RTR

RTR NET NEUTRALITY REPORT

2021

Report in accordance with Art. 5(1) of the TSM Regulation
and Par. 182 – 183 of the BEREC Guidelines
on the Implementation by National Regulators
of European Net Neutrality Rules

Net Neutrality
FIFTH ANNIVERSARY

www.rtr.at

2021

Austrian Regulatory Authority for Broadcasting and Telecommunications
(Rundfunk und Telekom Regulierungs GmbH)
Mariahilfer Strasse 77 – 79, 1060 Vienna, Austria
tel.: +43 (0)1 58058-0; fax: +43 (0)1 58058-9191; e-mail: rtr@rtr.at
www.rtr.at

RTR NET NEUTRALITY REPORT

2021

Report in accordance with Art. 5(1) of the TSM Regulation
and Par. 182 – 183 of the BEREC Guidelines
on the Implementation by National Regulators
of European Net Neutrality Rules

Net Neutrality
FIFTH ANNIVERSARY

Contents
Net Neutrality Report 2021

	By way of introduction	**6**
	PART I: Fifth Anniversary of Net neutrality	**9**
1	**The long path leading to the Net Neutrality Regulation**	**10**
2	**Issues upon initial implementation**	**13**
2.1	Port blocking	13
2.2	Public vs. private IP addresses	13
2.3	Disconnection of IP connections	14
2.4	Video on demand (VoD) – a specialised service	15
2.5	Revision of the Net Neutrality Regulation and the BEREC Guidelines	16
3	**Perennial issues in the past five years**	**17**
3.1	Network blocking	17
3.2	Zero-rating	18
3.3	Traffic identification	20
3.4	Transparency studies	21
4	**Supreme court rulings**	**22**
4.1	ECJ on zero-rating	22
4.2	Austrian Supreme Administrative Court on network blocking	22
5	**Changes in open internet access in 2016 – 2021**	**24**
6	**The major unknowns**	**28**
6.1	QoS differentiation for a single subscription	28
6.2	Specialised services	30
6.3	New network blocks?	30

Part II Reporting period 1 May 2020 - 30 April 2021 31

1 Stakeholders and institutions in enforcement 32

2 Timeline of regulatory authority activities 34

3 Safeguarding net neutrality and supervisory measures 36
3.1 Port blocking 38
3.2 Private IP addresses and services 40
3.3 Zero-Rating Monitoring 40
3.4 Network blocking 46
3.5 Supervisory measures 48

4 Other indicators and activities 52
4.1 RTR conciliation procedures 52
4.2 General requests 52
4.3 Indicators of continuous availability of non-discriminatory IAS 53

5 Outlook on further activities 60

Appendix 1: Mapping of the report to the structure of the guidelines 64
Appendix 2: Index of Figures and Tables 65
Appendix 3: Abbreviations 66

Publishing Information 69

Introduction

Five years in the digital industry are almost an eternity. Take LTE for example: it had just gotten off the ground five years ago. Now, 5G is all anybody ever talks about. The 2021 Net Neutrality Report, now the fifth report on the openness of the internet in Austria published by the RTR Telecommunications and Postal Services Division, is a little something to celebrate. With this report, we wish to bring into perspective the major net neutrality issues that have emerged in the past and are expected in the future. At the same time, we attempt to position and evaluate net neutrality as a regulatory field from the regulator's standpoint. It is also intended as a report to fulfil the 'classic reporting obligation' for the past twelve months, providing interested members of the public with an overview of the market trends relevant for a discussion of net neutrality issues, as well as of related activities and measures by the regulatory authority.

What has happened in the past five years? What future trends can be identified?

Net neutrality was a highly controversial issue before 2015, when the Net Neutrality Regulation was in preparation. Conflict at that time had centred on issues including: the opportunities for monetisation available to access networks, and the contribution to be made to infrastructure development by over-the-top players (OTTs), while the question was also debated as to how to ensure fairer competition (i.e. a level playing field) between access networks (ISPs) and OTTs. Considering the internet's significance as an engine of innovation, there was initially strong public interest in regulating net neutrality. This was additionally fuelled by a concern for safeguarding the stream of urgently needed innovations generated at the periphery of the internet.

Today, we now know how effective the Net Neutrality Regulation has been in guaranteeing free access to the open internet. Yet, today, we are also aware of new gatekeepers playing a key role at entirely different points within the internet. No longer can we meet the goal of safeguarding net neutrality by merely safeguarding it in relation to access networks. Other gatekeepers also need to be drawn into regulators' view. Such gatekeepers, who influence the openness of the internet and its potential for innovation at the levels of society and the economy, include app stores, operating systems, user devices and browsers. The open internet – the goal to which the Net Neutrality Regulation is committed – is threatened at other points by those whose business models had originally become feasible as a result of net neutrality. Thus, today we face the urgent challenge of taking a systemic view of the internet that spans value chains and ecosystems.

