hosting or caching providers as well as search engine operators. In Austria, the Telekom-Control-Kommission is the competent body for ordering the introduction of measures by certain online brokers in matters for which the Federal Office of Metrology and Surveying (*Bundesamt für Eich- und Vermessungswesen*) is the market surveillance authority.

In the previous period under review, one procedure was initiated pursuant to the EU Market Surveillance Regulation. This procedure involved a request from the Federal Office of Metrology and Surveying (*Bundesamt für Eich- und Vermessungswesen*, BEV) as the market surveillance body to order the introduction of restrictive measures by online intermediaries with the aim of preventing access to a website listing a dangerous product. The procedure was terminated in August 2025, as result of the request to initiate the procedure being withdrawn.

5.5 War in Ukraine: internet blocking pursuant to the EU Sanctions Regulation

The EU Sanctions Regulation¹³ adopted in March 2022 (and amended several times since) created new blocking requirements for ISPs, aimed at suppressing the EU-wide distribution of content from certain government-affiliated Russian media companies. In the opinion of the TTK and the RTR's Telecommunications and Postal Services Division—the competent regulatory authorities for safeguarding net neutrality—no national administrative act is needed to transpose the EU Sanction Regulations. As an EU Regulation, the law applies immediately in Austria and also applies to providers of internet access services. The regulatory authorities consider the law to be an EU legislative act within the meaning of Art. 3(3) subparagraph 3(a) TSM Regulation. This opinion is shared by BEREC.¹⁴

On 13 April 2022, supplementing the immediate applicability of the EU Sanctions Regulation, the Audio-visual Media Services Act (AMD-G)¹⁵ was amended to extend the remit of the Austrian Communications Authority (KommAustria) as a prosecuting authority to include measures against ISPs. Their website provides a detailed list of the content currently to be blocked according to their interpretation.¹⁶ Based on this publication, measures adopted by providers of internet access services in line with the accepted interpretation of the EU Sanctions Regulation therefore do not normally breach applicable laws aimed at safeguarding net neutrality.

5.6 Internet blocking pursuant to MiCA

The new EU Markets in Crypto-Assets Regulation (MiCA)¹⁷ has created a harmonised legislative framework within the EU for public offerings of crypto assets, their admission to trading and the provision of services in relation to crypto assets. In some circumstances, the powers awarded to the competent authorities also envisage placing third parties (such as ISPs) under an obligation to limit access to websites, with the aim of curtailing breaches of the corresponding provisions of this regulation. The Austrian national legislation introduced to implement MiCA names the Austrian Financial Market Authority (FMA) as the competent authority.

¹³ Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014, as since amended by Regulation (EU) 2022/879, Regulation (EU) 2022/2474, Regulation (EU) 2023/427, Regulation (EU) 2023/1214, Regulation (EU) 2024/1428, Regulation (EU) 2024/3192 and Regulation (EU) 2025/395

¹⁴ <https://www.berec.europa.eu/en/news-publications/news-and-newsletters/berec-supports-isps-in-implementing-the-eu-sanctions-to-block-rt-and-sputnik>

¹⁵ See Art. 64 Par. 3a AVMDG as amended by Federal Law Gazette (FLG) I No. 55/2022.

¹⁶ https://www.rtr.at/Paragraf_64_3a_AMD-G

¹⁷ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

In March 2026, four network operators notified the regulatory authority that they had set internet blocks for the `standardingold.com` domain in response to decisions taken by the FMA. This domain name had been used to host a website offering crypto assets in contravention of the MiCA provisions. In October 2025, the website operator was duly prohibited from offering the 'SOLID' crypto asset to users based in Austria.

In the opinion of the TKK and RTR's Telecommunications and Postal Services Division—the competent regulatory authorities for enforcing the EU Net Neutrality Regulation—the EU legislation MiCA and the FMA decision issued based on the MiCA should be seen as an official order pursuant to Art. 3(3) subparagraph 3(a) TSM Regulation. In addition, internet blocking was implemented using DNS blocks, which is in line with the TKK's earlier rulings on internet blocks. No breach of the net neutrality provisions was therefore identified.

5.7 Previous general decisions by the TKK on IP blocks

During the May 2023 to April 2024 reporting period, the TKK issued decisions on numerous blocks pursuant to Art. 3(3) subparagraph 3(a) TSM Regulation, set by several ISPs in response to complaints from rights holders about websites structured to breach copyright law pursuant to Art. 81 Par. 1a of the Austrian Copyright Act (UrhG).

Assessing a particular type of block proved to be especially challenging here. In this case, the ISPs had not only set up a block at the DNS resolver level for a website but had also instigated a block on a specific IP address. This had been done on the one hand because the rights holder considered a combination of a DNS and IP block to be a more effective blocking measure. On the other hand, the site to be blocked—one that cloned a film and series streaming portal that called itself 's.to' and which was structured to breach copyright law—was directly accessible from this IP address, while the domain as such, to which a DNS block had also been applied, resolved to a different IP address.

During the course of the procedure by the TKK, an official expert opinion was requested, elucidating the impact and effectiveness of the various blocking methods, as well as the differences between them and techniques for bypassing the same. A privately commissioned technical expert opinion was submitted by the rights holder. The TKK arrived at technical findings based on these two opinions.

It was ascertained that the IP address in question had been assigned to the hosting service and content delivery network DDoS-Guard. From a technical perspective, this provider—or their customer—is the only entity able to control, change or specify the content accessible under the IP address. The website itself was set up in such a way that the actual streams were not sent from the IP addresses that were the subject of the procedure but were provided by other IP addresses with the use of a technique known as inline frames (iframes). This technique was invisible to end users.

This proved an issue, since the specific IP address was also being used to host other content. In principle, it is impossible to identify in full all of the content accessible via an IP address. Accordingly, there is no clear-cut relationship between an IP address and a domain in either direction, since IP addresses and domains are independent components of the world wide web. From a technical perspective, a domain does not have to be assigned to exactly one IP address nor, conversely, does a single IP address have to be restricted to hosting only one specific domain. It is common industry practice for a domain to be assigned to multiple IP addresses and, conversely as well, industry-standard server software permits a virtually unlimited number of domains to be served from one single IP address.

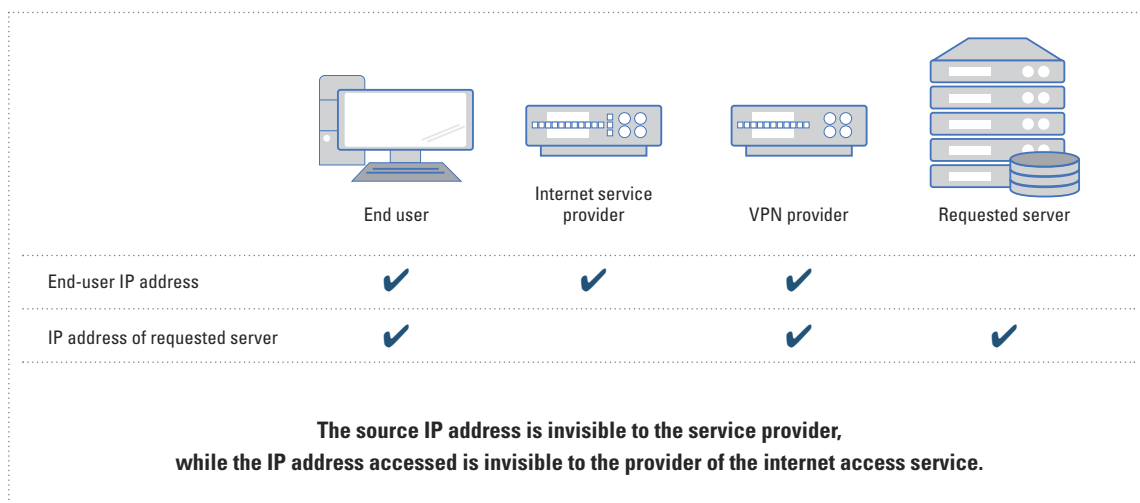
For a third party such as a technical expert, a regulatory authority or—in particular—a provider of internet access services, determining all of the IP addresses linked to a domain or all of the content accessible from a specific IP address is an impossible task. While a heuristic listing can be obtained by using certain third-party services, this listing is itself limited to the domains discovered using ‘web crawling’ techniques.

Domains and IP addresses are addressing elements that are deployed at separate layers within the OSI model. Domains are used to interact with end users on the internet. The fact that IP addresses are actually used in the engineering behind the scenes is a mere technicality that more often than not goes unnoticed by the vast majority of internet users. As the most visible characteristic of any service is its domain, the specific IP address used in practice is essentially irrelevant for end users.

As far as the effectiveness of a block is concerned, end users can make use of three techniques to bypass an IP access block such as the one that was the subject of this procedure, namely: VPN services, the Tor browser and the use of an HTTP proxy server. Essentially, these services work by rerouting data traffic between the end-user device and the server deployed by the operator of the streaming link portal via a server or network provided by a third party (such as a VPN provider). In such a case, the IP address of the server being accessed is no longer visible to the internet access provider (see figure 3).

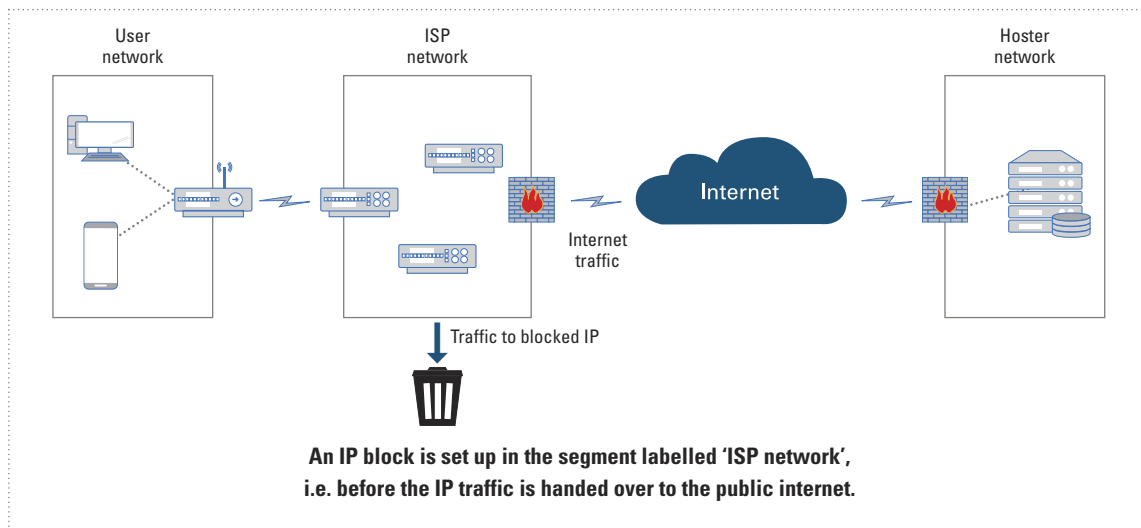
Such services (e.g. Apple Private Relay) can also be installed and used by individuals with minimal technical expertise.

