RTR

RTR NET NEUTRALITY REPORT

2024

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

www.rtr.at

2024

RTR NET NEUTRALITY REPORT

2024

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

June 2024

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

Contents

01

Preface

and executive summary

01 Preface and executive summary

Dear Reader,

The RTR Net Neutrality Report before you is the eighth such report on the openness of the internet in Austria. The report is intended to give the interested public a complete overview of our activities during the past twelve months, as well as to describe in general any changes in net neutrality and the current status in Austria.

Much the same as in previous years, the past year was marked by intensive debates related to the subject of net neutrality. One example of this is 'zero-rating', where we were able to finally resolve the apposite issues and identify a solution acceptable to all market players. Meanwhile, net neutrality continues to be subject to trends that change over time. This can currently be seen in the issues emerging as a result of implementing net neutrality models under 5G. One of these new issues is how to distribute resources across virtual network elements (network slicing), and how to classify these elements within the scope of the TSM Regulation. Another consistently weighty issue revolves around net blocking in conformity with various legal requirements.

During the reporting period, we at RTR specifically tackled the subject of free choice of user device and network termination points. The disputed issues could be largely resolved to the satisfaction of at least the majority of affected market participants.

Most recently, the controversial issue of whether content providers should provide a financial contribution, i.e. assume a 'fair share' of costs, for their 'use' of ISP networks, was again debated by the European Commission as well as major European players. While certainly nothing new, the question may need to be re-examined in the light of current ongoing discussions in the EU. It will be interesting to see which course the new Commission pursues.

On the whole, it is safe to say that, as more and more areas of day-to-day life shift to the internet, people in general are becoming increasingly aware of the importance of free access to and the openness of networks, and thus net neutrality.

Beyond our responsibility for enforcing the TSM Regulation domestically, net neutrality is a highly international issue. This is why our experts at RTR participate very actively in international efforts, specifically in the activities organised by the Body of European Regulators for Electronic Communications (BEREC) towards ensuring an open internet. The focus of our work at international level is the issue of 'fair share' and the recent ensuing evaluation of IP interconnection markets. Interconnection of networks within the internet is an important prerequisite for the provision of broadband access and the rendering of digital services. As early as 2012 and 2017, BEREC was already highlighting relevant technical and economic developments as well as legal frameworks in relation to IP interconnection. In June 2024, BEREC published a draft update to the 2017 report. During the reporting period, BEREC developed a questionnaire for collecting empirical data on IP interconnection markets, including data traffic and prices for IP interconnection with individual partners and content providers. This questionnaire was sent to internet access providers in Europe in summer 2023. In autumn 2023, workshops were also held with a number of stakeholders with the aim of gaining further insights. The draft report finds that developments in the IP interconnection

markets can continue to be described more as an evolution than a revolution. Although data traffic is rising, competition and technical progress are nonetheless making it possible to successfully respond to changes in the usage of internet connections as well as to changing demand for content in the IP interconnection ecosystem. That ecosystem continues to be characteristically competitive, even though isolated conflicts between market players have been observed since 2017. In future, BEREC will monitor conflicts in this context – including any relating to net neutrality and the TSM Regulation. On completion of the draft report consultation, the statements submitted will be processed and the final report on the IP interconnection ecosystem published at the end of 2024.

Another topic taking up a wide berth in the current Net Neutrality Report is net blocking by access providers. This means that internet service providers are often called on to take responsibility for enforcing legal requirements in an online context. The current legislative framework faces national regulatory authorities, providers and internet users with a dilemma, raising the question of how to harmonise the goals of preserving legal certainty, legal protection and fundamental rights. Numerous procedures in the reporting period concerned blocking measures taken to protect copyright. The regulatory authority Telekom-Control-Kommission (TKK) handed down a pivotal ruling in August 2023. Internet blocking based on the domain name system (DNS) is now deemed appropriate and sufficient for protecting the rights of third parties. Blocking based on IP addresses that goes beyond DNS blocks is not necessary in principle and hence inappropriate. As a result, net neutrality continues to be ensured for the future while any blocking measures are limited to those absolutely required. We can thus expect net blocking to remain a central issue for some time to come.

Once again this year, RTR's evaluations show a positive trend in the availability of internet access services for the period under review. It is especially worth pointing out how both download and upload traffic rates have continued to accelerate. The continued availability of internet access services at a level of quality that duly reflects advances in technology, as is required under the Net Neutrality Regulation, has once again been consistently ensured in this reporting period.

Aside from those highlights from the reporting period that are presented here, we should not overlook the work of our experts at RTR: day after day, and with renewed effort, these individuals provide valuable help towards ensuring net neutrality at both national and international planes, thus helping to guarantee continued free access to an open internet both in Austria and throughout the EU.

With an eye to the future, I wish in closing to confirm our unbroken commitment at RTR to reliable involvement in efforts towards ensuring the openness of the internet, in Austria and at international level. As a free and open space for all, the internet is of inestimable value for our democracy and society. All of us are called upon to take responsibility for ensuring that this continues to be the case in the future.

With this in mind, as you read through this report, I invite you to get involved in the conversation about the open internet and net neutrality, and to continue this conversation into the future. It is about freedom – yours and ours.

Vienna,
June 2024

Klaus M. Steinmaurer

Managing Director
Telecommunications and Postal Services Division
RTR

02

Introduction:
stakeholders and institutions in enforcement

02 Introduction: stakeholders and institutions in enforcement

This eighth Annual Report on Net Neutrality by the Telecommunications and Postal Services Division of the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) addresses the same major topics as covered in last year's report. In this way, we wish 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 2023 to 30 April 2024, 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.

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 areas of day-to-day life 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.

Section 3 presents the reader with a chronological overview of the activities of the national regulatory authority, while section 4 focuses on current developments as well as work in relation to net neutrality and IP interconnection (also as a result of the recently revived 'fair share' debate). Section 5 presents the regulatory authority's activities and responsibilities in relation to network internet blocks and also discusses some key decisions on IP blocks. Section 6 presents an overview of the legal obligations to set internet blocks as contained within the EU's proposal for a regulation on rules to prevent and combat child sexual abuse. Section 7 is dedicated to the checks carried out by the regulatory authority on the disconnection of IP connections as made by providers of internet access services. In the reporting period, the regulatory authority also looked at the topics of the free choice of user device and the location of the network termination point; results are presented in section 8. Section 9 summarises the regulatory measures used to protect net neutrality as well as related procedures. Section 10 provides an overview of key figures on the development of internet access services in Austria. Finally, section 11 presents a brief summary of the projects and events planned for the next reporting year.

03

Timeline

of regulatory authority activities

03 Timeline of regulatory authority activities

Figure 1: Timeline of events in the reporting period

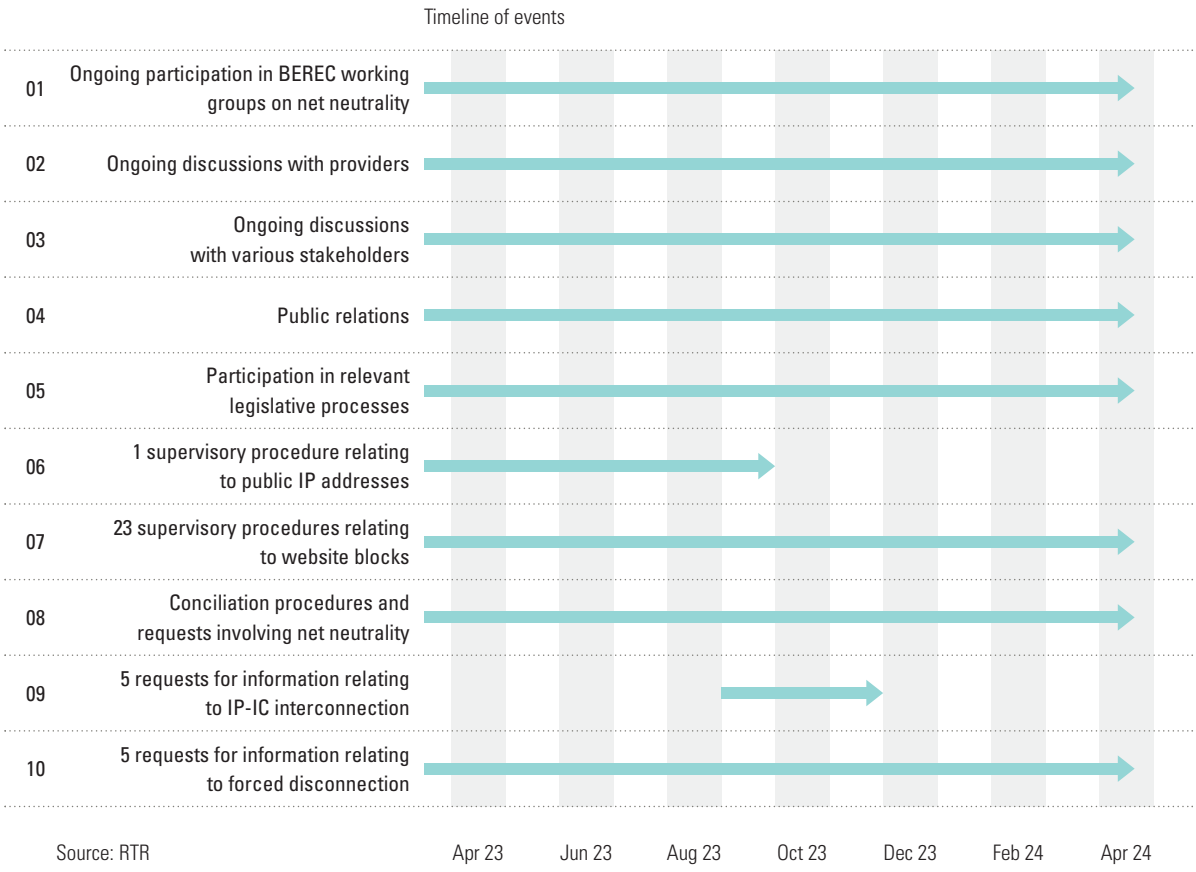


Figure 1 presents in chronological sequence the relevant events during the reporting period (May 2023 – April 2024). The table below gives an overview of these events, with a brief description in each case and giving the time period involved. Further details about these procedures can be found in sections 7 and 9.