Several issues, such as port blocking and automatic disconnection, have been largely resolved as a result of the awareness engendered by the Net Neutrality Regulation. Meanwhile, though, other issues have proven stubborn. Such perennial challenges include network blocking, a mechanism applied in an increasing number of areas (including copyright law, consumer protection and gambling). This means that ISPs are constantly being held accountable for enforcing legislation relating to online activities. 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 the fundamental rights of all those concerned.

Zero-rating is a different case. This term refers to providing various services without deducting the incurred data traffic from the volumes included in users' subscriptions. Practice, backed up by empirical research carried out by the RTR Telecommunications and Postal Services Division, has shown almost every product offered in the market to be an open service, accessible to any content provider.

Despite early fears that 'walled gardens' would develop as an alternative to open internet access, competition for customers and demand diversity have been identified as factors favouring the emergence of open products. Even though zero-rating offers have flourished in Austria, no case has been seen up to now involving any reduction of the data volume included in subscriptions or any increase of rates per GB. Instead, zero-rating in the Austrian market appears to be an intermediary step toward flatrate subscriptions.

We are facing technological upheavals that require new responses to basic questions familiar from the past: How can investments be made to pay off, and how can the options offered by technology be turned into revenue? How can we ensure further development of general internet access as well? How can we guarantee opportunities for innovation without express authorisation and consent from third parties?

Topics that are currently under discussion or that we have identified as emerging topics in the near future include: QoS differentiation among internet connections, the emergence of platforms in mobile networks, network slicing and specialised services, new, opaque forms of user control, and the relationship of these issues to developing open internet access. Discussion of these topics is already underway, even though related policies have not yet been fully worked out. We wish to discuss these issues during our five-year anniversary event.

Finally, I wish to comment briefly on the focus areas of our work during the past reporting period. Without wishing to go into detail here, four general areas mainly concerned us during this period, in addition to international and monitoring activities.

1) Zero-rating: after becoming substantially common, zero-rating is now offered by all major mobile network operators.

2) Network blocking: related discussions have now pivoted toward amending various specific pieces of legislation in order to create a legal framework.

3) The exceptional load on the internet caused by the Covid pandemic was well managed in Austria, without any significant impact on net neutrality.

4) New developments in the context of 5G spectrum awards in 2019 and 2020.

We enjoy a working relationship based on trust with all market participants, which proves especially worthwhile in this context. Many of the new issues linked in some way to net neutrality are discussed with providers early on, before action is taken later. Conversely, this approach usually avoids procedures, with many misunderstandings often being resolved at an early stage.

On the whole, the status of the open internet in Austria once again presents a highly positive picture in this reporting year. We are nonetheless aware of the complex, new challenges waiting at the doorstep. For the coming year, we have committed to the task of asking the right questions and identifying suitable answers.

To adequately meet this task in future, we set up a separate net neutrality team last year, along with a corresponding interdisciplinary 'one-stop shop.' In this way, we can appropriately respond in a focused and targeted way – in other words ensure an agile response – to the wide scope of issues currently falling under regulation in the context of digital challenges. The result is an enhanced capacity to meet the needs of consumers and businesses. Comprehensive expertise is a necessary condition for making the right decisions, even unprompted ones if required.

On this occasion, I wish to especially thank the experts from our net neutrality team, foremost of all Belma Abazagic, for her outstanding work in this area and most especially for preparing this report. Alongside one's daily duties, it is not always easy to find the patience and time necessary to draft a truly well-researched report of the kind presented here.

With this in mind, I hope you will find this an interesting look back at the recent history of net neutrality, and at the same time a look to future developments, inasmuch as the report provides at least a basis for forecasts.

Vienna,
June 2021

Dr. Klaus M. Steinmaurer

Managing Director
Telecommunications and Postal Services Division
RTR

01

PART I
Fifth Anniversary of Net neutrality

01 The long path leading to the Net Neutrality Regulation

Today, there is general agreement on the importance of net neutrality, at least in principle. Yet, eight or ten years back, the issue was the subject of intense discussion. This debate had been sparked by advances in technology. These advances enabled specific identification, routing and discriminating treatment of data traffic in the internet, a medium that had previously been neutral toward all applications. Internet access service providers (ISPs) now had the option of 'monetising' the new possibilities, meaning they could: sign exclusive contracts with providers of (proprietary or third-party) online content, charge customers for supplying the data they needed for certain services, or distinguish (or prioritise) service quality based on various criteria, or even block traffic. The discussion of online platforms that took place ten years ago was not as intense as the current debate surrounding the new Copyright Directive[1] or the proposals for a Digital Markets Act (DMA)[2] and a Digital Services Act (DSA). [3] But even ten years back, discussions were being dominated by ISPs calling for providers of online content (CAPs) to share in the costly expansion of internet access networks. The CAPs, the majority of them large American corporations, were either hosting third-party content or directly supplying their own.[4] Discriminating treatment of data traffic was to be allowed in order to recover network rollout costs. This contrasts with the position of content providers, who argued that demand by access network customers was generating this data traffic: with their subscriptions, network users had already paid for free access to an open internet. This access was either unlimited, as is usually the case with a flat rate for fixed network access, or limited in volume, in the case of mobile network access. According to this view, customers had in principle already paid for any and all traffic and had covered any associated costs. It followed that users must be allowed access to all legal content on the internet, whereas any additional fees could be seen as access providers taking advantage of their monopoly on terminating connections or as their way of protecting their services from unwanted competition. Customer demand for internet access services would cease if use were to be sharply limited, content providers further argued.