Figure 3: Using a VPN to access a service



Blocks also have only limited effectiveness against service providers. If an IP block has been applied to the service provider, then the latter can simply bypass this block by switching to another IP address. This technical change remains unnoticed by end users who are accessing the service via a domain.

In technical terms, IP blocks are implemented so that IP packets that have the IP address to be blocked as their target address are not forwarded by the provider but are discarded (see figure 4). The IP address is therefore no longer reachable for end users of the provider setting the block. The block, in turn, does not impact end users of other providers. Unlike DNS blocks, no information about the block is shown when trying to access the blocked IP address: instead, connections to the blocked IP address are simply prevented.

Figure 4: Networks involved in accessing a website

The implementation of IP blocks by individual providers of internet access services is also undetectable by the owners of the blocked IP address. Visitors can still access the site—connections are only prevented from end users of the internet access service provider who has set up the block.

From a technical perspective, an IP block therefore always carries a risk of ‘overblocking’—the accidental and unintentional blocking of content that is entirely unrelated to the reason for the block and its context. This is because it is technically impossible to identify all of the online content hosted under a single IP address.

Taking into account the risk of overblocking, the regulatory authority prohibited the implementation of an IP block. Pursuant to the principle of proportionality required by Art. 3(3) subparagraph 3(a) TSM Regulation, the potential impact of a block must be balanced against fundamental rights and freedoms. As a single IP address can be used to operate not just one but multiple websites and services, setting up IP blocks necessarily results in a (relatively far-reaching) restriction on the freedom of communication established by Art. 11 of the Charter of Fundamental Rights of the European Union (CFR), particularly as there is no means of obtaining a full list of websites that are (or were) being hosted by a specific IP address.¹⁸ When used with shared hosts or cloud-based services, where various IP addresses can be allocated to an individual service simultaneously or in a geographically distributed manner, IP blocks can constitute an encroachment on the freedom to conduct a business, as guaranteed by Art. 16 CFR, for both end users and the providers of services and applications. This makes it impossible for service providers to ascertain whether their own IP address is subject to any IP blocks set up by individual providers. A website operator who is using a dynamic public IP address instead of a static public IP address to host their website would become instantly affected by the consequences of an IP access block if their site were to be assigned an IP address that had been blocked by some provider or other. Nor would the timing of this event be precisely predictable.

Compared with DNS blocks, IP blocks necessarily involve a reduced level of transparency. With DNS blocks, internet users are usually forwarded to a page set up by the blocking provider when they attempt to access the blocked domain. This page informs them about the block and the reason for its implementation. In the case of IP blocks, however, the background IP connection to the blocked IP target address is simply prevented, so that no information is provided to the internet user about the existence of the IP block. This makes it more difficult for the affected party to discover the reason for the block and assert any relevant claims.

¹⁸ See for example TTK 7 August 2023 R 16/22 p. 28 ff.

On the other hand, owners of copyright claims have the interest (based on the protections to intellectual property guaranteed by Art. 17(2) CFR) in the reliable prevention of unlawful access. Yet it should be noted here that IP blocks can still be bypassed by end users with relatively basic IT skills using a reasonable amount of effort. Accordingly, an access restriction that could be considered impregnable or able to be circumvented only with an entirely unreasonable amount of effort cannot in fact be achieved even with the implementation of IP blocks.

In applying the principle of proportionality, the TTK therefore ruled that the implementation of an IP block was a disproportionate measure that constituted a breach of Art. 3(3) TSM Regulation and therefore had to be remedied.

The rights holder appealed these decisions from the TTK to the Federal Administrative Court (BVwG). During the appeal proceedings, that court submitted several cases to the ECJ for a preliminary ruling on the essential legal question raised by these cases, namely how legislation to protect intellectual property relates to legal acts aimed at protecting net neutrality. In particular, the ECJ was to clarify whether an IP block can be proportionate and therefore permissible.

After the initiation of the written procedure before the ECJ, the rights holder then withdrew their appeal at national level in Austria, causing the ECJ to duly terminate its preliminary ruling procedure. As a result, the TTK's decisions became final.

Potential breaches of net neutrality and procedures

06 Potential breaches of net neutrality and procedures

Since the enactment of the TSM Regulation, the regulatory authority has continuously reviewed the products currently offered on the market as well as the technical and commercial practices adopted by ISPs. As in previous reporting periods, the work of the regulatory authority focused on first auditing ISPs' products and technical/commercial practices and then confronting the ISPs with any potential breaches identified and consulting with them to identify legally compliant solutions. In the preceding reporting periods, the regulatory authority had conducted numerous procedures aimed at safeguarding net neutrality. The majority of these procedures concerned IP blocks, forced disconnections, zero-rating and failures to provide a public dynamic IPv4 address. During the current reporting period, various practices were again identified as raising issues in light of the provisions of Art. 3 of the TSM Regulation and needed to be reviewed for compliance. Most cases concerned internet blocks set on the basis of MiCA, while the EU Market Surveillance Regulation was the legal basis for just one procedure. For further details, see section 5.

Table 2: Summary of potentially problematic practices in relation to the TSM Regulation

Pos.	Type of practice	Description
01	Port blocking	Certain UDP or TCP ports are blocked for incoming and/or outgoing traffic. This might render certain services unusable, representing a contravention of Art. 3(1) and (3) of the TSM Regulation. → A more detailed description is given in section 6.1.
02	Private IP addresses and services	Customers are assigned private IP addresses, via network address translation (NAT). This prevents these customers from using or providing their own services; this right follows, however, from Art. 3(1) of the TSM Regulation. → A more detailed description is given in section 6.2.
03	Zero-rating	The data volume used by a specific application or for a specific CAP is not counted towards the data volume cap included in the customer's subscription. A more detailed description is given in section 6 of the 2023 Net Neutrality Report.
04	Specialised services	A specialised service is a service that is not offered by the ISP via normal internet access service (IAS) but instead as a prioritised/optimised service. To be offered as a specialised service as defined by Art. 3(5) of the TSM Regulation, a service must first satisfy certain conditions.
05	Technical discrimination and restriction of internet access	Traffic modification/redirection or the placing of restrictions on the IAS contravenes Art. 3(3) of the TSM Regulation.
06	Disconnection of IP connections	Automated disconnection of IP connections restricts the rights of the end user to provide their own services (Art. 3(1) TSM Regulation). → A more detailed description is given in section 7 of the 2025 Net Neutrality Report.

Pos.	Type of practice	Description
07	Internet blocking	Network blocks contravene net neutrality by their very nature, and are therefore only permitted if they are prescribed by law and the blocks are proportionate in the specific case. Legal provisions requiring ISPs to set up blocks can be found in the Copyright Act (UrhG), in the context of cooperative cross-border consumer protection (Consumer Protection Cooperation Act, VBKG), in relation to market surveillance (EU Market Surveillance Regulation) or the financial sector (EU Markets in Crypto-Assets Regulation), or may stem from sanctions (EU Sanctions Regulation). → A more detailed description is given in section 6.4

Alongside the regulatory authority's reviewing activities in relation to existing products, as described above, contractual documents such as general terms of business and fee provisions were also reviewed for compliance with the TSM Regulation, pursuant to the authority's statutory remit to review contract terms (Art. 133 TKG 2021). With respect to the minimum content of contracts as required in Art. 4(1) of the TSM Regulation, no immediate steps based on the TSM Regulation were required in formal procedures during the reporting period.

In the procedure concerning objections to general terms of business, the aim is to have non-conforming contract conditions amended before the conclusion of the procedure, so as to efficiently ensure the legal conformity of contract conditions.

6.1 Blocking of TCP/UDP ports or protocols

No new procedures addressing port blocking were initiated in the reporting period. Many such procedures have been completed in recent years. The technical reasons for blocking specific ports were clarified in most of these cases. Port blocking can be acceptable given sufficient legal justification, although blocks to date have been made solely from a security perspective. In comparison with recent years, there was a decline in active port blocking. This resulted from the replacement of a modem model whose inherent security vulnerabilities had previously been the reason for these blocks, which could then be consequently revoked.

Here it needs to be remembered that an assessment of the legitimacy of port blocking activities always requires a case-by-case approach. Accordingly, the fact that one procedure has considered a port block in a specific scenario to be legitimate does not automatically infer the outcome of other assessments of port blocking that involve other ISPs.

When attempting to assess the proportionality of port blocking, useful guidance is provided in the guidelines published by ENISA on assessing security measures adopted pursuant to Art. 3(3) TSM Regulation.¹⁹

The following section offers a summary of selected previous outcomes.

TCP port 25 (SMTP)

One mobile network provider and one fixed network provider stated that they block outgoing traffic on port 25. Another fixed network provider confirmed a bidirectional block on port 25. The key reason for such a block is to prevent a customer's computer from sending spam mail after becoming infected by malware. If the provider only assigns private IP addresses (via NAT) and a public IP address that is shared by many customers via NAT is blacklisted, all email from those customers could be blocked.

¹⁹ <https://www.enisa.europa.eu/publications/guideline-on-assessing-security-measures-in-the-context-of-article-3-3-of-the-open-internet-regulation>

When assessed pursuant to point (b) of Art. 3(3) third subparagraph, this block was considered to be legitimate—as in previous procedures—since (pure) SMTP is a protocol frequently misused at retail level (for sending spam).

TCP/UDP port 53 incoming (DNS)

Three ISPs reported using this block to avoid the risks of DNS amplification attacks and DNS spoofing. Two ISPs reported that use of these blocks was limited to end users with dynamic public IPs.

TCP ports 67–69 bidirectional (DHCP, BOOTPS, TFTP)

One fixed network provider blocks this port for use by specific internet access technologies for technical reasons based on their network topology (CPE maintenance).

After a lengthy analysis, the block was considered legitimate pursuant to point (b) of Art. 3(3) third subparagraph in the absence of a less intrusive solution and since the TFTP protocol now has hardly any practical relevance for end users in terms of internet access.

TCP ports 137–139 bidirectional (NetBIOS)

One fixed network provider blocks this port range, arguing that within a WAN there is no use case for the Windows file and printer sharing services, which function via these ports. Simultaneously, opening these ports would also expose customers to considerable risk, since they are not experienced in handling these services. In the event of a customer misconfiguration, there would be a risk of unauthorised parties gaining access to their network shares.

Following an analysis based on point (b) of Art. 3(3) third subparagraph, these blocks were considered legitimate for incoming traffic.

TCP port 445 incoming (SMB)

One fixed network provider blocks this port for incoming traffic on account of security concerns in relation to end users. In the case of the other fixed network provider, following an analysis based on point (b) of Art. 3(3) third subparagraph, these blocks were considered legitimate for incoming traffic.

TCP port 455 incoming (CreativePartnr)

One fixed network provider reported blocking this TCP port for maintenance reasons. The block has since been removed or is activated only in the event of maintenance.

TCP ports 10001, 10021, 10080 and 10081

One fixed network provider reported blocking these TCP ports for maintenance reasons. As this affected only a few modems and the ports are not in the ‘common port’ range, this block was considered to be justified based on point (b) of Art. 3(3) third subparagraph.

TCP port 8089

One MVNO requested an extension to allow time to replace affected hardware that sets up CPE maintenance connections via this port. This extension was granted due to the scope of replacement work. This block has since been lifted.