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 2023:** Implementation of the Open Internet Regulation and the BEREC Open Internet Guidelines, Collaboration on Internet access service measurement tools, BEREC Report on the IP Interconnection ecosystem (carry-over), BEREC Guidelines detailing Quality of Service (QoS) parameters, Charging for interconnection/fair share, BEREC input to the exploratory consultation on the future of the connectivity sector and its infrastructure **Topics in 2024:** BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services (carry-over), BEREC Report on the Member States' best practices to support the defining of adequate broadband Internet Access Service (IAS) (carry-over), BEREC Guidelines detailing Quality of Service (QoS) parameters (carry-over), Implementation of the Open Internet Regulation and the BEREC Open Internet Guidelines, BEREC Report on the IP interconnection ecosystem (carry-over), Collaboration on Internet access service measurement tools
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	August 2022 – August 2023	The TKK concluded twelve supervisory procedures with a decision. These procedures concerned DNS access blocks, which in these cases had been set in accordance with the law. While the IP access blocks addressed by some of these procedures constituted a breach of Art. 3 Par. 3 TSM Regulation, these blocks were no longer active at the time of the decision. Breaches were merely identified as lying in the past and the procedures were terminated for lack of a breach at the time of the decision.
07	August 2022 – October 2023	The TKK issued eight decisions that, among other matters, ruled that the DNS access blocks set did not constitute a breach of Art. 3 Par. 3 TSM Regulation whereas the IP blocks set for certain websites did indeed constitute a breach of this same provision. Appeals have been lodged against these decisions and a ruling from the Federal Administrative Court (BVwG) is pending.
08	April 2024 – (ongoing)	Three supervisory procedures pursuant to Art. 5 TSM Regulation were initiated against specified ISPs in order to audit access blocks set for certain websites due to injunction claims based on copyright. These procedures were still pending by the end of the reporting period.
09	March 2023 – September 2023	One supervisory procedure was initiated against an ISP as a result of their failure to assign (at least) a dynamic public IPv4 address to end users. The provider remedied this breach during the procedure. The procedure was terminated for lack of a breach of Art. 3 Par. 1 TSM Regulation at the time of the decision.

Enforcement of TSM Regulation		
10	August 2023 – November 2023	A total of five requests for information made to various ISPs in conjunction with IP-IC interconnections and therefore related to a reevaluation of developments in the IP interconnection markets.
11	February 2023 – November 2023	Initiation of 17 procedures against various ISPs regarding website blocks relating to Regulation (EU) 833/2014 as amended by Regulation (EU) 2022/350, Regulation (EU) 2022/879, Regulation (EU) 2022/2474, Regulation (EU) 2023/427 and Regulation (EU) 2023/1214 (EU packages of sanctions against Russia). These blocks were lawfully set and therefore not in breach of the TSM Regulation.
12	February 2023 – February 2024	RTR initiated three procedures against various ISPs pursuant to Art. 5 Par. 2 TSM Regulation, to ascertain whether forced disconnections of IP connections had been made and whether the end user had been provided with a dynamic public IP address as requested. No breach was identified in the course of the procedure.
13	February 2023 – May 2024	RTR initiated procedures against two ISPs to ascertain whether forced disconnections of IP connections had been made and whether the end user had been provided with a dynamic public IP address as requested. Owing to the circumstance of a suspected breach of Art. 3 TSM Regulation, the TKK requested that the providers take steps to remedy the presumed breach. During the reporting period, legal compliance was duly restored in both cases.
14	Ongoing	Conciliation procedures and enquiries relating to net neutrality (for further details, see section 9.7).

04

Net neutrality
and IP interconnection

04 Net neutrality and IP interconnection

The interconnection of networks within the internet is an important prerequisite for the provision of broadband access and the rendering of digital services. Such interconnection enables data exchange between networks based on the internet protocol (IP). In a more general sense, the topic of IP interconnection encompasses various services and infrastructures for data exchange within the internet (e.g. via peering, transit or internet exchange points). One point of contact with the IP interconnection markets, which are not directly regulated per se by the TSM Regulation, is identified by the BEREC guidelines on the Regulation. Paragraph 6 does indeed consider practices in these markets as being governed by the TSM Regulation where affecting the rights guaranteed under the Regulation.

As early as 2012 and 2017, BEREC was already highlighting relevant technical and economic developments as well as legal frameworks in relation to IP interconnection.[1] Significant findings from 2017 were that the IP interconnection markets and the internet ecosystem had been adjusting to new conditions (e.g. higher data volumes or changing business models), while driving both technical progress and competition at lower prices. In cases where conflicts had arisen between market participants, these were generally resolved without regulatory intervention.

In June 2024, BEREC published a draft update to the 2017 report, which is currently in public consultation.[2] During the reporting period, BEREC developed a questionnaire for collecting empirical data on IP interconnection markets (e.g. data traffic and prices for IP interconnection with individual partners and content providers). This questionnaire was sent to internet access providers in Europe in summer 2023. In autumn 2023, workshops were also held with a number of stakeholders with the aim of gaining further insights. The draft report finds that developments in the IP interconnection markets can continue to be described more as an evolution than a revolution. Although data traffic is rising, competition and technical progress are nonetheless enabling the successful integration of changes in the usage of the internet connection and in the demand for content in the IP interconnection ecosystem. That ecosystem continues to be characteristically competitive, even if isolated conflicts between market players have been observed since 2017. In the future, BEREC will track conflicts in this context – including in the context of net neutrality and the TSM Regulation. On completion of the draft report consultation, the statements submitted will be processed and the final report on the IP interconnection ecosystem published at the end of 2024.

In the 2023/2024 reporting period, BEREC also responded to an explorative consultation from the European Commission on the future of the electronic communications sector and its infrastructure.[3] In this consultation, the European Commission addressed the call by major ISPs to introduce obligatory fees ('fair share'). In this view, content providers should pay fees to ISPs in line with the 'sending party network pays' (SPNP) principle.

1 An assessment of IP interconnection in the context of Net Neutrality, BoR (12) 130, https://www.berec.europa.eu/en/document-categories/berec/reports/an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality

BEREC Report on IP-Interconnection practices in the Context of Net Neutrality, BoR (17) 184, https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-ip-interconnection-practices-in-the-context-of-net-neutrality

2 Draft BEREC Report on the IP Interconnection ecosystem, BoR (24) 93, https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-ip-interconnection-ecosystem

3 BEREC input to the EC's exploratory consultation on the future of the electronics communications sector and its infrastructure, BoR (23) 131, https://www.berec.europa.eu/en/document-categories/berec/others/berec-input-to-the-ecs-exploratory-consultation-on-the-future-of-the-electronics-communications-sector-and-its-infrastructure

In March 2023, the RTR's Telecommunications and Postal Services Division conducted a workshop to gather input from various stakeholders. The regulatory authority included the information obtained in a reply to the above-mentioned consultation, published by BEREC on 19 May 2023.

In this statement, BEREC warned of the potentially negative effects arising from such direct payments on competition, end users, innovation and net neutrality. Not only could smaller ISPs and smaller content providers suffer from a reduction in their negotiating power, but large telecoms operators could exploit the termination monopoly (i.e. their monopoly on the provision of access to their own end users) vis-à-vis content providers. Mandatory direct payments could also result in higher-priced content (e.g. streaming subscriptions) for end users. An SPNP model could also have a chilling effect on innovation, if ISPs were then able to influence the content requested by end users. As a consequence, such direct payments could also infringe the rights and duties set out in Art. 3 Par. 1 and 2 TSM Regulation, restrict end user freedoms and threaten the role of the internet ecosystem as a driver for innovation.

The RTR Telecommunications and Postal Services Division essentially follows the line of argument published by BEREC, taking a critical view of the introduction of mandatory fees, such as has been proposed by the provider lobby. The Austrian regulatory authority also continues to play an active part in the various European working groups at BEREC relating to IP interconnection.

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. This necessitates such measures to be used sparingly.

To ensure transparency, the RTR publishes all of the currently active blocking measures on its website.[4] This list is additionally provided as open data.[5]

[4] https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/Blockings.en.html

[5] https://www.data.gv.at/katalog/en/dataset/f7e9b0f3-60ab-4f53-964a-c6c88c3f681d

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 Regulation[6] and the Market Surveillance Regulation[7].

The last reporting period again featured many procedures arising from internet blocks justified by copyright law. Specifically, a large number of supervisory procedures were initiated in the reporting period, a large proportion of which were concluded with a decision, with cease orders only needing to be served in six cases. Since the TSM Regulation went into effect, dozens of procedures addressing net blocking in relation to copyright have been conducted to date, one procedure even involving multiple websites.

At the end of August 2022, the topic of internet blocking and the related problem of 'overblocking' once again attracted media interest.[8] After receiving copyright injunctions, several ISPs acted to block certain IP addresses, including those assigned to the cloud provider Cloudflare. This led to the unavailability of many other websites not the subject of the formal warning. These blocks were removed promptly, since a spokesperson from the rights holder announced that blocking of those IP addresses specifically blocked was not included in the formal warning issued to the ISP. This example once again highlights the very real practical dangers of 'overblocking', particularly in conjunction with blocking based on IP addresses. In addition, IP blocks were also utilised, which had been requested on behalf of another rights holder. 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. For more details, see 5.6.

6 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.

7 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.

8 https://blog.cloudflare.com/de-de/consequences-of-ip-blocking-de-de/, https://www.derstandard.de/story/2000138619757/ueberzogene-netzsperre-sorgt-fuer-probleme-im-oesterreichischen-internet

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)[9] 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 TKK 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 TKK 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 new Market Surveillance Regulation[10] 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 earlier loopholes that had permitted the EU market distribution of third-country goods without EU conformity via online platforms, and without responsible economic operators being identifiable in the EU itself. This Regulation follows the CPC Regulation in extending the potential addressees of orders to take steps to prevent online infringements, going beyond economic operators to 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. Network blocks based on the EU Market Surveillance Regulation were not initiated or required during the reporting period.

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

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

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

The EU Sanctions Regulation[11] 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 TKK and RTR FB TKP, the regulatory authorities responsible for safeguarding net neutrality, no additional transposition of the EU Sanction Regulations is required through a national administrative act. 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 in the sense of Art. 3(3) subparagraph 3(a) TSM Regulation. This opinion is shared by BEREC.[12]

On 13 April 2022, supplementing the immediate applicability of the EU Sanctions Regulation, the Audiovisual Media Services Act (AMD-G)[13] 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.[14] 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 Key decisions made by the TKK on IP blocks

In the reporting period, the TKK was required to rule on numerous blocks pursuant to Art. 3(3) subparagraph 3(a) TSM Regulation. Several rights holders applied for a block on many websites structured to breach copyright law pursuant to Art. 81 Par. 1a of the Austrian Copyright Act (UrhG).