At a higher, economic policy level, there was more at stake. Should an open internet continue to exist, in which every OTT player could supply products to consumers without having to sign elaborate agreements with numerous different ISPs? Or should the internet simply be transitioned into a new marketing phase? Already the central engine of innovation at the time, the internet was being discussed not only in terms of aspects specific to telecommunications but also in view of its impact on the innovation generated in downstream markets, as well as in light of demands for a comprehensive consideration of fundamental democratic rights. The demand for net neutrality has, after all, always been inextricably linked to the fundamental right to freedom of expression.

Thus, discussions about how to respond to these issues were typical in many countries at the beginning of the last decade. Responses differed, with the sector agreeing on its own code of conduct in some countries, such as in the UK and in Scandinavian countries, and individual ISPs in other countries laying down their own rules. In Austria at the time, there was considerable uncertainty as to which business models would be compatible both with the new options offered by technology and with the basic concept of net neutrality, and which models the regulatory authority would consider incompatible. There was a general expectation of a European solution, since net neutrality was clearly not a matter for negotiation at national level and uniform rules were needed at least EU-wide. Another approach would have run counter to the single market, with transaction costs and detrimental economic impact sure to follow. In the face of pressure from ISPs, after waiting so long

[1] Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ 2019 L 130, p. 112.

[2] Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

[3] Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.

[4] This discussion continues within a limited scope. Cf. for example https://www.serentschy.com/the-regulatory-journey-from-a-european-perspective/. This paper draws on research including an empirical survey of the impact of net neutrality rules on fibre rollout in OECD countries. Here it is observed that: "Monetization options for telcos are shrinking; in particular EU Net Neutrality rules are limiting monetization options for telcos."

for an EU solution, Austria briefly considered whether to introduce its own net neutrality rules. The idea was ultimately shelved, however.

In parallel with activities within the Telecommunications and Postal Services Division at RTR, the Body of European Regulators for Electronic Communications (BEREC) had also evaluated several related subtopics by 2013 (such as quality of service, transparency, IP interconnection and potential challenges to competition) while consistently sharing insights with other bodies including the European Parliament. No complete position had as yet been worked out, however.

In September 2013, the European Commission presented a proposal for a Digital Single Market.[5] In addition to identifying 'specialised services' alongside conventional internet access services, the proposal addressed numerous other topics beyond the scope of net neutrality, including harmonising wholesale products, quality assurance across networks, general authorisations and roaming. The Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) published a paper on net neutrality in May 2013,[6] recognising the key social and economic role of the internet in Austria and Europe, and calling for maintaining an open internet in the interests of growth and innovation. The regulator's aim here was to convey its view to market participants in Austria and to propose a position to the community of national regulatory authorities.

Net neutrality took centre stage in EU digital policy in 2014, after the European Parliament had voted in April 2013 to adopt the proposal for a regulation concerning a Digital Single Market and subsequent deliberations of the legislation within the Council of the European Union. It was during this period that net neutrality shifted from being a marginal issue relevant for insiders to becoming one of the most frequently discussed topics among telecom and media regulators, and a tech issue familiar to the general public. A number of events and consultations followed, among them one by the Council of Europe. Impetus came from developments both in Europe and the United States that aroused broad media interest and were widely discussed. The net neutrality rules previously established by US regulator the FCC were partially lifted through a court ruling.[7] The following discussion over new rules – including the possibility of prioritising services – led to legislation in early 2015 that classified the internet under Title II of the US Telecommunications Act, reclassifying it as a common carrier subject to regulation instead of an unregulated information society service.[8] This gave the FCC the possibility of intervening as regulator. A highly intense debate with broad participation ensued, as seen in the more than 4 million public comments received by the FCC. Specific business models such as zero-rating and specialised services also played a prominent role.

In Austria, many general issues were discussed at a conference, entitled "Net neutrality in the light of convergence", that was held in October 2014. The event was attended by prominent visitors from Austria and other countries. Further discussions with ISPs followed.

[5] Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM(2013) 627 final.