6.2 Private IP addresses and services

The TSM Regulation grants end users the right to use and provide applications and services. A key technical prerequisite for the self-hosting of services is the direct accessibility from the internet of the server or service operated by the end user, and the assignment of a public IP address.

In mobile networks in particular, end users are occasionally assigned private IP addresses (using NAT). Apart from technical aspects, among the reasons for this practice is the ISPs' interest in keeping public addresses in reserve, since—as with IPv4—these could become scarce. However, if multiple end users are required to share a single private IP address via NAT, this effectively prohibits any specific customer from directly providing services or content. The regulatory authority interprets Art. 3(1) as entitling the end user to at least one free public dynamic IP address—at least if the end user requests such an address, for example because of wishing to provide services. The end user can then utilise that address with dynamic DNS services to allow routing to their own services. Assigning a public IP address on condition of payment of an additional fee (defined for instance in a specific subscription model or as an added option) or only to certain customer segments (such as business customers) is unconditionally to be considered a breach of Art. 3(1). Particular attention was paid to problems arising from the need for the availability of public IPv4 addresses in connection with the use of new modems/routers on the part of one ISP. Here, a newly deployed provider device appeared to offer no support for bridge mode or port forwarding and therefore, from a technical perspective, would be incapable of utilising a public IPv4 address, if assigned. There was also a suspicion that technical means had been put in place by the provider to prevent end users from using an additionally purchased alternative modem possessing this functionality. Ultimately, it was discovered that end users could request the provision of an alternative modem at no extra cost and this modem would indeed support a configuration in bridge mode.

End user's right to provide their own services—as guaranteed by the TSM Regulation—was thereby maintained. Information obtained in the last reporting period has shown that end users occasionally receive incorrect information on this topic in response to enquiries made to their ISP and then contact the regulatory authority to clarify the current legal situation.

6.3 Disconnection of IP connections

In the course of review procedures pursuant to Art. 5(2) TSM Regulation, five providers of mobile internet access services were audited in the previous reporting period. These procedures made use of a 'mystery shopper' appointed by the regulatory authority, who requested a dynamic public IP address and conducted tests to determine how often the IP connection from the respective internet access service was disconnected by the provider. In all five procedures, the dynamic public IP address was provided on request. In three of the five procedures, a forced disconnection of the IP connection occurred every 31 days and was therefore acceptable. In two procedures, a forced disconnection of the IP connection occurred in less than 31 days. The providers were ordered to extend the disconnection period to 31 calendar days. Back in the previous reporting period, legal compliance was duly restored in both cases. In the period under review, there was no evidence of any breaches in relation to the disconnection of IP connections.

6.4 Internet blocking

Since 2018, the regulatory authority has conducted procedures in 100 cases involving network blocking. Here care has been given to ensure that any measures enacted comply with the Net Neutrality Regulation, by avoiding excessive interference with users' fundamental rights and by respecting the rights of other parties concerned, including ISPs and website operators. The majority of these procedures were supervisory procedures, meaning that ISPs had already set network blocks. A few of the cases involved 'assessment' procedures, where ISPs had requested an assessment as to whether a network block was prohibited. The administrative decisions issued in such cases are ultimately brought to the attention of the Supreme Administrative Court, which for the first time ruled on the Net Neutrality Regulation.

Major activities in connection with network blocking include exchanging information with stakeholders, public relations and participation in legislative processes. Accordingly, we have submitted numerous statements in review of draft legislation in recent years. In these reviews we have underscored the importance of free access to the open internet, and the technical challenges raised by network blocking. We as regulatory authority are clearly aware of the completely new challenges arising as more and more daily activities move online, making it even more difficult and tedious for users to assert their rights. Nonetheless, it needs to be emphasised that network blocking is and must always be a last resort. Any excessive use would result in collateral damage and potentially jeopardise freedom of expression in a liberal society. After all, network blocking often entails the risk of 'overblocking'. An ISP only has a certain set of options for blocking online content, and these options often result in the blocking of not only illegal but also legal content. Accordingly, such measures should be used sparingly.

Since March 2021, network blocks can also be set in another context, as permitted by the EU Consumer Protection Cooperation Regulation (CPC) and accompanying Austrian legislation, the Consumer Protection Cooperation Act (VBKG). These rules are intended as an effective means of countering cross-border infringements of consumer rights. Numerous European authorities coordinate their efforts in this cause. Authorities can now file injunctions against businesses that infringe upon consumer rights. Sometimes, however, companies cannot be directly prosecuted in an online context. This might be the case where a firm is established outside the EU and does not respond to claims. In such cases, the online intermediaries can be held accountable for remedying infringements at internet level. This could potentially be any information society service, including access providers, host providers, caching providers, search engine providers or even domain registration services. These providers are then ordered to delete the unlawful online content or set a network block. In Austria, the TTK is the authority responsible for taking measures involving intermediary online service providers. Here, network blocks can only be set after review and authorisation by an authority. The corresponding procedure defined by the TTK is aimed at resolving challenges and deficits relating to network blocking arising in the past. The procedure could serve as a model to be applied in other areas as well. Network blocks based on the CPC Regulation have not been implemented to date.

The EU sanctions regulation imposed in March 2022 initially introduced new blocking obligations for ISPs. In the years that followed, new packages of sanctions further extended these obligations. In the opinion of the TTK and the RTR's Telecommunications and Postal Services Division—the competent regulatory authorities for safeguarding net neutrality—no additional national administrative act is needed to transpose the EU Sanction Regulation. As an EU Regulation, the law applies immediately in Austria and also applies to providers of internet access services. The regulatory authorities consider the law to be an EU legislative act within the meaning of Art. 3(3) subparagraph 3(a) TSM Regulation. Measures adopted by providers of internet access services in line with the accepted interpretation of the EU Sanctions Regulation therefore do not normally breach applicable laws aimed at safeguarding net neutrality.

Additional, more specific legal bases for network blocking exist for copyright law, market surveillance and financial market supervision. (For details, see section 5—Internet blocking).

Website blocking in the reporting period

During the reporting period, the regulatory authority was notified of internet blocks set for the standardgold.com website by four providers. This was in response to decisions issued by the Austrian Financial Markets Authority (FMA), the competent authority for enforcing the MiCA Regulation. The blocks were implemented as DNS blocks. In the TKK's opinion, these blocks do not breach net neutrality, as MiCA and the related decision are to be seen as establishing a legal basis as defined in Art. 3(3) subparagraph 3(a) TSM Regulation.

6.5 Measures in accordance with Art. 5(1) TSM Regulation

Various supervisory procedures are not listed here that were initiated but then terminated with a decision. These include cases where the ISP resolved the issue before the end of the procedure or was not found to be in breach of the TSM Regulation. The regulatory authority nonetheless monitored compliance with the provisions of the Net Neutrality Regulation on an ongoing basis. Table 3 lists all decisions issued since the entry into force of the TSM Regulation. The full text of these decisions can also be accessed on the RTR website (in German) at: <https://www.rtr.at/TKP/aktuelles/entscheidungen>

On the topic of access blocks, the TKK issued eight cease orders in August 2023 (R 16/22, R 17/22, R 29/22, R 31/22, R 33/22, R 38/22, R 39/22 and R 43/22). The rights holder appealed these decisions. In the appeal proceedings before the BVwG, a preliminary ruling was initially requested from the ECJ, addressing issues including the legality of IP blocks under EU law. As the appellant subsequently withdrew their appeal in February 2025, however, the appeal proceedings were cancelled, thus rendering the referred questions irrelevant. As a result, the TKK's decisions became final.

In November 2022, four providers were ordered to cease offering zero-rating contracts to existing customers by March 2023 (R 12/22, R 13/22, R 14/22 and R 15/22). (1) A1 Telekom was prohibited from offering its zero-rated 'Free-Stream' service in subscriptions and options, and the zero-rated 'epaper' subscription service as part of existing customer contracts. (2) T-Mobile was prohibited from offering its zero-rated 'Magenta Stream' service in subscriptions, as well as zero-rating as part of its add-on 'Mediencenter' subscription package for existing customer contracts. (3) Hutchison was prohibited from offering its zero-rated 'MyStream' subscription service, as well as zero-rating as part of its 'Spotify Premium' and '3 Cloud' add-on subscription packages for existing customer contracts. (4) educom was prohibited from offering its zero-rated 'free e-learning' subscription service for existing customer contracts, due to breaching the principle of equal treatment as defined in the TSM Regulation.

All providers had proactively withdrawn their zero-rated offers for new customers by 2022. As required by the TKK decisions, all zero-rating for existing customers had been discontinued by the end of March 2023.

The decisions on measures issued in December 2017 and April 2021 (R 3/16, R 5/17 and R 9/19), concerning the prioritisation of a VoD service, traffic shaping, forced disconnection and the allocation of a public IP address, all remain valid. In the appeal proceedings for R 3/16, the VwGH issued a ruling in December 2021 that confirmed the regulatory authority's decision in all points. A termination for R 5/17 was issued by the BVwG in April 2022, since the provider had withdrawn their complaint in response to the decision. The decision issued against another ISP in April 2021 has since become final (R 9/19).

Table 3: Procedures pursuant to Art. 5(1) TSM Regulation since 2016
 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 3/16	A1 Telekom Austria AG	- Prohibition of prioritising a VoD service for lack of a specialised service, within 3 years - Free assignment of public IPv4 at customer demand - Increase in period for disconnecting IP connections from 24 hours to 31 days	2017-12-18	
R 5/17	A1 Telekom Austria AG	Prohibition of applying traffic-shaping to an add-on package with zero-rated audio and video streaming services.	2017-12-18	
R 1/18	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2018-11-26	
R 2/18	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2018-11-26	
R 3/18	Salzburg AG für Energie, Verkehr und Telekommunikation	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2018-11-26	
R 4/18	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2018-11-26	
R 5/18	UPC Telekabel Wien GmbH, UPC Telekabel-Fernsehtz Region Baden Betriebs-gesellschaft m.b.H., T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2018-11-26	
R 8/18	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2018-11-26	

 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 9/18	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2018-11-26	
R 1/19	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-04-12	
R 2/19	Salzburg AG für Energie, Verkehr und Telekommunikation	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-04-12	
R 3/19	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-04-12	
R 4/19	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-04-12	
R 5/19	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-04-12	
R 6/19	UPC Telekabel Wien GmbH, UPC Telekabel-Fernsehnetz Region Baden Betriebs-gesellschaft m.b.H., T-Mobile Austria GmbH, Lisa Film GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-04-12	
R 7/19	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-07-08	
R 8/19	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2019-10-22	