The assessment of a particular type of block proved to be especially challenging here. In this case, the providers of access internet access services 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, 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 both of these 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 via 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.

11 Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014

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

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

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

This was problematic, since the IP address itself was also being used to host other content. A theoretical point was also made that, from a technical perspective, 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, as 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. On the contrary, it is common industry practice for a domain to be assigned to multiple IP addresses and, in the opposite direction, industry-standard server software permits a virtually unlimited number of domains to be served from one single IP address.

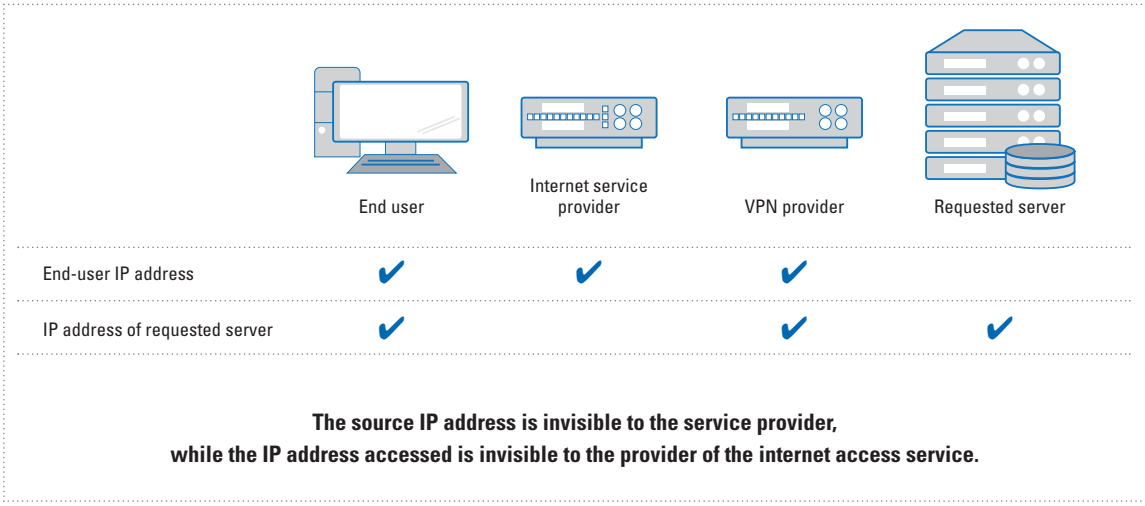
For a third party such as a technical expert, a regulatory authority or – in particular – a provider of internet access services, determining all of the IP addresses linked to a domain or all of the content accessible from a specific IP address is an impossible task. While a heuristic listing can be 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.

Turning now to look at the effectiveness of blocks, 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, for example). In such a case, the IP address of the server being accessed is no longer visible to the internet access provider (see figure 2).

This type of service (such as Apple Private Relay) can be installed and used even by people who are not IT professionals and have not acquired any technical skills by attending relevant training courses.

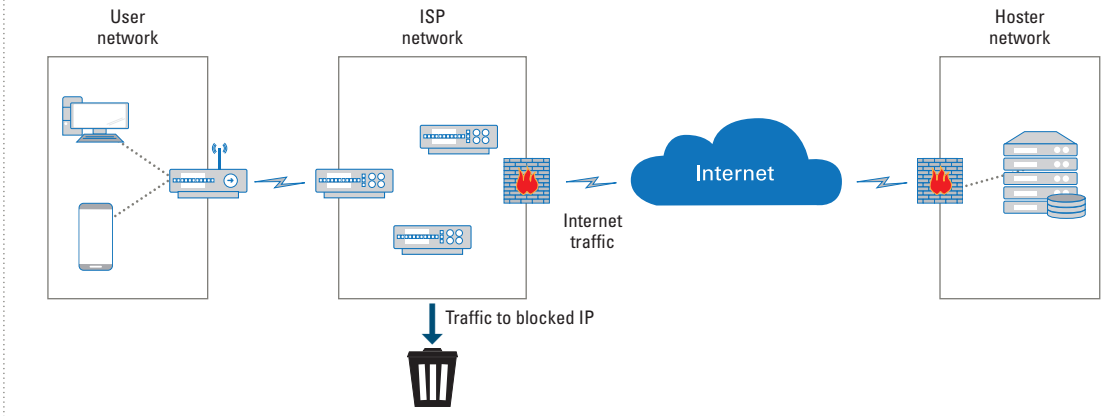
Figure 2: Using a VPN to access a service



Blocks also have only limited effectiveness against service providers. If an IP block has been applied to a service provider, then the latter can simply bypass this block by switching to another IP address. This technical change is invisible to 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 3). For end users of the provider to be blocked, this means that the IP address is no longer reachable, while the block has no effect on 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 3: Networks involved in accessing a website



An IP block is set up in the segment labelled 'ISP network', i.e. before the IP traffic is handed over to the public internet.

The implementation of IP blocks by individual providers of internet access services is also undetectable by the owners of the blocked IP address. After all, many 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, the inherent nature of 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 exhaustively investigate an 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 basic 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[15]. When

[15] See for example TKK 7 August 2023 R 16/22 p. 28 ff.

used with shared hosters 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.

On the other hand, owners of copyright claims have the interest (based on the protections to intellectual property guaranteed by Art. 17 Par. 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 TKK therefore ruled that the implementation of an IP block was a disproportionate measure that constituted a breach of Art. 3 Par. 3 TSM Regulation and therefore had to be remedied.

06

Internet blocking

proposal for a regulation on rules to prevent and combat child sexual abuse

06 Internet blocking proposal for a regulation on rules to prevent and combat child sexual abuse

In May 2022, the European Commission submitted a proposal "on rules to prevent and combat child sexual abuse" in the online environment. This proposal primarily addresses the situation where providers of communications and hosting services, including number-independent interpersonal communications services (messaging apps like WhatsApp or Signal, for example), must respond to official orders to scan the private content of their users for suspected child sexual abuse material (CSAM). This is why the proposal has often been referred to in the media as 'chat control'. Yet the proposal also envisages internet blocks being set up by providers of internet access services.

To date, EU Member States have been unable to agree a joint position on this controversial proposal for a regulation. The voluntary system of chat control has therefore been extended by the EU. The proposal has been criticised not only by civil rights and privacy organisations,[16] but also by the European Parliamentary Research Service,[17] and the European Data Protection Supervisor and European Data Protection Board.[18]

Belgium, current holding the presidency of the Council, recently proposed a new approach that specifically addresses the issuing of official orders to scan chat logs. Published on 9 April 2024, this compromise envisages first assigning the various providers to a set of discrete risk categories.[19] Proposed risk categorisation strategies include analysing the type of the service, i.e. message service, social media or similar, as well as the architecture, e.g. interactions, and also the effectiveness of policies and safety by design, statistical data and a mapping of user tendencies. Another bone of contention here is the handling of end-to-end encryption. While providers should not be obliged to provide access to communications secured with end-to-end encryption, scanning should still be possible even for these end-to-end encrypted communications.

In the event of CSAM being discovered, blocking orders could be issued, which would naturally result in internet blocks. Proposals currently envisage this kind of internet block order being issued jointly by regulatory authorities acting in concert. Such a block order at domain level may nonetheless result in entire services becoming unavailable, however, as individual pages on a website cannot be blocked using DNS blocking techniques. This could also affect cloud storage services, for example. Appropriate steps must therefore be taken to prevent unlawful 'overblocking' scenarios.

16 https://edri.org/wp-content/uploads/2023/09/Statement-to-EU-countries-Do-not-agree-to-mass-surveillance-proposal-warn-NGOs.pdf

17 https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf

18 https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

19 https://data.consilium.europa.eu/doc/document/ST-8579-2024-INIT/en/pdf

07

Reviewing disconnections
of IP connections

07 Reviewing disconnections of IP connections

According to the adjudicatory practice of the Telekom-Control-Kommission (TKK), an established internet connection may be disconnected only once within 31 calendar days; the IP address must remain static within this period (TKK 18 December 2017 R 3/16). Regulation (EU) 2015/2120 (TSM Regulation) grants end users not only the right to use online services but also to host their own services or applications over the internet. In order for end users to provide these services or content (e.g. via a self-operated web server), such users require (at least) a dynamic public IPv4 address, which is directly assigned by the internet access service provider to the IP terminal device (smartphone, LTE modem, DSL router etc.) utilised by the end user. This makes the end user directly accessible via the internet. To provide services and applications from their terminal device on a permanent and unrestricted basis, the end user requires an IP connection with this IPv4 address. Accordingly, and in line with the TKK's adjudicatory practice, end users have the right to receive a public (and at least dynamic) IPv4 address on request.

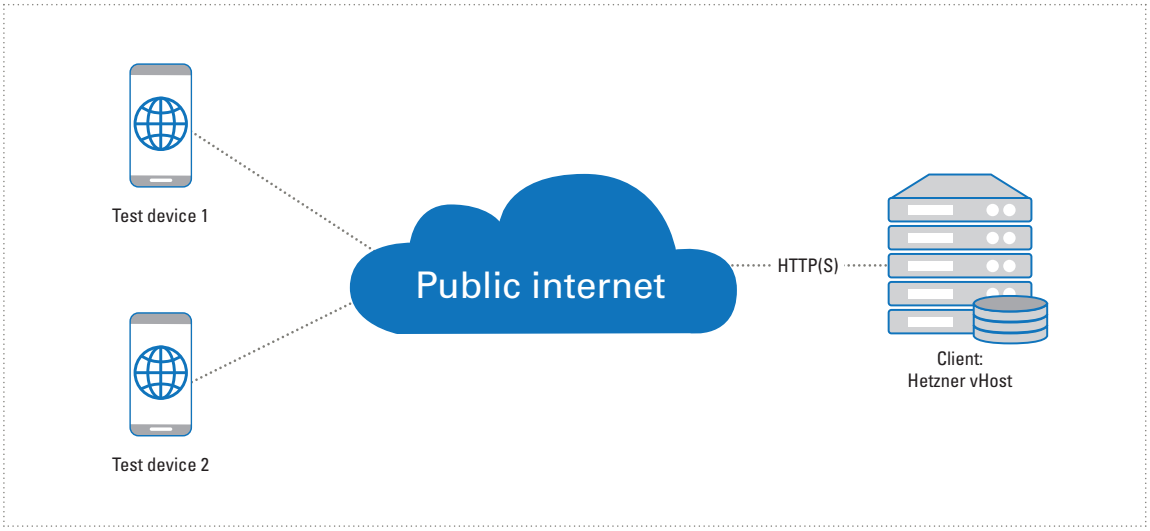
In the course of procedures pursuant to Art. 5 Par. 2 TSM Regulation, RTR conducted a review of whether end user rights were actually honoured during the reporting period. In the case of five providers, checks were made to verify whether a dynamic public IPv4 address had been assigned as requested by end users and whether a connection had been maintained over a period of at least 31 days.