[6] https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/RTRPosition2013.en.html

[7] Net neutrality had been discussed in the United States as early as the 1990s. The ruling in question was handed down in the case of Verizon v. FCC. The latter had issued an order in 2010, requiring ISPs to provide transparent information on network traffic management and to refrain from content blocking and 'unreasonable' content discrimination.

[8] This order was rolled back under the Trump Administration. The FCC under Chairman Ajit Pai reclassified the internet as an information society service under Title I, effective as of 11 June 2018. Since then, no uniform net neutrality rules have been in effect in the United States. At this point it is not yet clear whether a new law reintroducing a uniform set of federal rules will indeed be enacted, as Democratic Vice President Kamala Harris had promised during her election campaign. Additional details relating to this topic will be presented by Prof. Barbara van Schewick at the RTR net neutrality fifth anniversary event on 6 July 2021.

An initial proposal for a regulation was published in July 2015, following intense deliberations. Finally, in November of that year, the European Union issued the Net Neutrality Regulation (Telecoms Single Market (TSM) Regulation).[9] The new rules became effective as of 30 April 2016. At the same time, BEREC was tasked with preparing guidelines to aid in interpreting the Regulation, to be published by 31 August 2016. The guidelines were intended to ensure that the Regulation would be applied as uniformly as possible throughout the EU – in line with the Single Market concept. The draft guidelines were then put out for consultation for a six-week period beginning in June 2016. Participation was overwhelming, particularly on the part of civil society actors. With more than 480,000 responses received, participation was the broadest of any public consultation in BEREC's history.

The Net Neutrality Regulation and the 2016 BEREC Guidelines[10] became the key elements for the subsequent implementation of net neutrality in the Member States. Still in effect today in unamended form, the Net Neutrality Regulation is the basis for annual reporting at national and European level on the implementation of net neutrality – and as such the basis for this report. Based on initial experience, the BEREC Guidelines were later revised in 2020, with several additions included.[11]

[9] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015. The Regulation represents the legal basis for both net neutrality and roaming.

[10] BoR (16) 127.

[11] BEREC Guidelines on the Implementation of the Open Internet Regulation, BoR (20) 112. https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation

02 Issues upon initial implementation

2.1 Port blocking

The issue of port blocking has been a focal point for regulators, especially in the early years of the Net Neutrality Regulation, as well as on several occasions since.

What is behind the term? At a technical level, data are transmitted within the internet via the Internet Protocol (IP), which is supplemented by transport protocols such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Both of these protocols have the option of assigning differing identity numbers to the various services. These are referred to as 'ports.' This is particularly important on the server side, because port numbers allow incoming traffic to be assigned to the proper service where more than one service is running under one and the same IP address. Examples of widely used port numbers include: 443 (HTTPS), 80 (HTTP) and 465 (SMTPS).

This means that, in order to run and use services, it is critical that all data traffic be successfully delivered, regardless of the port number used. This is ensured by the Net Neutrality Regulation, through a ban on the 'blocking' of services without justification. Port blocking is currently used in Austria in order to safeguard net integrity and security. Here, specific obsolete or unsafe services are blocked as they would otherwise threaten the internet. When deciding whether to permit blocking, the seriousness of any risk is always weighed against potential restrictions to the availability and use of services. This might mean that, in some cases, blocking is only allowed for a defined period – until the specific threat has been averted. On numerous past occasions, operators rolled out large numbers of modems to customers with administration ports that proved vulnerable for attacks. Such ports subsequently had to be blocked for traffic within the particular operator network. In these cases, the regulatory authority set a deadline by which the ISP concerned was required to replace the vulnerable customer devices and subsequently unblock the port.

See Part II section 3.1 for an overview of current port blocking decisions.

2.2 Public vs. private IP addresses

The Net Neutrality Regulation envisages an internet that is as open as possible. The goal is an internet not dominated by only a handful of large content providers who serve a multitude of content users. Rather, every end user ought to play both parts – the role of content producer and the role of content consumer.

The Net Neutrality Regulation entitles end users to not only view, use or download applications and services or information and content, but also to publish their own content and provide their own services. The range of such applications and services includes: smart home devices for personal use (such as 'smart' thermometers or weather stations), data sharing via network attached storage (NAS) and consumeroperated web servers.

Providing such services assumes the capability of directly accessing the service involved. In technical terms, this requires a public IP address to be assigned to the end user wishing to provide a service. This address then allows other users to access the service. This compares more or less to a conventional telephone service, which presupposes a given subscriber being assigned a phone number in order to be able to accept calls directly from other parties.

In the past, end users were usually directly assigned public IP addresses. Nowadays, though, private IPv4 address assignment is common, especially in mobile networks, with network address translation (NAT) being used. Apart from technical aspects, this is, among other things, because ISPs wish to save on public addresses, which, as with IPv4, could become scarce. Where multiple users have to share a single public IPv4 address via NAT, they will not be able to provide their own services in practice. Technical solutions do in fact exist that allow the provision of certain services even in such cases, for example by assigning public IPv6 addresses to enable end users to access their devices. But simply assigning IPv6 addresses is not a satisfactory solution, at least not yet, since IPv6 connectivity is not yet available in broad regions within the internet. Assigning an IPv4 address, in contrast, is a viable solution, with IPv4 connectivity available throughout the internet.