 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 11/19	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2020-03-17	
R 12/19	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2020-03-17	
R 13/19	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2020-03-17	
R 14/19	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2020-03-17	
R 15/19	Kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2020-06-23	
R 1/20	Mass Response GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2020-07-21	
R 9/19	Lycamobile Austria Ltd.	Supervisory procedure resulting from failing to assign (at least) a dynamic public IPv4 address to end users.	2021-04-07	
R 1-9/22	Multiple providers of internet access services	Procedure pursuant to Art. 5 TSM Regulation assessing the admissibility of network blocks based on the EU Sanctions Regulation.	2022-06-13	
R 12/22	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 of the TSM Regulation, relating to zero-rated offers for existing customers.	2022-11-04	
R 13/22	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 of the TSM Regulation, relating to zero-rated offers for existing customers.	2022-11-04	
R 14/22	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 of the TSM Regulation, relating to zero-rated offers for existing customers.	2022-11-04	
R 15/22	educom GmbH	Supervisory procedure pursuant to Art. 5 of the TSM Regulation, relating to zero-rated offers for existing customers.	2022-11-04	

 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 16/22	next layer Telekommunikationsdienstleistungs- und Beratungs GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The rights holder initially appealed these decisions but subsequently withdrew their appeal and the procedure could therefore be dropped. As a result, the TKK's decisions became final.	2023-08-07	
R 17/22	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The rights holder initially appealed these decisions but subsequently withdrew their appeal and the procedure was therefore terminated.	2023-08-07	
R 18/22	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 19/22	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	
R 20/22	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-05-15	
R 21/22	next layer Telekommunikationsdienstleistungs- und Beratungs GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	
R 22/22	next layer Telekommunikationsdienstleistungs- und Beratungs GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 23/22	Mass Response Service GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure terminated for lack of a breach or, at time of decision, lack of an active breach of Art. 3(1) TSM Regulation.	2023-08-07	

 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 24/22	Mass Response Service GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 25/22	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure terminated for lack of a breach or, at time of decision, lack of an active breach of Art. 3(1) TSM Regulation.	2023-08-07	
R 26/22	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 27/22	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 28/22	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	
R 29/22	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The decisions were appealed. In the appeal proceedings, the BVwG requested a preliminary ruling, addressing issues including the legality of IP blocks under EU law. As the rights holder subsequently withdrew their appeal, however, this procedure was cancelled, also rendering the referred question irrelevant. As a result, the TKK's decisions became final.	2023-08-07	
R 30/22	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure terminated for lack of a breach or, at time of decision, lack of an active breach of Art. 3(1) TSM Regulation.	2023-08-07	
R 31/22	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The rights holder initially appealed these decisions but subsequently withdrew their appeal and the procedure could therefore be dropped.	2023-08-07	
R 32/22	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	

 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 33/22	Mass Response Service GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The rights holder initially appealed these decisions but subsequently withdrew their appeal and the procedure could therefore be dropped.	2023-08-07	
R 34/22	Mass Response Service GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	
R 35/22	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure terminated for lack of a breach or, at time of decision, lack of an active breach of Art. 3(1) TSM Regulation.	2023-08-07	
R 36/22	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 37/22	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	
R 38/22	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The decisions were appealed. In the appeal proceedings, the BVwG requested a preliminary ruling, addressing issues including the legality of IP blocks under EU law. As the rights holder subsequently withdrew their appeal, however, this procedure was cancelled, also rendering the referred question irrelevant. As a result, the TKK's decisions became final.	2023-08-07	
R 39/22	Salzburg AG für Energie, Verkehr und Telekommunikation	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The decisions were appealed. In the appeal proceedings, the BVwG requested a preliminary ruling, addressing issues including the legality of IP blocks under EU law. As the rights holder subsequently withdrew their appeal, however, this procedure was cancelled, also rendering the referred question irrelevant. As a result, the TKK's decisions became final.	2023-08-07	

 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 40/22	Salzburg AG für Energie, Verkehr und Telekommunikation	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure terminated for lack of a breach or, at time of decision, lack of an active breach of Art. 3(1) TSM Regulation.	2023-08-07	
R 41/22	Salzburg AG für Energie, Verkehr und Telekommunikation	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	
R 42/22	Salzburg AG für Energie, Verkehr und Telekommunikation	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 43/22	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Certain IP blocks set for specific websites as a result of copyright claims were found to constitute a breach of Art. 3(3) TSM Regulation. The rights holder initially appealed these decisions but subsequently withdrew their appeal and the procedure could therefore be dropped.	2023-08-07	
R 44/22	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-03-20	
R 45/22	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-01-09	
R 46/22	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-05-15	
R 1/23	Innonet ICT-Services GmbH	Supervisory procedure resulting from failing to assign (at least) a dynamic public IPv4 address to end users Procedure dropped for lack of an active breach of Art. 3(1) TSM Regulation at time of decision.	2023-09-11	
R 2/23	Mass Response Service GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-08-07	
R 3/23	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-08-07	

 : challenged |  : final

Procedure	ISP	Brief description	Date of decision	Status
R 4/23	kabelplus GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-08-07	
R 5/23	LIWEST Kabelmedien GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-08-07	
R 6/23	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no infringement of Art. 3 TSM Regulation identified.	2023-08-07	
R 1/24	T-Mobile Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright.	2024-06-10	
R 2/24	A1 Telekom Austria AG	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright.	2024-06-10	
R 3/24	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright.	2024-06-10	

6.6 Ensuring legally compliant terms of contract

With the TKG 2021, the TKG's task of ensuring that communications service providers' contractual terms and conditions (including general terms of service, service descriptions and tariff provisions) are legally compliant was transferred to RTR as of 1 November 2021. Providers must draw up contract terms and notify them to RTR in advance for review. RTR can reject the application of these contract terms to business transactions if the terms infringe any provisions of telecommunications law or certain points of civil or consumer protection law. Compliance specifically with the net neutrality-relevant provisions of Art. 4 TSM Regulation is also reviewed, so as to ensure that these transparency provisions are observed in order to safeguard net neutrality.

In 2025, 619 procedures were carried out. This represents an increase year on year of around 17% when compared with the 527 cases in 2025. Overall, when compared with 2021 (402 procedures) and 2020 (333 procedures), this points to a significant rise in cases. The factors responsible include the various adjustments made necessary by the TKG 2021, while providers of interpersonal communications services (NIICS) have also become subject to reporting requirements. Numerous enquiries from both end users and providers, relating to the notification or review of contractual conditions, were also handled. Content reviews of terms and conditions focus not only on compliance with provisions of telecommunications law but also civil and consumer protection legislation. In detail, it became apparent in 2024 that more and more European and international companies are becoming active as providers on the Austrian market. In ensuring legal compliance of contract terms, the TKG, along with RTR since 1 November 2021, has been facing a new set of challenges, since some of these providers have only limited knowledge of the relevant substantive and procedural provisions of Austrian and EU law, and may also not have an adequate command of German as Austria's official language.

The TKK, and since 1 November 2021 RTR, have been primarily concerned with ensuring that telecoms make any necessary changes to contract terms already doing procedures, thus ensuring that legal compliance is established as soon as possible. In every procedure in 2025, the TKK once again achieved this goal. For telecoms customers, checking through contract terms in advance reduces their risk of needing to go to court to clarify the legality of individual clauses once the contract has already been signed. Such legal proceedings are also associated with a very high financial risk. At the same time, consumers are often unable to identify potential legally non-compliant clauses that, although specified in the general terms of service, cannot be agreed with legal effect. This practice of vetting contract terms also makes an important contribution to fair competition between communications service providers while also preventing any competitive edge through the use of unlawful terms. In terms of net neutrality breaches, this also ensures monitoring and thus an early warning system as referred to in Art. 3 TSM Regulation.

6.7 RTR conciliation procedures

Pursuant to Art. 205 TKG 2021, end users can use conciliation procedures to submit complaints about communications services to the Telecommunications and Postal Services Division at RTR as a conciliation body, if they have been unable to come to an agreement with their provider. First and foremost, this body attempts to identify a solution that is acceptable to both the end user and provider. If consensus cannot be attained, then the conciliation body assesses the complaint from a technical and legal standpoint and expresses its legal opinion.

Of the roughly 1,900 telecoms conciliation cases in the period May 2025 to April 2026, 186 related to net neutrality, specifically involving complaints about quality. No changes were observed as regards complaint subject matter. Complaints addressed the following topics:

- Internet speed
- Provision of a public IP address
- Free choice of user device ('router freedom') and location of network termination point

For most of these complaints, ultimately a mutually agreeable solution could be identified for the end users and providers in the course of conciliation procedures.

The section below presents a chronological overview of conciliation procedures arising from complaints about quality (in most cases relating to contractual internet access speeds), compared with the prior period.

Table 4: Overview of conciliation procedures relating to quality complaints

Network quality	05/20 to 04/21	05/21 to 04/22	05/22 to 04/23	05/23 to 04/24	05/24 to 04/25	05/25 to 04/26
Mobile networks	162	118	69	87	68	125
Fixed network	85	54	47	26	39	61

6.8 General enquiries

RTR's Telecommunications and Postal Services Division also received enquiries relating to net neutrality independently of conciliation cases. Specifically, enquiries in the reporting period addressed minimum content pursuant to Art. 4 TSM Regulation, dynamic public IP and especially IPv6 addresses, router freedom and bandwidth. The relevant investigations found that providers had acted in compliance with the law on these issues. Ultimately, these enquiries can be attributed to a general interest in the subject or to misunderstandings in communications between providers and their customers.

On the topic of router freedom, an evaluation was carried out in 2023 to ascertain the need for a regulation pursuant to Art. 49 TKG 2021 (specification of the network termination point). The network termination point is the point at which the private network begins and the public network ends. The results of the evaluation did not identify any need to specify the network termination point at this time. Further details are available from our website.

Correspondents who submitted requests associated with router freedom, which also touched on the general legal framework applicable to this topic, were referred to the ongoing evaluation. Users requesting information about configuring bridge mode on routers from individual ISPs were referred to the body of information on this topic as collected by RTR and published on its website.