A 'mystery shopper' approach was also used to conclude a contract for a SIM-only product at all five providers reviewed. The selected products were among the most inexpensive on offer, with some budget brands also being selected from certain providers. During the order process itself (and with no further activity on the part of the regulatory authority) none of the providers proactively supplied a public IPv4 address. Information about the availability of a free public IPv4 address was not provided during any of the order processes.

An attempt was therefore made to achieve the assignment of a public IPv4 address using a standardised email. With one provider, this public IPv4 address was assigned directly after contacting them, while another provider noted this could be completed using the self-service portal and a third provider provided a guide to configuring this kind of IPv4 address by editing access point name (APN) settings. One provider sent back a form that could be used to apply for a public IPv4 address. With the fifth provider, several requests were necessary, but the public IPv4 address was then ultimately also assigned. In conclusion, our mystery shopper was able to secure the assignment of a public (and at least dynamic) IPv4 address from all five providers.

In a next step, a check was made to confirm that services could actually be provided via the IPv4 address. This involved using SIM cards from two providers at the same time in Android user devices, setting up a web server accordingly and then monitoring the continuous availability of the server over the internet. The test setup is presented in figure 4.

Figure 4: Test setup for reviewing forced disconnections



Availability over the internet was confirmed for all five providers. The web server, operated on port 8080, was reachable from a server hosted by Hetzner, with traffic being routed unmodified and connections remaining established over a long period of time.

For three providers, a connection lasting for 31 calendar days was also determined during the reporting period. These providers either made no forced disconnections or a disconnection of this kind was identified only after 31 calendar days.

At two providers, the connection was also maintained over a longer period of time, but these providers then forced disconnections after approximately 28 calendar days. These providers were advised of the suspected breach of Art. 3 TSM Regulation and ordered to remedy the breach. Both providers duly remedied the breach and forced disconnections now only take place every 31 calendar days.

08

Free choice of user device

and location of network termination point

08 Free choice of user device and location of network termination point

Art. 3 Par. 1 TSM Regulation grants end users a free choice of user device. This choice constitutes a key aspect of net neutrality. The question of the extent to which end users enjoy a free choice of the user device (modem or router) that they use to gain access to a communications network or the internet, is typically discussed using terms such as 'router freedom' or 'device neutrality'. Such discussions address the question of where the network termination point (NTP) is located, which represents the boundary between the public communications network and the user's (private) network. This boundary can be seen either at the 'wall box' (i.e. a wall-mounted device installed at the end customer) or at the end customer's interface as provided by their user device (modem or router), which is supplied by the provider. In Austria, the internet provider typically specifies the location of the network termination point in their terms and conditions. However, Art. 3 Par. 1 TSM Regulation grants users a right to use their router of choice. If the provider supplies a router with an integrated modem, however, this router must have the option of being configured to use 'bridge mode': in this mode, the router no longer works as a modem and all related features (e.g. Wi-Fi, firewall) are also deactivated. In this scenario, users can then connect their own choice of router. While there is no legal definition of the NTP as of this writing, it would be possible for RTR to codify this by issuing a corresponding ordinance. In 2023, RTR conducted an evaluation of this issue. The results of this evaluation showed that the current situation in Austria does not require any official specification of the network termination point.

In the course of that evaluation, talks were held with ISPs and advocacy groups, with complaints and queries in an Austrian context being analysed alongside international practice. These investigations revealed that only nine of 27 EU Member States had specified the network termination point to date. In most of these cases, the end user's wall box was defined as the network termination point. In recent years, RTR has received only isolated complaints in relation to users wanting to use their own router. ISPs also informed the regulatory authority that few users actually make use of this free choice of router.

On the other hand, the evaluation did find that ISPs could improve transparency in relation to router freedom. Several major providers have therefore now improved the information on their websites. Users can also visit a page on the RTR website (https://www.rtr.at/nap) that includes links to guides provided by ISPs about configuring routers in bridge mode.

RTR will continue to monitor national and international developments, one aim being to identify a greater interest in own router use on the part of end users. If the general conditions should change, the conclusions drawn about legislative measures may need to be re-evaluated.

The full evaluation report can also be found on the RTR website.[20]

[20] https://www.rtr.at/TKP/presse/pressemitteilungen/presseinformationen_2023/pinfo10112023tkp.de.html

09

Potential breaches of net neutrality

and procedures

09 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.

Of the resulting procedures to be completed with the issuing of a decision, one procedure had been decided (by the Federal Administrative Court, BVwG) on 30 April 2020. In June 2020, the ISP appealed to the Supreme Administrative Court (VwGH), submitting a petition to recognise the suspensory effect. On 9 December 2021, this appeal was dismissed as unjustified by the VwGH and the decision of the regulatory authority confirmed on all points (R 3/16). A complaint was also raised in response to another decision to impose a cease order by the TKK and a request for recognition of the suspensory effect submitted. The BVwG also rejected this request for recognition of the suspensory effect. In April 2022, the ISP withdrew the complaint and the BVwG ruled to terminate proceedings (R 5/17).

As in previous reporting periods, the work of the regulatory authority focused on auditing the products and the technical/commercial practices adopted by ISPs, first notifying the latter of any potential breaches identified and consulting with them to identify legally compliant solutions. The procedures completed in the reporting period were able to identify technical and commercial practices that raised issues in light of the provisions of Art. 3 of the TSM Regulation and therefore required investigation.

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 9.1.
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 9.2.
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.
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.

Pos.	Type of practice	Description
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 9.3.
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 (VBKG), in relation to market surveillance (EU Market Surveillance Regulation) or in the form of sanctions (EU Sanctions Regulation). → A more detailed description is given in section 9.4.
08	Domain blocks resulting from the EU Sanctions Regulation	The regulatory authority considers the EU Sanctions Regulation to be an EU legislative act in the sense of Art. 3(3) subparagraph 3(a) TSM Regulation. Measures adopted by ISPs in line with the accepted interpretation of the regulation therefore do not normally infringe applicable laws aimed at safeguarding net neutrality.

In previous reporting periods, alongside the major providers of internet access services, many minor providers of fixed and mobile networks have been reviewed to detect this practice. A total of twelve ISPs were selected, to whom questionnaires requesting information about products and technical practices were sent. On a positive note, we emphasise numerous ISPs' continuing readiness to cooperate, without the need for a formal supervisory procedure. In one of these procedures, a longer implementation period was granted (until April 2022) to enable technical changes establishing compliance with the TSM Regulation. All other request-for-information procedures had been terminated, although two only after referring them to the TKK for initiation of a supervisory procedure.

In all procedures, the focus of TSM Regulation violations was primarily on the non-assignment of public IPv4 addresses, port blocking and the forced disconnection of IP connections. The two procedures that had been referred to the TKK for the initiation of a supervisory procedure pursuant to Art. 5(1) of the TSM Regulation largely concerned a refusal to assign public IP addresses to end users on the part of these two MVNOs. A supervisory procedure against one of these MVNOs was dropped in April 2021. In the same month, the TKK also issued a decision against the second MVNO in response to the failure to allocate public IP addresses to end users (R 9/19). Both procedures were very time-consuming, since intermittent technical audits were required (see the 2021 Net Neutrality Report for details).

In the 2021 reporting year, the regulatory authority had sent requests for information (questionnaires) to the four providers of zero-rated products ('zero-tariff' options). Corresponding details can be found in the 2022 Net Neutrality Report. In June 2022, four supervisory procedures were then initiated against four providers as a result of zero-rating in existing customer contracts (R 12/22, R 13/22, R 14/22 and R 15/22). The corresponding decisions, issued in November 2022, have since become legally enforceable and all measures required of the providers were duly implemented by March 2023. Nine other supervisory procedures were also initiated in response to domains blocked as a result of the EU Sanctions Regulation (Council Regulation (EU) 2022/350) and then dropped in June 2022 as no net neutrality breach was identified.

In the current reporting period, one procedure was initiated by the TKK because an ISP had not provided a free dynamic public IPv4 address as requested by end users. End users were therefore unable to provide reliable applications or services themselves, which constituted a breach of Art. 3 Par. 1 TSM Regulation. During the course of the procedure, the ISP remedied the breach. As a result, the procedure was terminated for lack of a breach at the time of the decision (R 1/23).

In the current reporting year, the TKK opened twelve procedures on its own initiative against various ISPs. Some of these cases investigated DNS blocks affecting various domains, which were not adjudged to be breaches of Art. 3 Par. 3 TSM Regulation. While several IP access blocks that had been put into place did constitute a breach of Art. 3 Par. 3 TSM Regulation, these were no longer active at the time of the decision and the procedures were therefore terminated. An additional three procedures relating to network blocks were initiated by the TKK against several ISPs. These procedures had not been completed by the end of the reporting period.

The TKK also initiated eight procedures ex officio against various ISPs in which it was determined that the DNS blocks set up for various domains by these ISPs did not constitute a breach of Art. 3 Par. 3 TSM Regulation. IP access blocks set up by the ISPs and still active at the time of the decision were found to constitute a breach of Art. 3 Par. 3 TSM Regulation, however. The ISPs were ordered to remove these blocks by the stated deadline and to notify the TKK accordingly. This decision has been appealed and a ruling from the Federal Administrative Court (BVwG) is pending.

On the subject of forced disconnections, a total of five investigations of various ISPs were initiated by RTR in the reporting period, with the aim of ascertaining whether or not an established internet connection had indeed been disconnected only once within 31 calendar days. For three of the five ISPs, no evidence of a breach of Art. 3 TSM Regulation was found. For the other two ISPs, there was reason to suspect legally non-compliant behaviour and the results were submitted to the TKK. As a result of the fact that the ISPs duly restored legal compliance in good time, no cease orders needed to be issued on the part of the TKK.