All that said, it follows that end users are entitled to receive at least a dynamic public IPv4 address from their ISPs free of charge on request. Dynamic IP addresses satisfy requirements as they allow end users to register their personal domains using 'dynamic DNS.' In this way, services can be provided continuously for the most part, because connections are permitted to be terminated no more than once every 31 days.[12] ISPs are not allowed to charge fees for public dynamic IPv4 addresses, as users' option of providing their own services is considered to be part of internet access service offers.

The regulatory authority addressed this issue shortly after the Net Neutrality Regulation came into effect. In mid-2016 a supervisory procedure was initiated against an ISP after this provider had marketed a product for which IPv4 addresses were issued against payment alone. This ISP was prohibited from charging fees for assigning dynamic public IPv4 addresses in future and ordered to refund any payments previously collected.[13] This regulatory authority decision was upheld by the Federal Administrative Court in mid-2020. A ruling by the Supreme Administrative Court is pending. The Telekom-Control-Kommission (TKK) issued a similarly worded decision against another ISP in early 2021.[14]

In the case of every ISP, regardless of size, the regulatory authority has been enforcing end users' right to assignment of a public IPv4 address since 2017. Only a relatively small number of end users request public IPv4 addresses, so that even small ISPs and those just entering the market are able to comply with this right.

2.3 Disconnection of IP connections

The need for a public IPv4 address is one factor that limits end users in their ability to exercise the right to provide their own services. Another factor is automatic disconnection of internet connections (IP connections), which may occur repeatedly after brief, regular intervals.

Before the Net Neutrality Regulation took effect, it was common for some ISPs to disconnect their customers' data connections (IP connections) automatically after a certain period of time (usually 24 hours). No heed was given here to existing internet connections, in other words, the connection was always disconnected after this period, not only when it was idle. The reasons given here by the ISPs ranged from technical considerations relating to the assignment of IP addresses, to claims of effectiveness in protecting user privacy. This is a problematic measure, mainly because of reassigning dynamic public IP addresses – even when user devices are automatically reconnected. It can take from several minutes up to half an hour until a dynamic DNS service in use recognises the change in IP address and updates the clients. In effect, the frequency of disconnections constitutes a disproportionate restriction of end user rights under Art. 3(1) of the TSM Regulation.

The regulatory authority issued a formal decision on this matter back in 2017, in a case involving an ISP. Accordingly, any termination of an IP connection after an interval of less than 31 days infringes end user rights under Art. 3(1) of the TSM Regulation.[15] The regulator's legal opinion was upheld by the Federal Administrative Court (BVwG), while a ruling by the Supreme Administrative Court (VwGH) is pending.

[12] Refer to "Disconnection of IP connections" below for more details.

[13] https://www.rtr.at/TKP/aktuelles/entscheidungen/entscheidungen/R3_16_Bescheid_18122017.de.html (in German).

[14] https://www.rtr.at/TKP/aktuelles/entscheidungen/entscheidungen/R9_19.de.html (in German).

[15] https://www.rtr.at/TKP/aktuelles/entscheidungen/entscheidungen/R3_16_Bescheid_18122017.de.html (in German).

2.4 Video on demand (VoD) – a specialised service

The TKK initiated the first procedure in response to suspected breaches of the Net Neutrality Regulation in 2016. As part of this procedure, alongside issues surrounding the interruption of service after 24 hours and compulsory fees for the assignment of dynamic public IP addresses, the TKK also dealt with what are referred to as specialised services.

The procedure centred on A1TV, a two-component product consisting of a live linear IPTV service and a video-on-demand service including 'catchup TV.' The isosynchronous linear IPTV service clearly qualified as a specialised service under the BEREC Guidelines.[16] The status of the VoD component, in contrast, was dubious, as it shared the market with broad competition (including Netflix, Amazon, YouTube, Maxdome and Flimmit). What is more, the particular ISP was currently deliberating over a new TV platform to be engineered along as yet unclear lines. The issue then was whether the product did indeed entail quality requirements going beyond those generally applying to an internet access service, and was to be appropriately classified as a specialised service under Art. 3(5) of the TSM Regulation.

The evaluation report commissioned by the TKK concluded that no justification existed, either in relation to technical or business considerations, for prioritising the service. The underlying technology, a constant bitrate process, had in fact been developed by the ISP several years earlier, and the linear IPTV platform was used also for the VoD component. The TKK consequently prohibited prioritisation of the service.