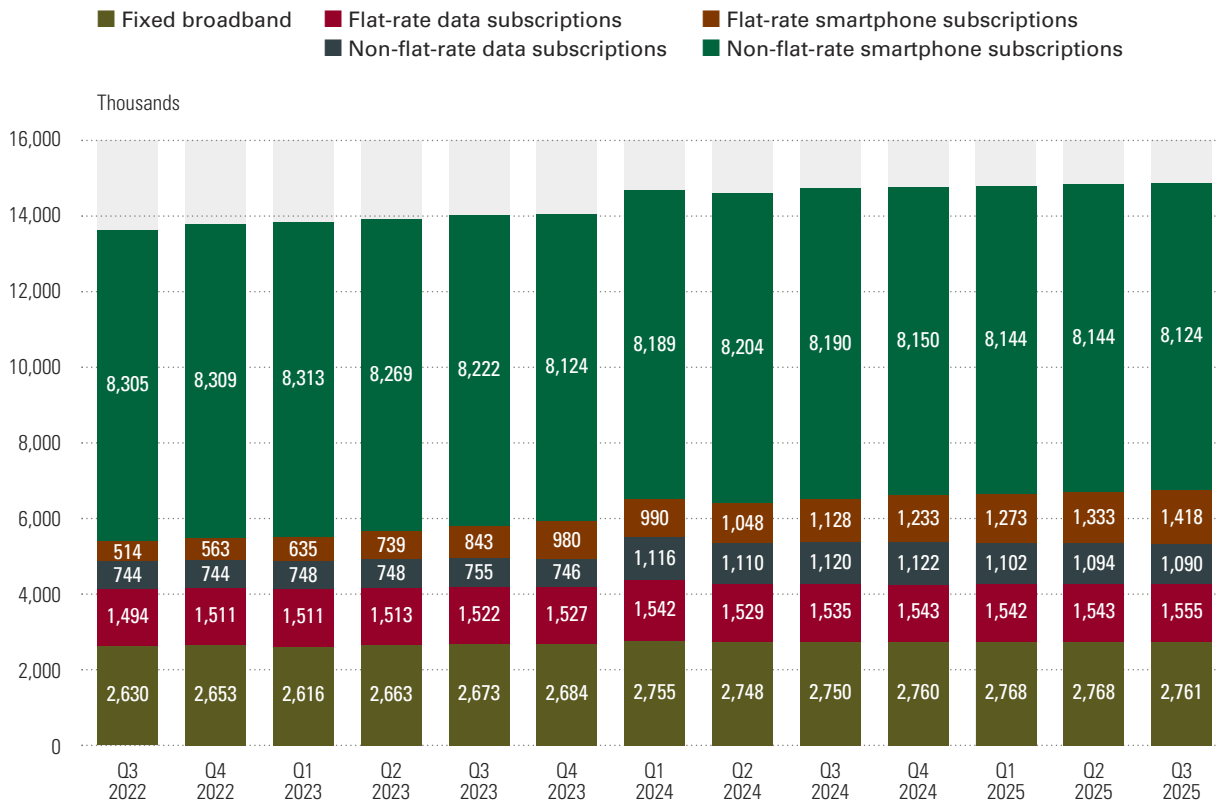
Indicators of continuous
availability of non-discriminatory
internet access services

07 Indicators of continuous availability of non-discriminatory internet access services

National regulatory authorities assess the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology (Art. 5(1) TSM Regulation). The following key figures are evaluated here:

- Number of broadband connections
- Distribution of download and upload speeds
- Median of download and upload speeds and latency
- Distribution of download and upload speeds by hour of day
- Price baskets: fixed vs. mobile broadband
- Quality dimensions

Figure 5 presents figures for fixed and mobile broadband connections over time. In the third quarter of 2025, total broadband connections rose to around 14.9 million—a 2% increase from about 14.7 million in the third quarter of 2024. Non-flat-rate smartphone subscriptions declined by 1%, falling from 8.2 to 8.1 million connections in this period. This contrasts with flat-rate smartphone subscriptions, showing the strongest percentage growth (although low in absolute terms) by rising 26% from 1.1 to 1.4 million. Data subscriptions also saw growth in subscriptions with unlimited data volume. The number of non-flat-rate data subscriptions fell 3% to 1.1 million, while the number of flat-rate data subscriptions rose 1% to 1.6 million.

Figure 5: Fixed and mobile broadband connections^{*)}

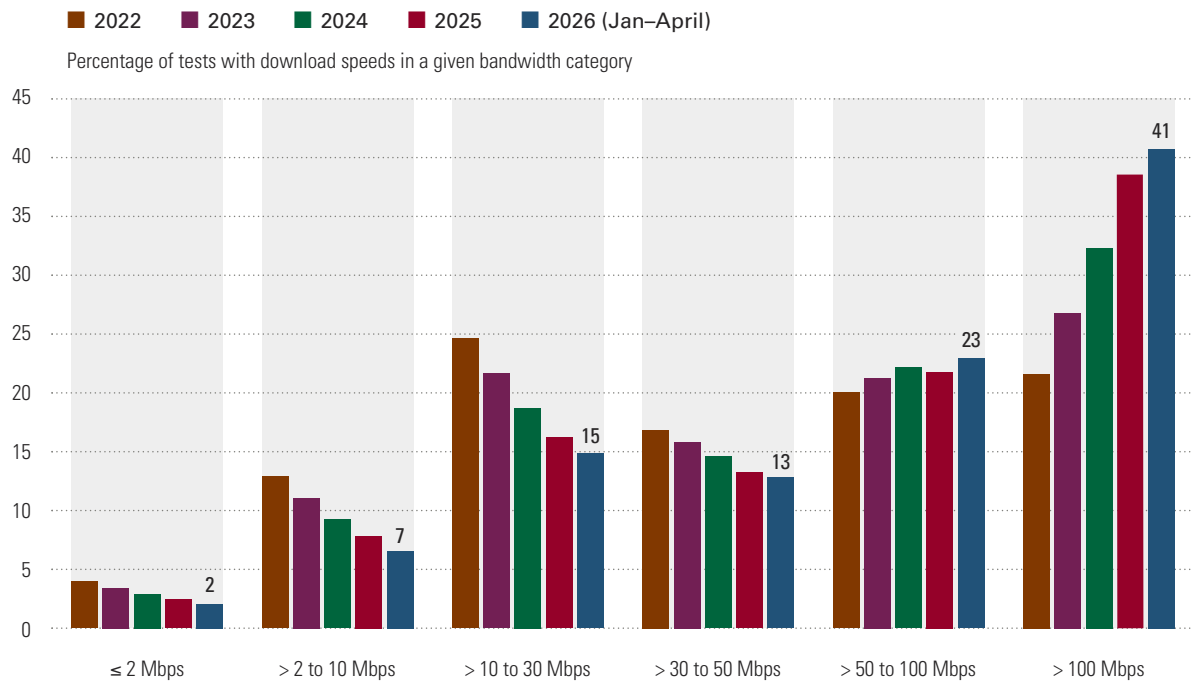
Source: RTR

^{*)} Data on broadband connections are collected quarterly. M2M SIM cards are not shown in the chart. KEV data are available in the form of Open Data at: https://www.rtr.at/rtr/service/opendata/OD_Uebersicht.de.html

Data from the RTR-NetTest are used to assess quality metrics in relation to internet access. The NetTest lets end users test the speed and quality of their internet access using a reliable method that is not dependent on a specific provider.²⁰ NetTest data are made publicly available as Open Data.²¹ Figure 6 shows the percentage of tests with download speeds in a given bandwidth category. In 2025 and 2026 (January to April), most tests can be assigned to the top category: download speeds of more than 100 Mbps. During 2025 and 2026 (January to April), categories featuring download speeds of less than 50 Mbps once again reveal a decline in share in comparison with previous periods. This contrasts with the strong growth posted in the category of download speeds of more than 100 Mbps. Since 2022, this category's share has risen from 22% to 41%. Thus, the trend measured indicating ever higher download speeds continues.

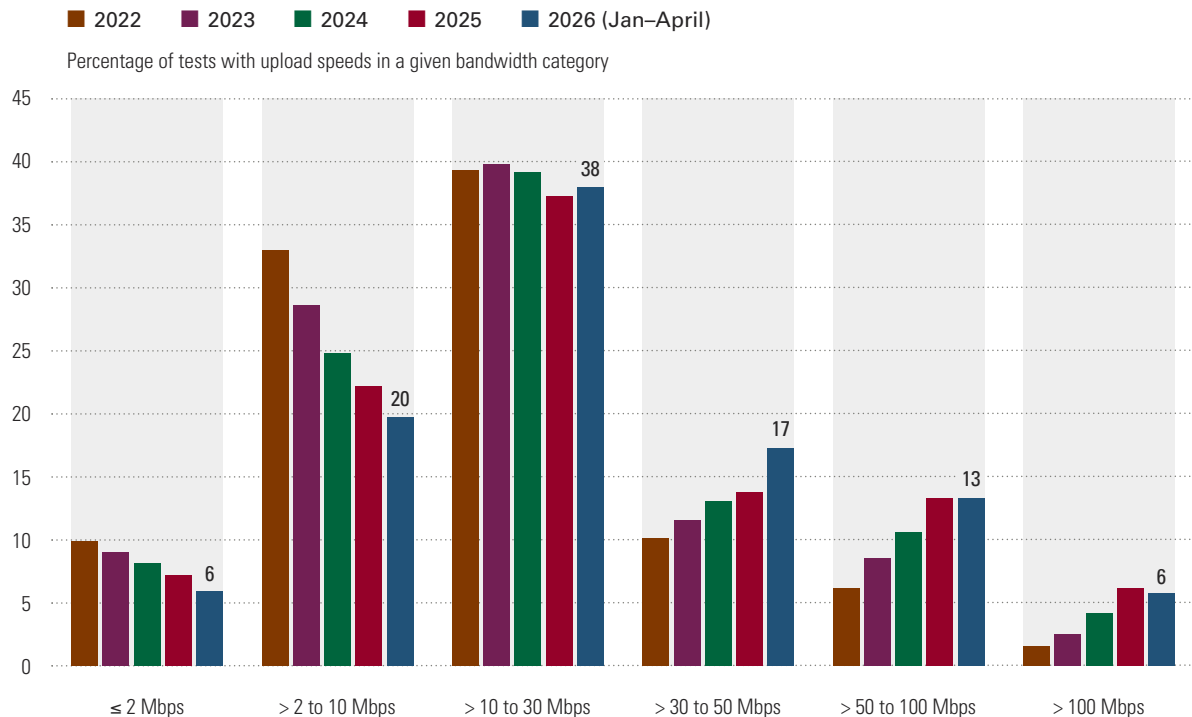
²⁰ Available as a mobile app (Android, iOS) and as a browser test.

²¹ <https://www.netztest.at/de/Opendata>

Figure 6: Distribution of download speeds by reporting period

Source: RTR-NetTest

Figure 7 shows the percentage of tests with upload speeds in a given category. Once again, the category of upload speeds between 10 and 30 Mbps is the category with the highest proportion of tests in 2025 and 2026 (January to April). Shares are shrinking for categories with measurements under 10 Mbps and over 100 Mbps in 2026 (Jan-Apr), while other categories are showing growth.