In its work programme, the Body of European Regulators for Electronic Communications (BEREC) identified the need for a re-evaluation of developments in the IP interconnection markets. In this context, information was sought from five ISPs pursuant to Art. 181 of the Telecommunications Act 2021 (TKG 2021).

In relation to the EU Sanctions Regulation, 17 notifications were received from various ISPs about DNS blocks that had been set up as a result of this regulation. The measures taken were necessary to ensure the legitimate enforcement of the EU Sanctions Regulation and did not constitute a breach of net neutrality.

Alongside activities previously described as part of the cited procedures involving existing products, 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.

9.1 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.

At this juncture, it needs to be understood 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.[21]

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.

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 DNA 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.

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

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.

9.2 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.

9.3 Disconnection of IP connections

In the course of review procedures pursuant to Art. 5 Par. 2 TSM Regulation, five providers of mobile internet access services were audited in the relevant 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 days and complied with this requirement in good time. For further details, see section 7.

9.4 Internet blocking

Since 2018, the regulatory authority has conducted procedures in 80 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.

As of March 2021, network blocks can now also be set in another context, as permitted by the EU Consumer Protection Cooperation (CPC) Regulation 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 TKK 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 TKK 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 of March 2022 effectively created new blocking obligations for ISPs. In the opinion of the TKK and RTR FB TKP, the regulatory authorities responsible for safeguarding net neutrality, no additional transposition of the EU Sanction Regulations is required through a national administrative act. 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.

Website blocking in the reporting period

In the reporting period, a total of 40 supervisory procedures were pending against ISPs, of which 23 involved copyright law and 17 the EU Sanctions Regulation. In the case of internet blocks pursuant to the EU Sanctions Regulation, no breach of the Net Neutrality Regulation was identified. Of the 23 procedures relating to copyright law, twelve were terminated, a removal of IP blocks was ordered in eight procedures and three procedures were still pending at the end of the reporting period. Further details of the procedures are provided in section 5.

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

In relation to compliance with provisions on net neutrality, eight decisions regarding the setting of access blocks (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) were made in the eighth reporting period (until April 2024). These decisions were issued in August 2023 and have been appealed. A ruling from the BVwG is pending. 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.

The decisions on measures issued in December 2017 and April 2021 (in R 3/16, R 5/17 and R 9/19) 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).

On 4 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). 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. 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. 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. Lastly, educom was prohibited from offering its zero-rated 'free e-learning' subscription service for existing customer contracts.

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.

Table 3: Procedures pursuant to Art. 5 Par. 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	✓

⚖: challenged | ✓: final

Procedure	ISP	Brief description	Date of decision	Status
R 5/18	UPC Telekabel Wien GmbH, UPC Telekabel-Fernsehnetz Region Baden Betriebsgesellschaft 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	✓
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	✓

⚖: challenged | ✓: final

Procedure	ISP	Brief description	Date of decision	Status
R 6/19	UPC Telekabel Wien GmbH, UPC Telekabel-Fernsehnetz Region Baden Betriebsgesellschaft 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	✓
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	✓

⚖: challenged | ✓: final

Procedure	ISP	Brief description	Date of decision	Status
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	✓
R 16/22	next layer Telekommu-nikations-dienstleis-tungs- 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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	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	✓

⚖: challenged | ✓: final

Procedure	ISP	Brief description	Date of decision	Status
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 Telekommu-nikations-dienstleis-tungs- 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 Telekommu-nikations-dienstleis-tungs- 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 Par. 1 TSM Regulation.**	2023-08-07	✓
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 Par. 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	✓

⚖: challenged | ✓: final

Procedure	ISP	Brief description	Date of decision	Status
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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	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 Par. 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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	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	✓
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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	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 Par. 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	✓

⚖: challenged | ✓: final

Procedure	ISP	Brief description	Date of decision	Status
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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	2023-08-07	⚖
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 Par. 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 Par. 3 TSM Regulation. **These decisions were appealed and a corresponding ruling is to be issued by the BVwG.**	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	✓

⚖: challenged | ✓: final

Procedure	ISP	Brief description	Date of decision	Status
R 1/23	Innonet ICT-Services 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.**	2023-09-11	✓
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	✓
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. **Procedure is still pending (as of 30 April 2024).**	Ongoing	
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. **Procedure is still pending (as of 30 April 2024).**	Ongoing	
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. **Procedure is still pending (as of 30 April 2024).**	Ongoing	

9.6 Ensuring legally compliant terms of contract

With the TKG 2021, the TKK'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 2023, 441 procedures were carried out. This represents a slight decrease from 489 such cases in the previous year (2022). Overall, however, when compared with 2021, at 402 procedures, and 2020 at 333, this constitutes a significant rise in cases. Reasons for this change include the various adjustments necessitated by the new TKG 2021 as well as the fact that providers of interpersonal communications services (NIICS) are now also subject to reporting requirements. Numerous enquiries from both end users and providers were also handled on the subject of notifying or reviewing contractual conditions. 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 2023 that more and more European and international undertakings are becoming active as providers on the Austrian market. In ensuring legal compliance of contract terms, the TKK – and since 1 November 2021 RTR – 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, has 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. Once again in every procedure in 2023, the TKK 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 conditions 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.

9.7 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 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 more than 1,400 telecoms conciliation cases in the period May 2023 to April 2024, around 100 related to net neutrality. As was the case in previous years, most of these complaints related to the bandwidth made available by the provider. While the number of complaints relating to mobile service quality has increased slightly year on year, the case volume is nowhere near the level that was observed during the covid crisis. The downward trend in complaints relating to internet speeds for fixed networks, as observed in recent years, became even more firmly entrenched during this reporting period. In this same context, it is encouraging that most of these cases ultimately resulted in an amicable solution being identified for the end users and providers in the course of the conciliation procedure.

There were also a few isolated conciliation cases relating to requests for public IP addresses from providers and on the topic of 'router freedom' or 'device neutrality' (see also the section on 'General enquiries').

On the whole, it can be assumed that Austrian providers generally fulfil their duties towards end users under the TSM Regulation.

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 – 04/21	05/21 – 04/22	05/22 – 04/23	05/23 – 04/24
Mobile network	162	118	69	87
Fixed network	85	54	47	26

9.8 General enquiries

On the topic of net neutrality, RTR's Telecommunications and Postal Services Division also received enquiries unrelated to conciliation cases. Specifically, enquiries in the reporting period addressed minimum content pursuant to Art. 4 TSM Regulation, dynamic public IP addresses and router freedom. 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.

10

Indicators

of continuous availability of non-discriminatory internet access services

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

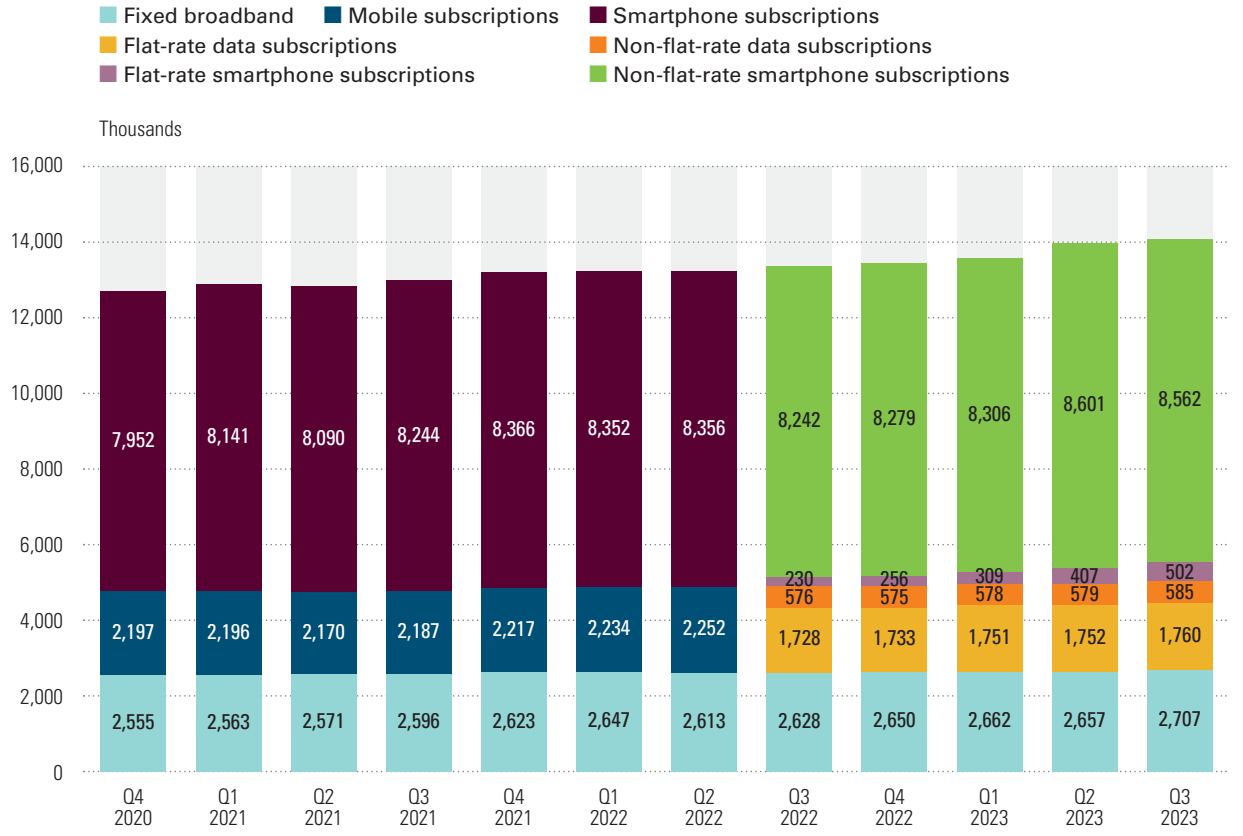
National regulatory authorities assess the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology (Art. 5 Par. 1 TSM Regulation). The following key figures are evaluated here:

- 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.[22] In the third quarter of 2023, total broadband connections rose to 14.1 million – a 5% increase from 13.4 million in the third quarter of 2022. The number of fixed connections, data subscriptions (flat-rate or non-flat-rate) and non-flat-rate smartphone subscriptions grew by rates between 2% and 4% in this period. In percentage terms, the largest growth (although still with low volumes) was seen in flat-rate smartphone subscriptions, which jumped by 118% from 230,000 to 502,000.

[22] A new counting method has been used from the third quarter of 2022 onwards.