What made this procedure especially significant was that, for the first time ever, a service was reviewed to decide whether it qualified as a specialised service. Beyond this, the procedure also addressed matters such as combinations of services as well as conditions of competition and continued recognition of specialised services over time.

Because the product had been marketed before the Net Neutrality Regulation entered into force and had in the meantime been widely distributed, the TKK decision provided for a three-year transition period. After this period, the VoD component was no longer permitted to be offered as a prioritised service.

The ISP subsequently contested the TKK decision before the BVwG. In April 2021, the latter court, concurring with the regulatory authority's legal position, dismissed the appeal as unfounded. The BVwG held that there was no objective technical need to optimise the service in question in order to meet a QoS level beyond that applying to non'prioritised' data transmissions. In addition, setting a three-year period for remedying the unlawful circumstances, beginning as of delivery of the contested decision, was permissible, according the BVwG ruling. At the same time, the right to appeal the decision before the VwGH was granted.[17] The BVwG ruling did not become final, since the ISP did in fact file a high court appeal. The VwGH has not yet handed down a ruling in the case.

[16] BoR (16) 127, 113.

[17] BVwG 23.04.2020 W120 2183616-1/29E.

2.5 Revision of the Net Neutrality Regulation and the BEREC Guidelines

The Commission published a report on the implementation of the TSM Regulation on 30 April 2019. The report was intended as a review of the Net Neutrality Regulation. In it, the Commission concluded that the principles set out in the Regulation continued to be an appropriate and effective way of protecting enduser rights and of supporting the internet in its role as an engine of innovation: *"Compared with the situation in 2015, before the regulation applied, endusers and content application providers express great satisfaction with today's state of affairs. Internet service providers also support the principles of an open internet and do not consider that it is necessary to amend these principles."*[18] No amendments to the Regulation were proposed, in order to maintain the current phase of regulatory stability and protect the rights of end users while supporting open internet access. The Commission stated that it would continue to monitor market developments as well as work closely with BEREC, *"[...] which is carrying out a coordination process that has successfully led Member States to converge their decisionmaking".* [19] A new Commission report on the TSM Regulation is expected four years after the initial report, which will be in 2023.

On 17 June 2020, BEREC published a revision of the Guidelines on the TSM Regulation in view of current market developments. The aim continues to be to contribute to consistent and uniform application of the TSM Regulation throughout Europe, as well as to regulatory certainty for all stakeholders.[20] BEREC's main focus, and that of its Open Internet Working Group, in 2019 and 2020 was to revise the Guidelines originally published in 2016. One of the activities was a stakeholder workshop held on 29 May 2019. The first focus topics to be included in the Guidelines were discussed at the event. The revised draft Guidelines were put to public consultation between 10 October 2019 and 28 November 2019. A total of 52 statements were received from various stakeholders. Apart from two statements declared confidential, all can be viewed on the BEREC website. Upon review, BEREC announced that the statements would require no major changes to the revised draft Guidelines. Only a few clarifications were correspondingly added. BEREC also published a consultation report[21] as well as a comparison of the 2016 and 2020 versions of the BEREC Guidelines.[22] The current version includes amendments and more precise wordings relating to: agreements between ISPs and end users, zero-rating, traffic management measures, specialised services and transparency measures. The RTR Telecommunications and Postal Services Division has played an active and leading role at the coordination meetings held periodically by the BEREC Open Internet Working Group. The division also contributed to the revision of the Guidelines. The RTR Telecommunications and Postal Services Division later also revised the (non-authorised) German translation of the 2016 BEREC Guidelines, in cooperation with German NRA Bundesnetzagentur.[23]

[18] European Commission, Report from the Commission to the European Parliament and the Council on the implementation of the open internet access provisions of Regulation (EU) 2015/2120, COM(2019) 13 final, 30 April 2021, p. 12, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0203

[19] European Commission, Report from the Commission to the European Parliament and the Council on the implementation of the open internet access provisions of Regulation (EU) 2015/2120, COM(2019) 13 final, 30 April 2021, p. 12, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0203

[20] BEREC Guidelines on the Implementation of the Open Internet Regulation, BoR (20) 112. https://berec.europa.eu/files/document_register_store/2020/9/Comparison_2020-BEREC-OI-GL_vs_2016_BEREC-NN-GL.pdf

[21] https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9276-berec-report-on-the-outcome-of-the-public-consultation-on-draft-berec-guidelines-on-the-implementation-of-the-open-internet-regulation

[22] https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9276-berec-report-on-the-outcome-of-the-public-consultation-on-draft-berec-guidelines-on-the-implementation-of-the-open-internet-regulation

[23] https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/2020-06-11_BEREC_Leitlinien_Netzneutralitaet.pdf

03 Perennial issues in the past five years

3.1 Network blocking

To safeguard net neutrality, the Net Neutrality Regulation prohibits ISPs from blocking net content. Only a very few exceptions are permitted here, such as when legislation specifically requires blocking. One example here is copyright law, which for 20 years has obliged ISPs to block access to websites that are intentionally structured to breach rules. 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[24] and the Market Surveillance Regulation.[25]

The regulatory authority has been taking a closer look at 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, and also forces 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. To this end, legislative activities at national and European level are closely observed, with the resulting insights actively applied when transposing EU-level provisions into national law.