Figure 7: Distribution of upload speeds by reporting period

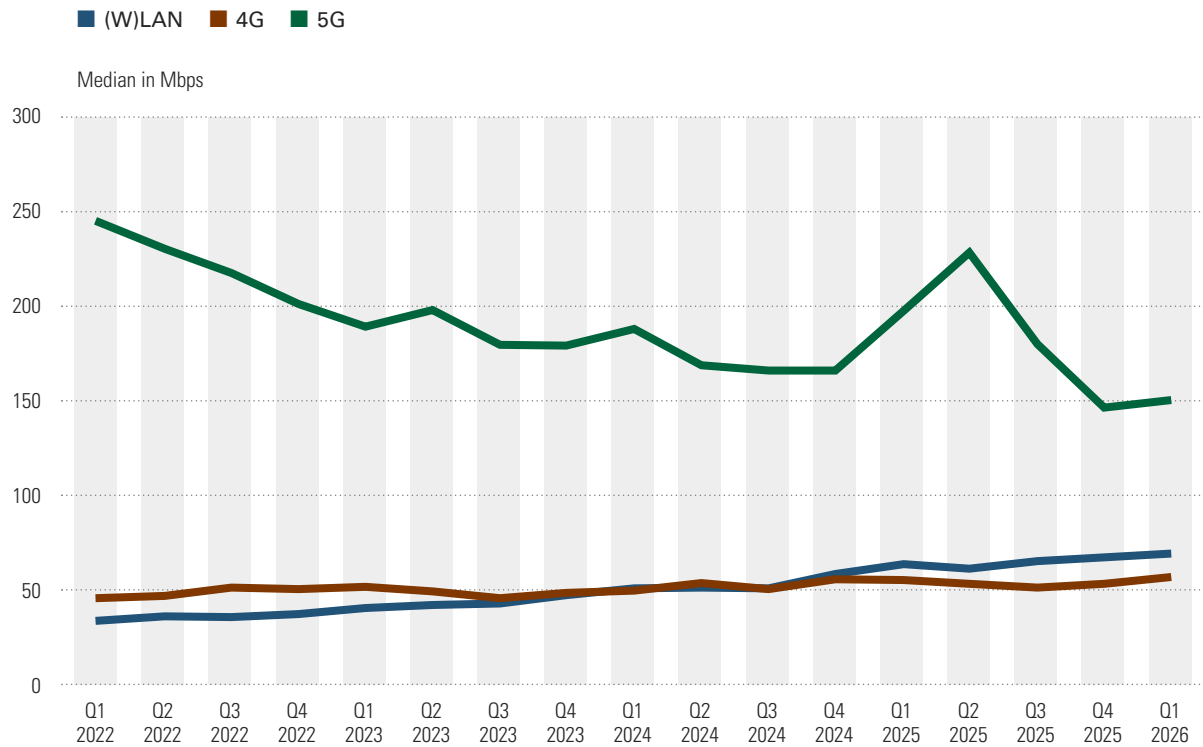
Source: RTR-NetTest

NetTest data also include information about the various technologies being used. Figure 8 depicts the median download speeds measured with the RTR-NetTest over time, broken down by type of technology.²² The chart distinguishes between 4G (LTE) and 5G (NR) as well as based on measurements for various fixed and network technologies. These measurements were taken with the aid of a browser or app (for Wi-Fi) and have been aggregated here under the heading of (W)LAN.²³ 5G achieves significantly higher download speeds than other technology standards. Median 5G measurements dropped from 197 Mbps in the first quarter of 2025 to 150 Mbps in the first quarter of 2026.²⁴ Meanwhile, median 4G measurements have risen from 55 Mbps to 57 Mbps. Median measurements for (wireless) LAN speed rose 9% to 69 Mbps in the first quarter of 2026 (Q1 2025: 64 Mbps).

²² The median is the value at the exact midpoint of a list sorted according to magnitude.

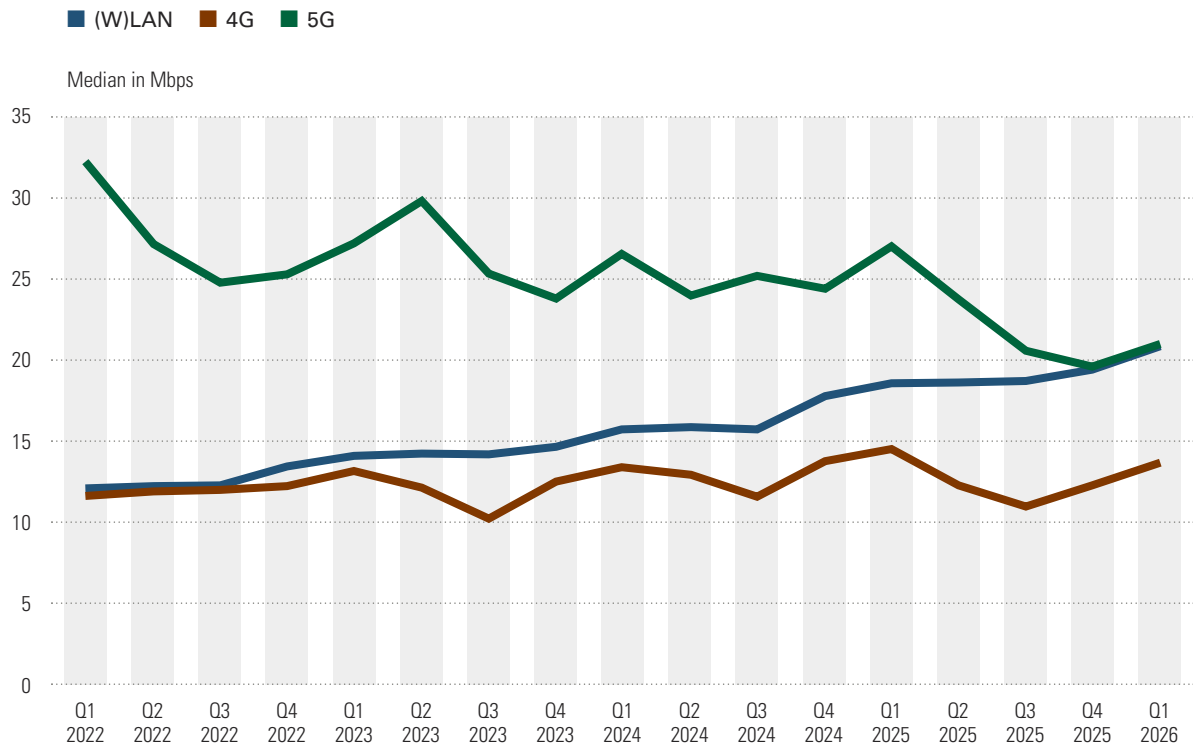
²³ No measurements were taken for 3G technology (UMTS, HSPA) in the first quarter of 2026. Such measurements showed only single-digit values in previous quarters. Accordingly, the charts do not show 3G measurements separately.

²⁴ With the introduction of a new mobile telecommunications technology, the capacities available at any given time generally follow a cycle that can be observed. When a new technology is introduced, there are initially free capacities available, which are then gradually utilised as a result of market competition and demand, until the next technology (often accompanied by new spectrum) in turn creates new capacities.

Figure 8: Download speed by technology

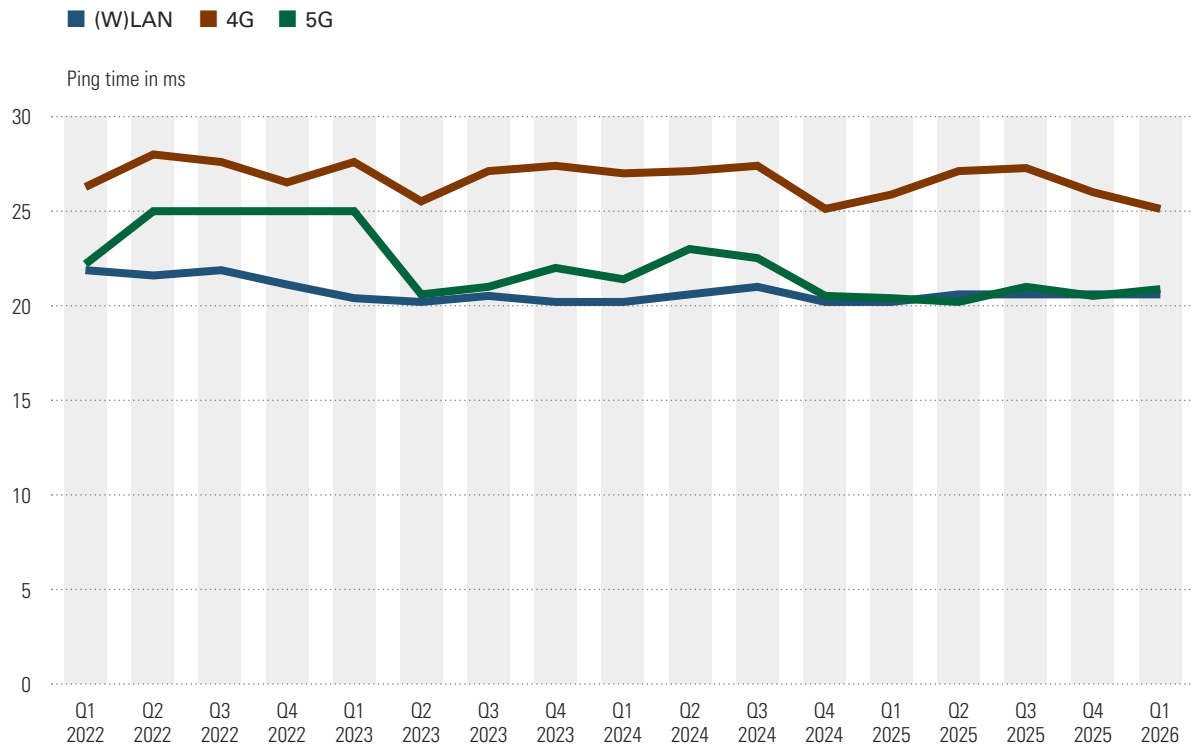
Source: RTR-NetTest

Figure 9 shows median upload speeds by technology. A pattern similar to download speeds can be observed. For both 5G and (wireless) LAN, the median upload speed was 21 Mbps in the first quarter of 2026. The median of measurements higher than 4G slid back slightly from 15 Mbps in the first quarter of 2025 to 14 Mbps in the first quarter of 2026.

Figure 9: Upload speed by technology

Source: RTR-NetTest

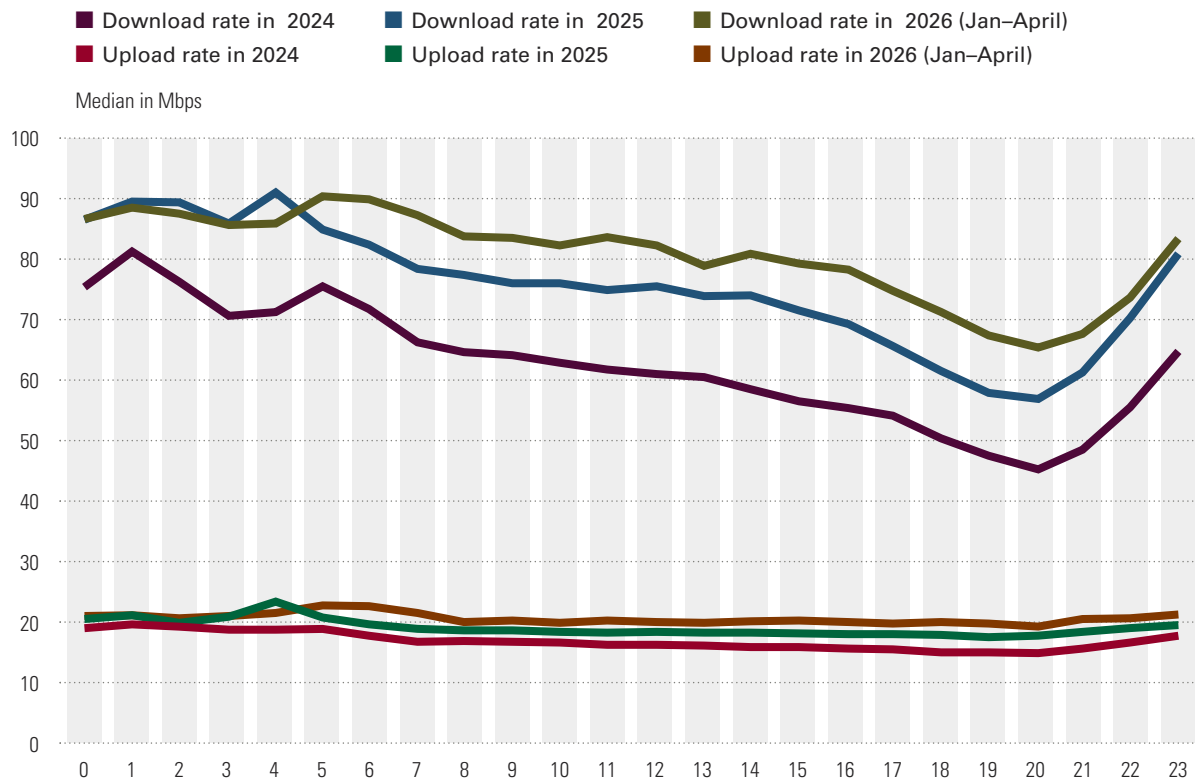
'Ping time' (more correctly termed 'latency') is the time a small data packet needs to make its way from a user device to an online server and back. Figure 10 shows median values for latency measurements. This figure was 25 ms for 4G measurements in the first quarter of 2026. A low median value of 21 ms was recorded for both 5G and (wireless) LAN. Compared with the first quarter of 2025 and 2026, latency figures for all technologies stayed much the same.