Figure 5: Fixed and mobile broadband connections*)



Source: RTR

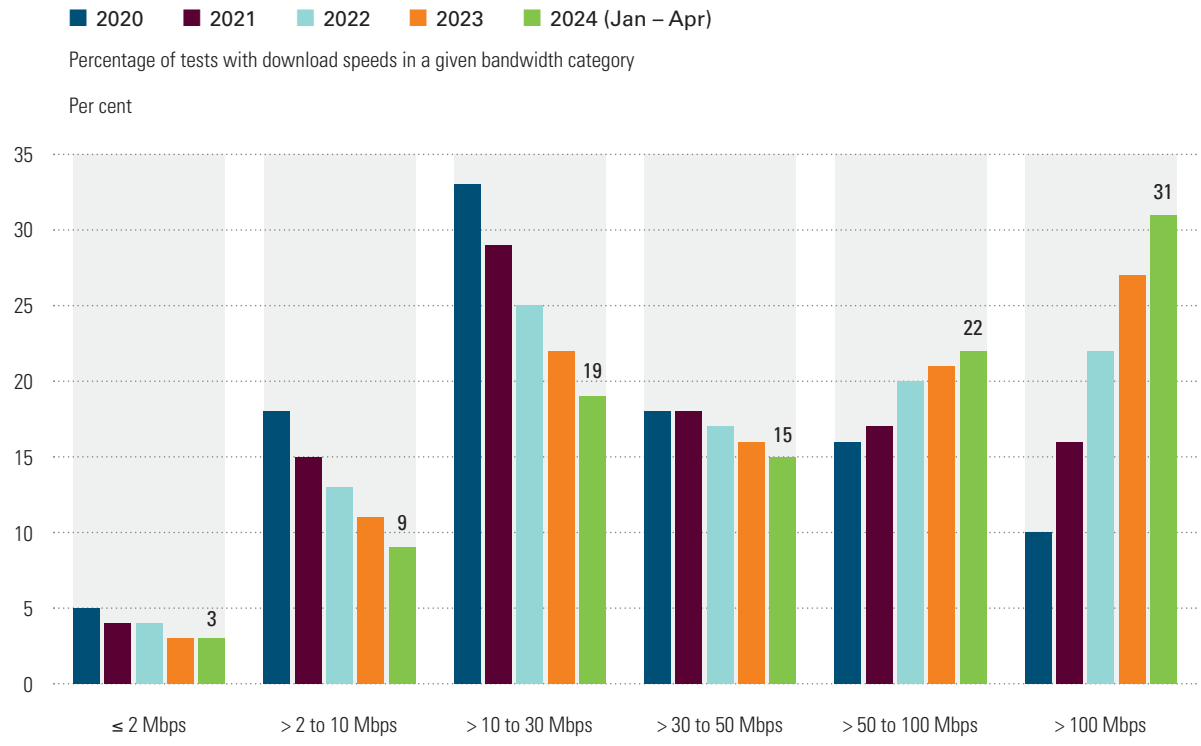
*) Data on broadband connections are collected quarterly. M2M SIM cards are not shown in the chart.
KEV data are available in the form of Open Data at: https://www.rtr.at/rtr/service/opendata/OD_Uebersicht.de.html

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.[23] NetTest data are made publicly available as open data.[24] Figure 6 shows the percentage of tests with download speeds in a given bandwidth category. In 2023 and 2024 (January to April), most tests can be assigned to the top category: download speeds of more than 100 Mbps. During 2023 and 2024 (January to April), categories featuring download speeds of less than 50 Mbps once again reveal a decline in share in comparison with previous periods. In contrast, growth has been posted by categories featuring download speeds of more than 50 Mbps. As a result, the trend continues to be towards the measurement of higher download speeds.

[23] Available as a mobile app (Android, iOS) and as a browser test.

[24] https://www.netztest.at/de/Opendata

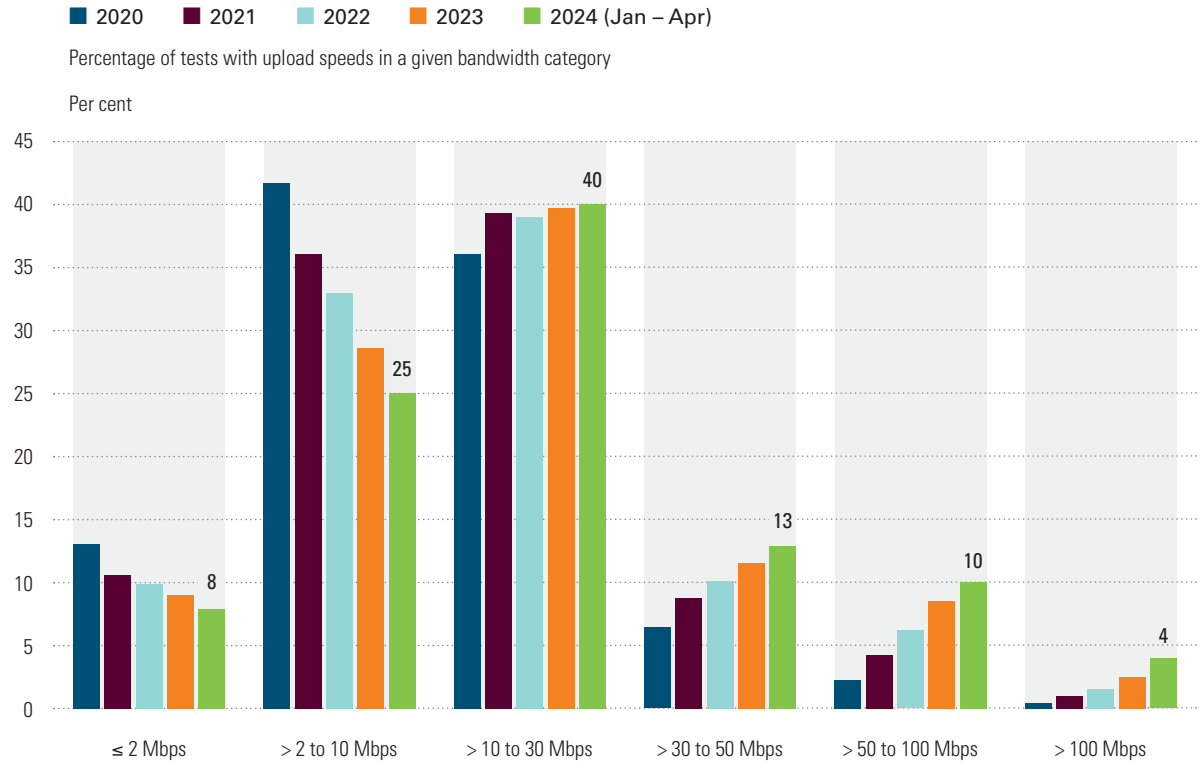
Figure 6: Distribution of download speeds by reporting period



Source: RTR-NetTest

Download speeds are not the only metric showing an upward trajectory. 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 2023 and 2024 (January to April). Proportions are shrinking for categories with measurements under 10 Mbps, while categories with measurements above this figure are showing growth. A continuous uptick in proportions continues to be seen for categories with measurements above 30 Mbps.

Figure 7: Distribution of upload speeds by reporting period

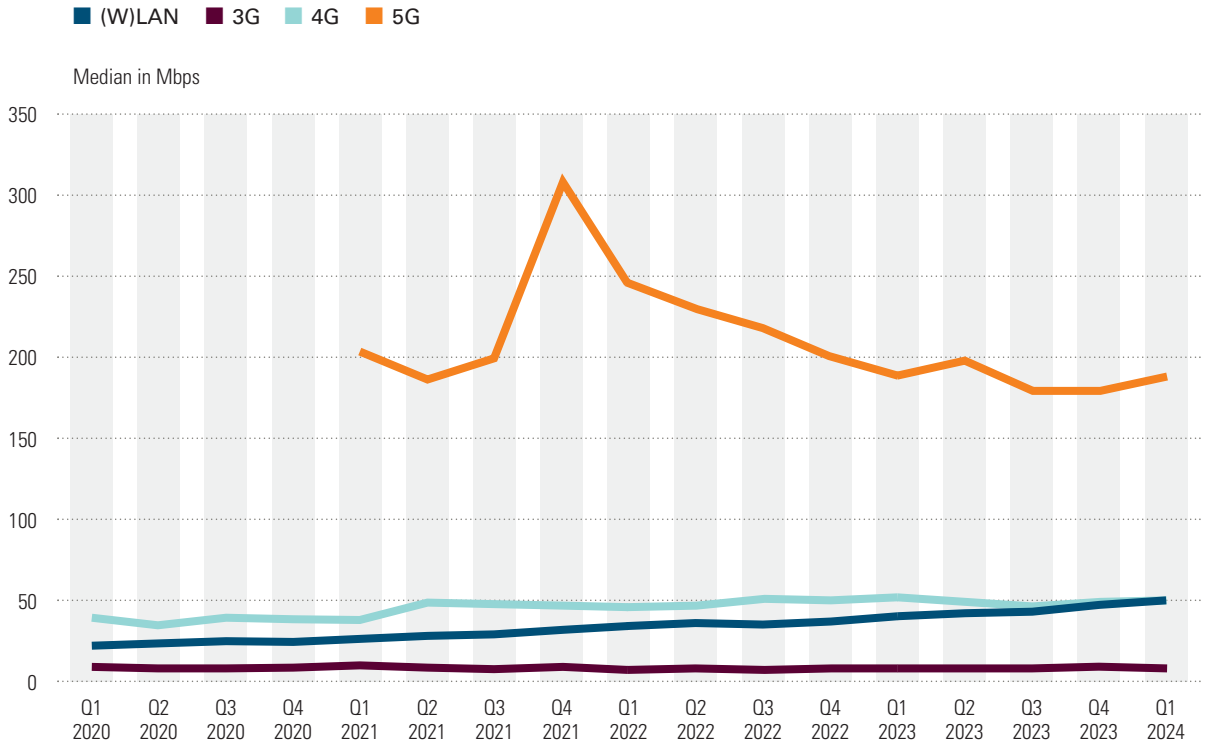


Source: RTR-NetTest

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.[25] Distinctions are made between 3G (UMTS, HSPA), 4G (LTE), 5G (NR) as well as on the basis of measurements of 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. The median for 5G connections is shown from the first quarter of 2021. 5G achieves significantly higher download speeds than other mobile telecommunications standards. Compared with the first quarters of 2023 and 2024, similar median values were recorded for 3G, 4G and 5G: for 3G, the median download speed in the first quarter of 2024 was 8 Mbps, with 50 Mbps for 4G and 188 Mbps for 5G. For (wireless) LAN, median figures rose instead by 25%, from 40 Mbps in the first quarter of 2023 to 51 Mbps in the first quarter of 2024.