Since 2018, the regulatory authority has conducted procedures in 29 cases involving network blocking. Here care has been given to ensure that any measures enacted comply with the Net Neutrality Regulation, i.e. by avoiding excessive interference with users' fundamental rights and by respecting the rights of other parties concerned, including ISPs and website operators. Of the total of 29 cases, 23 involved supervisory procedures, meaning ISPs had already set network blocks. The other six 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 (more details under Part I, section 4.2).

Major activities in connection with network blocking include exchanging information with stakeholders, public relations and participation in legislative processes. For example, 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. The regulatory authority is clearly aware of the completely new challenges arising as more and more daily activities are shifted to the internet, making it even more difficult and tedious for users to assert their rights. It needs to be emphasised, on the other hand, 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 runs the risk of becoming '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 crossborder infringements of consumer rights. Numerous European authorities coordinate their efforts in this cause. Authorities can now file injunctions against companies that infringe upon consumer rights. Sometimes, however, companies cannot be directly prosecuted in an online context. This might be the case where a company is established outside the EU and does not respond to claims. In such cases, the online intermediaries can be held accountable for

[24] 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.

[25] 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.

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 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 that arose in the past. The procedure could serve as a model to be applied in other areas as well.

3.2 Zero-rating

This term refers to products on offer that do not deduct the data consumed by designated applications (apps) or services/content from the data volume included in a customer's subscription rate. Such data volumes are therefore charged at a rate of 'zero' (i.e. are 'zero-rated'). Zero-rating, which is practised by several mobile network operators (see Part II section 3.3), plays a role within the broad discussion of net neutrality in the EU.

The regulatory authority consistently monitors zero-rating products offered in the Austrian market. The aim here is to identify any limitations to the free choice of available services, applications or content, and to stop such abuses where necessary. Observations are periodically analysed, with the findings published in the annual Net Neutrality Report.

Zero-rating can occur in various forms:

- Exclusive versus non-exclusive offer of the service subject to zero-rating (e.g. a service that may not be zero-rated by a competing ISP for contractual reasons)
- Offer comprising a single service (a specific application) or a category of services
- Offer updated at specific intervals and referencing a 'Most Popular' list (for example, top downloads in app stores)
- ISP product integrating proprietary services
- Offer providing for CAP-sponsored data, with the ISP providing the CAP's application to customers on a zero-rated basis
- Included in a subscription, or available as a payable subscription add-on for a set fee
- Part of a public wholesale offer, available to every CAP for use under a wholesale agreement
- Offer potentially linked to differentiated technical management (throttling of the service, discriminatory treatment based on data volume used)
- Offer potentially involving varying levels of intervention with regard to underlying traffic management or measures for identifying and charging for traffic

Zero-rating is not prohibited per se. Even so, ISPs are not allowed to throttle or block individual services as part of zero-rating offers. The principle of equal treatment applies even after customers have used up included data volumes. This means that technical traffic management measures must not be used to treat zero-rated services any differently from any other internet service. If the user is not generally allowed to visit any websites after using up their included data volume, this restriction must also apply to any zero-rated services.[26] This type of zero-rating is clearly prohibited. But a more differentiated view needs to be taken of other types.

A number of potential benefits are generally associated with zero-rating offers. One of the benefits is that end users are able to purchase a service without it counting toward the data included in their subscriptions (in other words, users are able to consume more of the service). ISPs also benefit by being able to attract more customers through zero-rating offers, in this way achieving heightened visibility over other ISPs competing in the mobile retail market. From the consumer vantage point, zero-rating could, if the supply were expanded, be interpreted as a stepping stone to flat rates.

[26] European Court of Justice (ECJ) 15 September 2020 C-807/19 and C-39/19.

On the darker side, with their zero-rating offers, ISPs can act as gatekeepers. For CAPs, zero-rating offers entail the risk of market fragmentation and elevated transaction costs (for example, as a result of varying wholesale agreements). With zero-rating, an ISP may select the applications to be included in the offer. The ISP defines and distinguishes the categories, and also specifies the technical standards and other wholesale conditions or criteria. An ISP with a zero-rating offer that is limited to services provided by designated CAPs is in effect determining the winners and losers in downstream markets. Zero-rating can also influence competition, among mobile network operators (MNOs) and between MNOs and mobile virtual network operators (MVNOs) or retailers (competitors without their own mobile networks).