Figure 10: Latency (ping) by technology

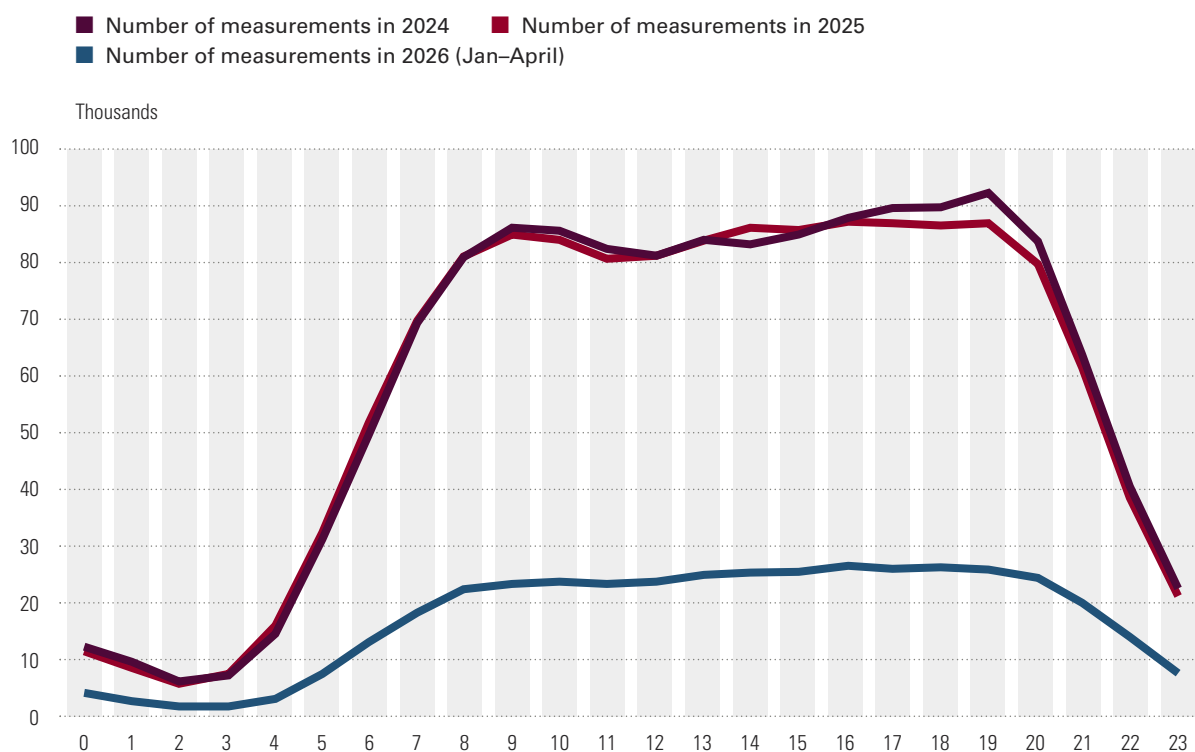
Source: RTR-NetTest

Figure 11 shows the median download and upload speeds by time of day in 2024, 2025 and 2026 (January to April). Median download speed figures are lower between 6 p.m. and 10 p.m. (peak time) than at other times of the day. The upload speed is barely affected during this period. During the night (between 12 a.m. and 6 a.m.), data traffic is very low: as a result, network loads are lighter, typically resulting in higher download speeds than at other times of the day. Comparatively few measurements are carried out in this timeframe. Individual measurements therefore have more weight and can result in fluctuations in the speeds measured. In 2026 (January to April), the median download speed measured during these hours was 88 Mbps. After 6 a.m., the median download speed measured declined continuously until it reached the figure of 65 Mbps during the peak hour, which is between 8 p.m. and 9 p.m. Outside nighttime hours (when fewer measurements are made), both the download speed and the upload speed are higher in 2026 (Jan–Apr) than in 2025.

The number of measurements differs widely from hour to hour during the day. In 2025, most measurements (roughly 87,000) were made in the hour between 4 p.m. and 5 p.m.

Figure 11: Download and upload speeds by time of day

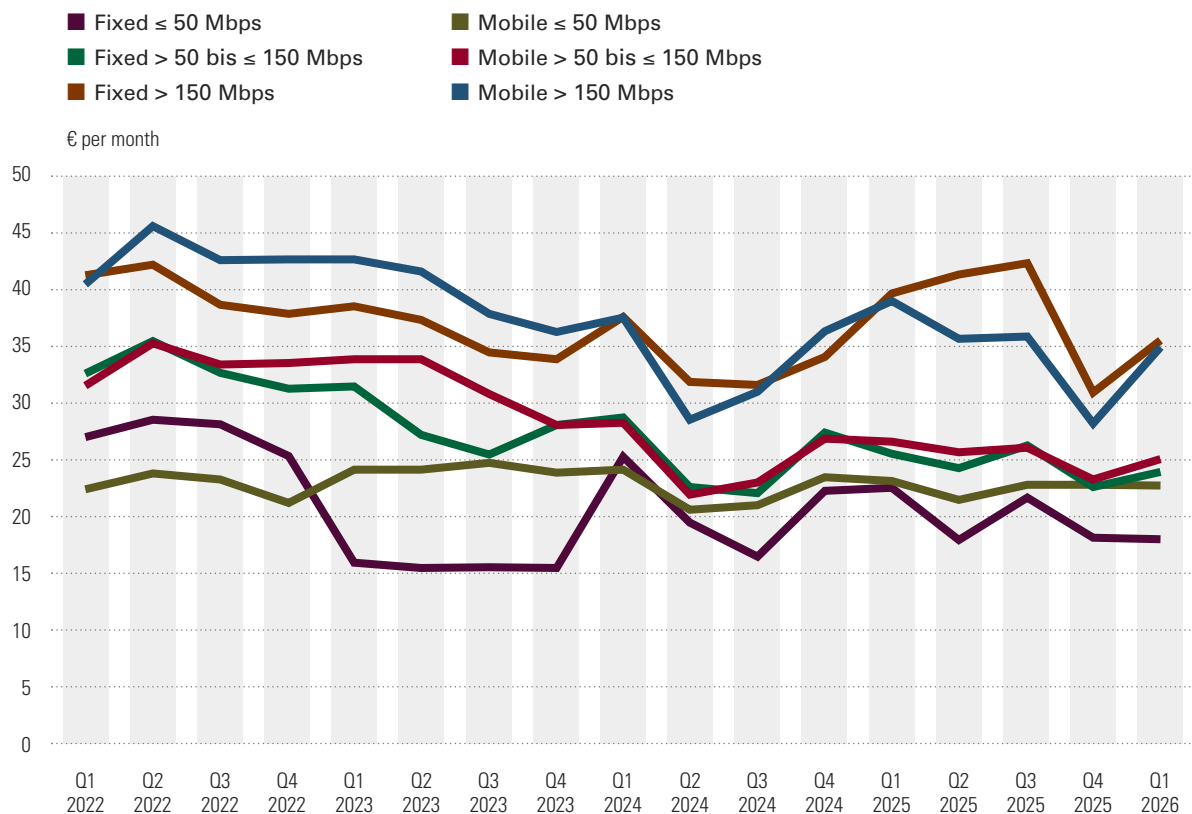
Source: RTR

Figure 12: Number of measurements by hour of day

Source: RTR-NetTest

Figure 13, finally, presents three price baskets for fixed network broadband and three price baskets for mobile broadband. The chart contrasts the three price baskets for fixed broadband (each without TV; the figures include products both with and without voice telephony) with the three price baskets for mobile broadband (with unlimited data volume). Each basket price consists of the least expensive product (excluding youth tariffs) from each operator, weighted by the respective operator's market share. Compared with the first quarter of 2025, all price baskets—for both mobile and fixed broadband—fell in the first quarter of 2026. Mobile broadband ≤50 Mbps fell by the smallest amount (2%), while the price basket for fixed broadband ≤50 Mbps fell by the largest amount (20%), declining from EUR 23 to EUR 18.

Figure 13: Price baskets: fixed vs. mobile broadband



Source: RTR

End users can also use the RTR-NetTest to independently measure other quality metrics related to their internet access. The results for quality of service (QoS) tests are shown immediately after running the test, including: 'Voice over IP', 'Unmodified content', 'Website', 'Transparent connectivity', 'DNS', 'TCP ports', 'UDP ports'. In this way, consumers can evaluate the quality of their internet access while also identifying any potential restrictions affecting use.

Conclusions

The key figures as presented here can be understood as revealing a basically positive development in the availability of non-discriminatory internet access services during the reporting period. In view of the indicators above, it can be concluded that the availability of non-discriminatory internet access services at levels of quality that reflect advances in technology (requirement in Art. 5(1) TSM Regulation) was ensured in Austria over the past five years.

08

Outlook on further
activities

08 Outlook on further activities

In our future work, we at the Austrian regulatory authority will continue on the previous path. This means a commitment to proactively monitoring developments in the markets while also being available as a partner to ISPs, internet users and all other stakeholders to consult on net neutrality issues. Within our organisation, we have also met requirements to fulfil this commitment. Specifically, the activities described below are currently planned for 2026/2027 or by the end of the next reporting period in April 2027.