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

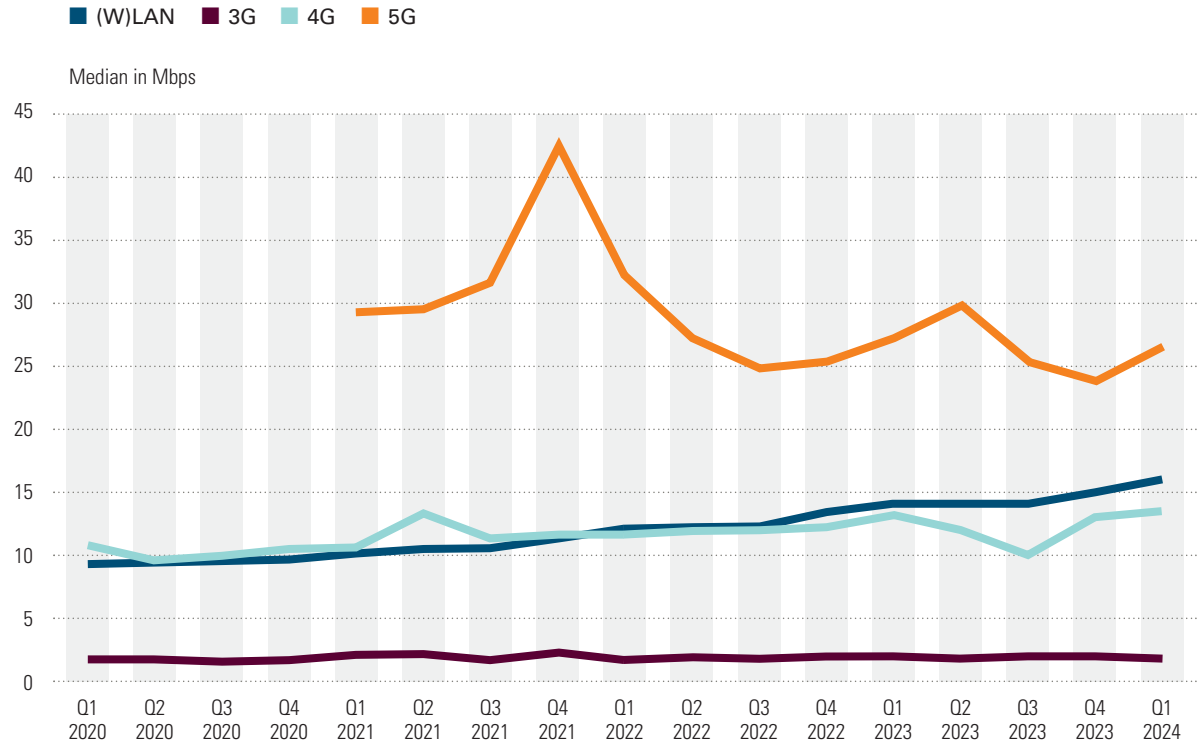
Figure 8: Download speed by technology



Source: RTR-NetTest

As is shown in figure 9, 5G also achieves significantly higher measurements for upload speed than other mobile telecommunications standards. In terms of median upload speeds, a pattern similar to download speeds is therefore observed. In the first quarter of 2024, the median upload speed for 3G was 2 Mbps, with 13 Mbps for 4G and 27 Mbps for 5G. These figures are similar to those recorded in the first quarter of 2023. For (wireless) LAN, median measurements rose by around 12%, from 14 Mbps in the first quarter of 2023 to 16 Mbps in the first quarter of 2024.

Figure 9: Upload speed by technology

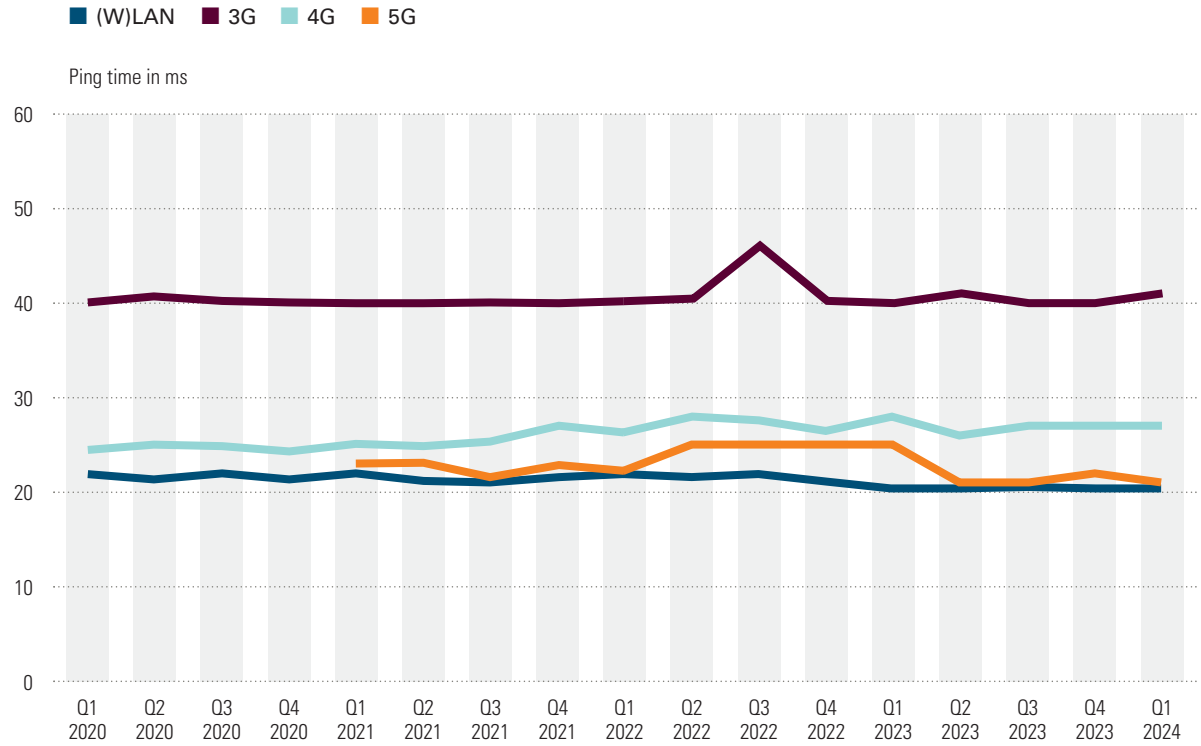


Source: RTR-NetTest

'Ping time' – or 'latency' as it is more correctly termed – 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. In the first quarter of 2024, 3G measurements recorded the highest latency of 41 ms.[26] The lowest latency in this period was 20 ms, achieved using (wireless) LAN measurements, although 5G measurements were only slightly higher, at 21 ms. Compared with the first quarter of 2023 and 2024, latency figures for all technologies stayed much the same.

[26] Compared with other technologies, the number of measurements over 3G is very low and can lead to fluctuations in median values as reported.

Figure 10: Latency (ping) by technology

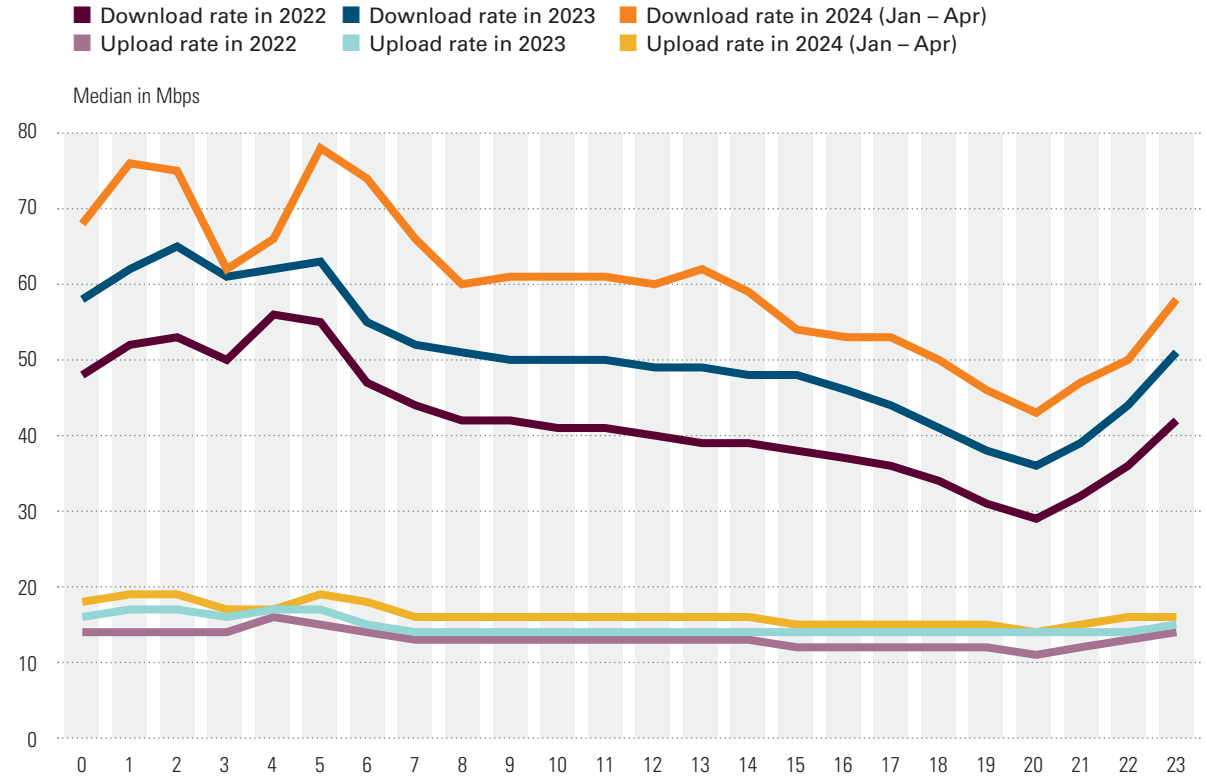


Source: RTR-NetTest

Figure 11 shows the median download and upload speeds by time of day in 2022, 2023 and 2024 (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 2024 (January to April), the median of download speed measurements was 71 Mbps. After 6 a.m., the median of download speeds measured declined continuously until it reached the figure of 43 Mbps during the peak hour, which is between 8 p.m. and 9 p.m. During 2023, both download and upload speeds were higher for each hour of the day than in 2022. In 2024 (January to April), the speeds measured were again higher than in 2023.