I. Monitoring

- 1. Requests for information.** As in previous years, the verification of internet access products by additional request-for-information procedures is also planned for the next reporting year.
- 2. Customer complaints as a source of information.** Customer complaints are viewed as a further source of information for ongoing monitoring of compliance with the provisions of the TSM Regulation. Any irregularities are to be followed up on accordingly.
- 3. Ongoing review of general terms of business.** The regulatory authority's work of reviewing general terms of business also involves monitoring compliance with net neutrality rules. The use of these terms is prohibited if they are found to breach the provisions of Art. 4(1) of the TSM Regulation. Where products touch on net neutrality issues (such as the provision of specialised services) to a significant extent, the regulatory authority sets up monitoring teams as appropriate.
- 4. Data from market observation and RTR-NetTest.** The regulatory authority periodically collects data (via the KEV, ZIB and ZIS) on aspects such as developments in telecommunications and internet access markets, the technologies implemented, infrastructure, and trends in demand and prices. These data are made available, together with related analyses (including hedonic prices, the mobile price index and geographical comparisons) as Open Data or in the form of quarterly reports (Internet Monitor, Telekom Monitor). Another important system that is used to provide information about the structure and development of the internet is RTR-NetTest.²⁵ This crowd-sourced tool provides a wealth of increasingly reliable information on technologies and QoS indicators such as upload and download speeds, ping times and signal strength. RTR-NetTest is being further enhanced on an ongoing basis.
- 5. Certified monitoring mechanism.** A long-standing RTR measurement tool, RTR-NetTest was first deployed in conciliation procedures and court proceedings in November 2018, in order to furnish evidence for an ISP's compliance or lack of compliance with a contractually agreed service level. This type of review is considered a certified monitoring mechanism within the meaning of Art. 4(4) of the TSM Regulation.
- 6. Internet blocking.** Network blocks are a topic of increasing significance. The TKK's remit here has been further expanded by the Consumer Protection Cooperation Act (VBKG) in 2021 as well as responsibilities relating to the EU Market Surveillance Regulation in 2022. The regulatory authority expects to see network blocks receiving heightened attention because of the resulting need to weigh up one fundamental right against another, a factor also potentially impacting business models.

²⁵ See <https://www.netztest.at/en/>

7. Empirical collections and analyses of platforms and digital gatekeepers. While the Net Neutrality Regulation addresses questions of unhindered access to the open internet, the internet also faces risks beyond basic access that affect its status as a key driver of technical and social innovation. The RTR has prepared a series of analyses addressing these risks and is also working with other institutions such as the Federal Competition Authority (BWB) as part of the digital platforms task force. BEREC is also one of six European networks and bodies that make up the High-Level Group for the Digital Markets Act (DMA). This group advises and supports the European Commission in efforts to enforce the Digital Markets Act (DMA), and therefore ensure competitiveness and fairness in digital markets. Klaus M. Steinmaurer, Managing Director of the RTR's Telecommunications and Postal Services Division, is currently one of six BEREC delegates participating in the High-Level Group.

II. International cooperation

- 1. Net neutrality provisions.** To drive harmonised implementation of net neutrality provisions, international exchange among regulatory authorities (within the framework of BEREC but also bilaterally) will continue in the form of ongoing procedures as well as the joint discussion and analysis of relevant products. In this context, the RTR Telecommunications and Postal Services Division also makes every effort to ensure the confidential handling of issues raised by domestic ISPs (e.g. relating to individual products) and the rapid clarification of ambiguities in the interpretation of net neutrality provisions at international level.
- 2. Internet measurement tool and net neutrality.** For 2026, the BEREC Work Programme envisages the continuation of activities involving the application of tools to measure quality and net neutrality in relation to internet access services and their use in a regulatory context. RTR, which has had a tool of this kind available for a long time now in the form of RTR-NetTest, is closely involved in these activities, as well as in the auditing and updating of methods for the measurement of quality parameters in VHC networks.
- 3. BEREC annual report on net neutrality in Europe.** A BEREC report on implementing the TSM Regulation will be compiled and published towards the end of 2026. The report will be based on the net neutrality reports to be published by the NRAs by 30 June 2026.
- 4. Digital gatekeepers and the internet ecosystem.** The RTR's Telecommunications and Postal Services Division also contributes to studies of the internet ecosystem. Investigations here focus on topics such as openness and competition. The consultation launched by the European Commission to evaluate the Digital Markets Act (DMA) was a key work area in the reporting period. Among other things, this evaluation aims to establish whether the goals of the DMA—namely to guarantee fair and contestable markets—have been achieved or whether the requirements imposed need to be modified. BEREC duly participated in the consultation, with our specialist division contributing actively to the process. The division also assessed the implementation of interoperability obligations for certain number-independent interpersonal communications services by gatekeepers pursuant to the DMA; this work will continue in the next reporting period.
- 5. International work supports knowledge transfer.** Work at international level not only creates a space for dialogue and discussion of the issues at hand. It also offers an opportunity to follow the work of other regulatory authorities on the topic of net neutrality, while reviewing relevance for Austria and adopting suitable approaches where appropriate. Topics currently of particular importance internationally include network slicing, quality differentiation, specialised services and the approaches taken by regulatory authorities in the case of network blocks.

III. Cooperation with ISPs and the general public

1. **Cooperation is key.** The RTR Telecommunications and Postal Services Division will continue to pursue and further expand the strategy mentioned above in this section. We are committed to identifying solutions by promptly and constructively discussing any new issues, within the framework of an open dialogue with the sector or individual companies. This is the key component of all regulatory activities relating to net neutrality. In many cases, any specific proposed activity must first be understood in detail before any recommendations can be made or any conclusions can be drawn that might relate to potential regulation.
2. As was the case this year, due attention will also be paid to **expanding the net neutrality website** in the next reporting year. Alongside other activities, RTR not only maintains a list of all decisions made by the national regulatory authority and the courts, but also a list of all active network blocks in Austria. This service is offered in the form of Open Data to internet users and providers.
3. Finally, an **event** will also be organised to address **current net neutrality issues**. Further details of an event of this kind—planned for early 2027—will be offered for comment as part of the budget consultation to be published later this year.

09 Appendix

9.1 Mapping

Here, as described above in the introduction, interested readers are furnished with details on how this report maps to the BEREC Guidelines. This is important first and foremost to allow international comparisons of the report. Par. 183 of the BEREC Guidelines describes which sections should be included in national reports on net neutrality. In the following table these points are mapped to the individual chapters of the report.

Table 5: Sections of this report as mapped to the BEREC Guidelines

Text of the BEREC Guidelines (Par. 183)	Section
“overall description of the national situation regarding compliance with the Regulation”	→ Section 1
	→ Section 2
“description of the monitoring activities carried out by the NRA”	→ Section 5
	→ Section 6
“the number and types of complaints and infringements related to the Regulation”	→ Section 6
“main results of surveys conducted in relation to supervising and enforcing the Regulation”	→ Section 3
	→ Section 6
“main results and values retrieved from technical measurements and evaluations conducted in relation to supervising and enforcing the Regulation”	→ Section 6
	→ Section 7
“an assessment of the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology”	→ Section 7
“measures adopted/applied by NRAs pursuant to Article 5(1)”	→ Section 6.5

9.2 Index of Figures and Tables

Figures	Page
Figure 1: Timeline of events in the reporting period	11
Figure 2: Schematic diagram of quality of service indicators for two slices	15
Figure 3: Using a VPN to access a service	22
Figure 4: Various networks involved in accessing a website	23
Figure 5: Fixed and mobile broadband connections	44
Figure 6: Distribution of download speeds by reporting period	45
Figure 7: Distribution of upload speeds by reporting period	46
Figure 8: Download speed by technology	47
Figure 9: Upload speed by technology	48
Figure 10: Latency (ping) by technology	49
Figure 11: Download and upload speeds by time of day	50
Figure 12: Number of measurements by hour of day	50
Figure 13: Price baskets: fixed vs. mobile broadband	51

Tables	Page
Table 1: Timeline of events in the reporting period	12
Table 2: Summary of potentially problematic practices in relation to the TSM Regulation	26
Table 3: Procedures pursuant to Art. 5(1) TSM Regulation since 2016	32
Table 4: Overview of conciliation procedures relating to quality complaints	40
Table 5: Sections of this report as mapped to the BEREC Guidelines	58

9.3 Abbreviations

AGB	AGB: general terms and conditions
BEREC	Body of European Regulators for Electronic Communications
BEV	Austrian Federal Office of Metrology and Surveying
BOOTPS	bootstrap protocol, serves to assign an IP address and other parameters to a computer in a TCP/IP network
BVwG	Federal Administrative Court
CAP	content and application provider
CPE	customer premises equipment (user device)
CreativePartnr	service via port 455/TCP
DHCP	dynamic host configuration protocol. This protocol allows a server to assign the network configuration to clients.
DNS	domain name system
EC	European Commission
ECJ	European Court of Justice
FMA	Financial Markets Authority
HTTPS	hypertext transfer protocol secure; communications protocol on the world wide web that allows data to be transferred securely
IAS	internet access service
IP	internet protocol
IPv4	internet protocol version 4
IPv6	internet protocol version 6
ISP	internet service provider
KEV	Communications Survey Ordinance (<i>Kommunikations-Erhebungs-Verordnung</i>)
KommAustria	Austrian Communications Authority
MiCA	EU Markets in Crypto-Assets Regulation
MNO	mobile network operator
MVNO	mobile virtual network operator
NAT	network address translation
NetBIOS	network basic input output system; an application programming interface (API) for communication between two programs via a local network
NN	net neutrality
NRA	national regulatory authority
RTR	Austrian Regulatory Authority for Broadcasting and Telecommunications (Rundfunk und Telekom Regulierungs-GmbH)
SMB	server message block; also known as common internet file system (CIFS), is a network protocol for file, printing and other server services in computer networks

SMTP	simple mail transfer protocol
SNI	see TLS-SNI
TCP	Transmission Control Protocol
TFTP	trivial file transfer protocol; very simple (and early) file transfer protocol
TKG	Telecommunications Act (<i>Telekommunikationsgesetz</i>)
TKK	Telekom-Control-Kommission
TLS-SNI	Transport Layer Security–Server Name Indication; an extension of the transport layer security protocol that allows multiple encrypted, retrievable websites with different domains to share one server on TLS port 443, even if it has only one IP address
TSM Regulation	Telecoms Single Market Regulation; Regulation (EU) 2015/2120 laying down measures concerning open internet access
UDP	user datagram protocol; a minimal, connectionless network protocol that is part of the transport layer of the internet protocol family
UrhG	Federal Act on Copyright in Literary and Artistic Works and Related Rights (<i>Urheberrechtsgesetz</i>)
VoD	video on demand
WAN	wide area network
WWW	world wide web

Publishing information

Owner and publisher

Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)
Mariahilfer Straße 77–79
1060 Vienna, Austria
Phone: +43 1 58058-0 | Mail: rtr@rtr.at
www.rtr.at

Responsible for content

Klaus M. Steinmaurer, Managing Director for Telecommunications and Postal Services
Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)

Design, text and figures

Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)

Implementation and layout

Johannes Bulgarini Advertising Agency
Gföhl 8, 3053 Laaben, Austria

Translation

Dr. Robert Schlarb eU
Buchdrucker Straße 5
8704 Dürwagersbach, Austria

All parts of this publication are protected by copyright. All rights reserved under copyright, in particular rights to distribution, reprinting, translations, presentations, the use of illustrations and tables, broadcasting, microfilms or reproduction of this document in photocopies or any other form, as well as storage in computer systems, even in cases where excerpts are used.

All data in the RTR 2026 Net Neutrality Report were reviewed with the utmost care. Nonetheless, errors cannot be ruled out. No guarantee of accuracy can consequently be extended for the content.

Copyright Rundfunk und Telekom Regulierungs-GmbH 2026