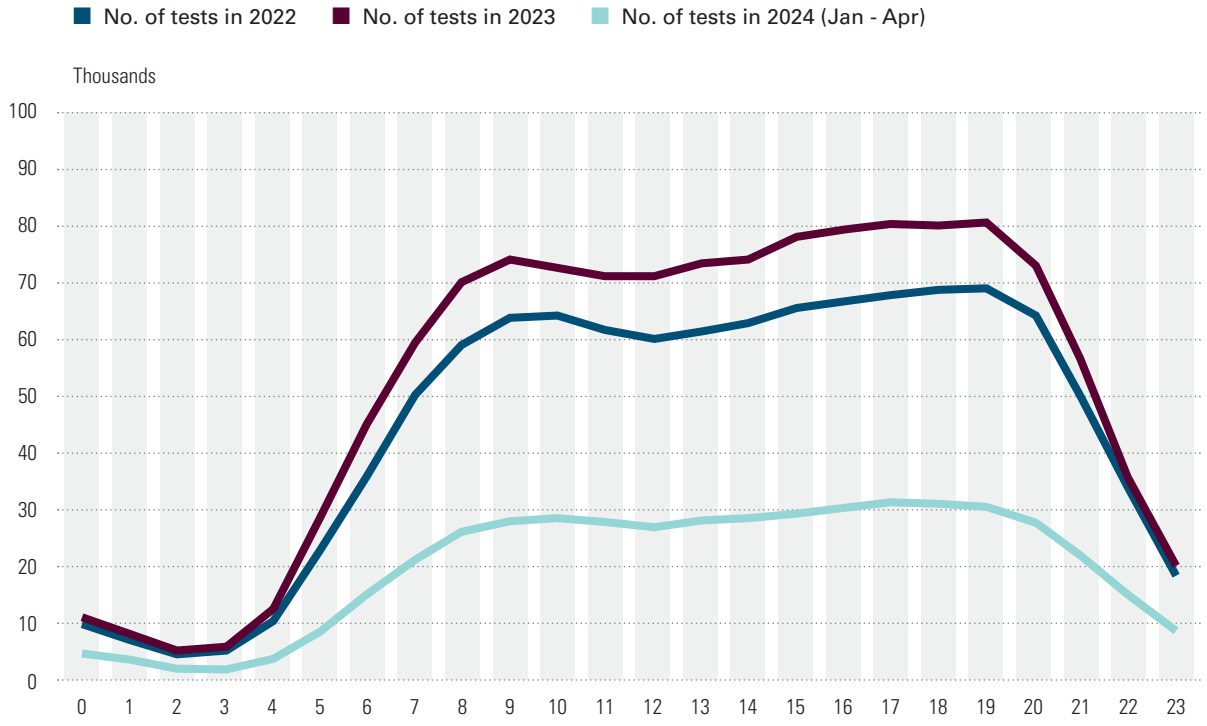
The number of measurements differs widely from one hour to another during the day. In 2023, most measurements (81,000) were made in the hour between 7 p.m. and 8 p.m. Compared with 2022, more measurements were recorded for every hour of the day in 2023.

Figure 11: Download and upload speeds by time of day



Source: RTR

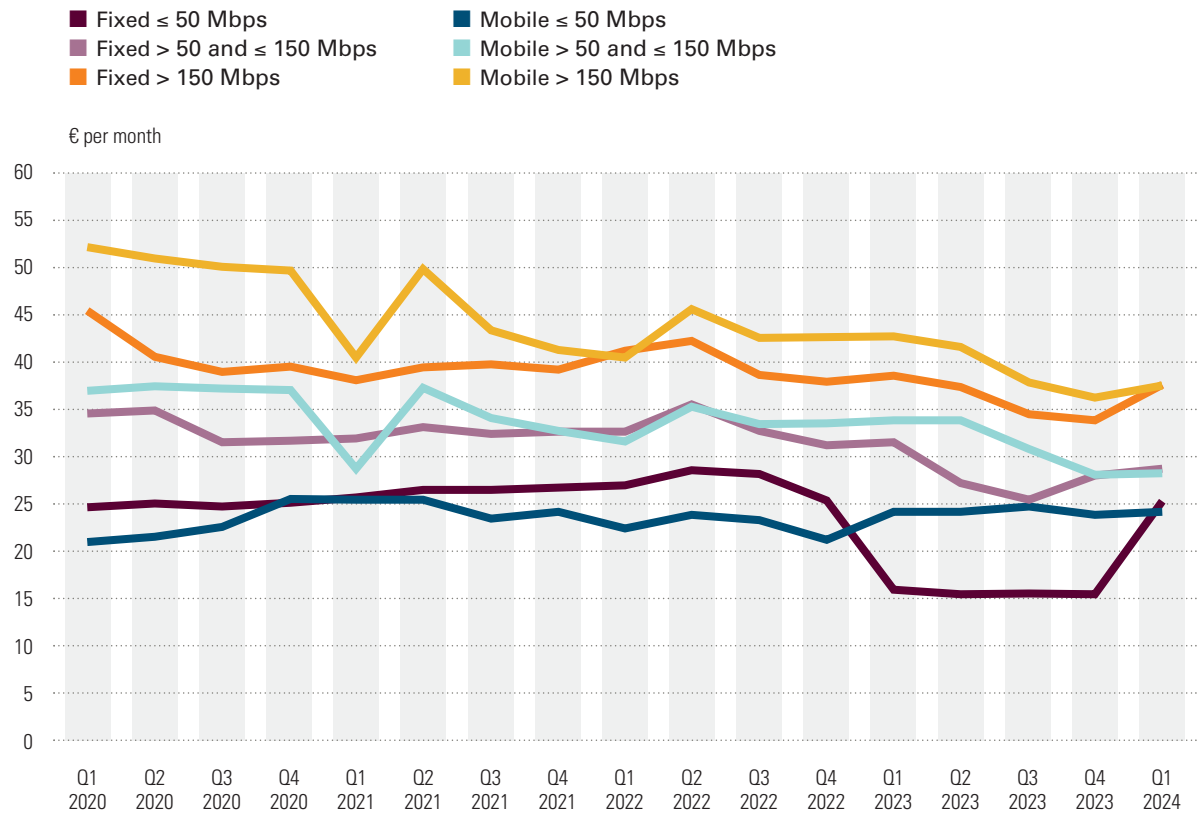
Figure 12: No. of tests by time of day



Source: RTR-NetTest

Finally, figure 13 contrasts three price baskets for fixed network broadband and three price baskets for mobile broadband. In recognition of the greater availability of higher bandwidths, this year's report is the first to include price baskets for the following bandwidth categories: ≤50 Mbps, >50 to ≤150 Mbps and >150 Mbps.[27] 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). The basket price is based on the least expensive product from each operator that can be included in the respective basket. Compared with the first quarter of 2023 and 2024, the price basket for fixed network ≤50 Mbps shows an increase of 58% to around EUR 25, therefore again attaining a level seen in the fourth quarter of 2022.[28] At EUR 24, the price basket for mobile broadband ≤50 Mbps remains at a similar level. A decline can be observed for the four remaining price baskets. The largest percentage decline – of around 17%, down to EUR 28 – can be seen for mobile broadband in the >50 to ≤150 Mbps category.

Figure 13: Price baskets: fixed vs. mobile broadband



Source: RTR

[27] Instead of the previous ≤30 Mbps, >30 to ≤100 Mbps and >100 Mbps

[28] In 2023, a significant factor in this basket's decline was the price cut to EUR 9.90 (excl. fixed service fee) made by A1 Telekom Austria AG to its 10 Mbps product.

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 connection while also identifying any potential restrictions affecting their access.

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. Download and upload speeds have also seen further improvements in the reporting period. In recognition of the greater availability of higher bandwidths, this year's report is the first to include price baskets for new categories featuring higher sets of bandwidths. 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) Net Neutrality Regulation) was ensured in Austria over the past five years.

11

Outlook

on further activities

11 Outlook on further activities

In our future work, we at the Austrian regulatory authority will continue to follow the approach taken in the past. Specifically, we are committed to proactively monitoring developments in the markets as well as to being available as a partner to ISPs, internet users and all other stakeholders to consult on net neutrality issues. To this end, the corresponding organisational prerequisites have also been met. Specifically, the activities described below are currently planned for 2023/2024 or by the end of the next reporting period in April 2024.

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.[29] 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 basic right against another, a factor also potentially impacting business models.

[29] See https://www.netztest.at/de/

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. Within this framework, 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 2024, 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 2024. The report will be based on the net neutrality reports to be published by the NRAs by 30 June 2024.

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. One key focus in the reporting period was on the entry of major content providers into markets for electronic communications networks and services. It is planned to continue this work 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 **further development of 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 2025 – will be offered for comment as part of the budget consultation to be published later this year.

12

Appendix

12 Appendix

12.1 Mapping of the report to the structure of the guidelines

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 4 → Section 5 → Section 7 → Section 8 → Section 9
"the number and types of complaints and infringements related to the Regulation"	→ Section 9
"main results of surveys conducted in relation to supervising and enforcing the Regulation"	→ Section 3 → Section 9
"main results and values retrieved from technical measurements and evaluations conducted in relation to supervising and enforcing the Regulation"	→ Section 9 → Section 10
"an assessment of the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology"	→ Section 10
"measures adopted/applied by NRAs pursuant to Article 5(1)"	→ Section 9.5

12.2 Index of Figures and Tables

Figure

Page

Table

Page

12.3 Abbreviations

AGB:	general terms and conditions
BEREC:	Body of European Regulators for Electronic Communications
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
CDN:	content delivery network
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
GDPR:	General Data Protection Regulation
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 *(Kommunikations-Erhebungs-Verordnung)*
KommAustria:	Austrian Communications Authority
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)*
SSH:	secure shell; refers to a network protocol and corresponding program, used to securely establish an encrypted network connection with a remote device
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 *(Telekommunikationsgesetzt)*
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 *(Urheberrechtsgesetz)*
VIX:	Vienna Internet eXchange
VoD:	video on demand
WAN:	wide area network

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

RTR

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