One of the main concerns that accompanies the introduction of zero-rating offers is the possible increase in price per gigabyte; in other words, that rates will increase and/or included data volumes be reduced as a result. Businesses could reason that customers require smaller additional data volumes if the applications most frequently used are already zero-rated. From a net neutrality perspective, this would be an alarming trend, resulting in an increasingly smaller volume of data (or an increasingly higherpriced data volume) available to end users for other or new services. A situation is also conceivable where customers might no longer be able to try out and compare new services without having to reckon with additional fees. This could all but stifle the innovation process.

Many theoretical papers on the impact of zero-rating have appeared to date, but hardly any empirical studies were published in the early years. The RTR Telecommunications and Postal Services Division responded in late 2018 by resolving to prepare an international comparative study to examine the situation in Austria and several other Europe countries.[27] As part of the study, an analysis was conducted of data relating to over 11,000 subscriptions, offered by more than 50 different mobile network operators in 15 EU Member States between 2015 and 2018. The objective was to determine the impact of zero-rating on included data volumes, prices and prices per included data unit. In order to more precisely distinguish between subscriptions with and without zero-rating, regression analyses were used to control for factors such as other subscription characteristics and systematic differences among operators and over time (constant operator and time effects). Additionally, an operatorlevel basket approach was used to track developments at operator level.

Overall, the study concluded that zero-rating apparently has no systematic impact on other subscription characteristics such as included data, price or price per gigabyte. Instead, the effects vary across countries, the period observed, and among application categories. The findings therefore support a case-by-base evaluation of the (potential) consequences of zero-rating. This approach had already been recommended in the Net Neutrality Regulation and by the BEREC Guidelines serving to interpret it. Where zero-rating is to be assessed on a case-by-case basis (and its impact on the market as a whole), the assessment of specific effects in the various countries should take into account the situation in the particular country. Accordingly, no general observation can apparently be made about the relationship between zero-rating and subscription characteristics (included data and price).

[27] The RTR study, in English, entitled "Zero-Rating in the EU" can be downloaded from https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/ZeroRatingEU2019.en.html

3.3 Traffic identification

To enable billing of zero-rating products, ISPs need to be able to distinguish within the data consumed by consumers between zero-rated traffic and other types of traffic. This distinction can normally be made based on various technical characteristics.

In practice, as stipulated in agreements between ISPs and CAPs, zero-rated data traffic is potentially identified based on characteristics such as:

- IP addresses
- SNI
- Host name

These technical terms are explained briefly below.

IP addresses: Based on Recital 4 of the TSM Regulation, internet access services provide access to the internet and in principle to all the endpoints thereof. These endpoints are addressed at technical level using IP addresses. The IP address '81.16.157.3', for example, addresses the RTR web server. Technically, all communications activity in the internet is based on the exchange of data packets between various IP addresses. The underlying task performed by ISPs is to deliver these data packets to the IP addresses stored in the packets.

SNI: SNI refers to server name identification. Where an encrypted connection is established, the SNI includes the host name as well as what is generally referred to as the website 'domain.' The latter refers to the easily remembered address labels commonly used in the internet, such as 'rtr.at.' At technical level, no unambiguous relationship exists between a given IP address and a domain. As a result, one domain can be distributed over several IP addresses, for example to enable load sharing. Similarly, single IP addresses can be used for several different domains. This is commonly the case with shared hosting or content delivery networks. There is no technical means available of retrieving a complete list of all the content hosted under one IP address.

URL: This stands for 'uniform resource locator', a descriptor used in several protocols including HTTP, the one discussed here. A URL references a specific resource, which is often a subwebsite such as 'http://www.rtr.at/nn.'

To enable a distinction between zero-rated and non-zero-rated traffic, an ISP must ultimately monitor all traffic to determine whether it contains the characteristics for identifying content partner content. It is precisely this procedure, depending on how it is implemented, that potentially gives rise to data privacy concerns. While the regulatory authority sees the use of IP addresses for traffic identification as unproblematic and compliant with BEREC Guidelines, it nonetheless has doubts as to whether using other distinguishing characteristics such as SNIs and URLs is compatible with applicable data privacy law. The regulatory authority takes a critical view of products that use additional characteristics besides IP addresses. To date, the regulatory authority has not received any end user complaints in this regard.

3.4 Transparency studies

The RTR Telecommunications and Postal Services Division has commissioned or directly conducted several studies in recent years to determine whether data packets were being transmitted unaltered (referred to as 'transparency studies'). This has uncovered deep insights into the workings of various ISPs' telecommunications networks and their practices.

The tests included:

- General TCP and UDP measurements (for example of port blocking)
- Testing for SYN flooding
- DNS resolver responses to non-existent domains
- DNS blocks set
- HTTP caching and HTTP content manipulation
- HTTP virus protection test
- Tests of invalid HTTP syntax
- VOIP manipulation
- Tests of invalid TLS handshake syntax
- Identification of zero-rated traffic based on IP, SNI, host name or URL
- Manipulation of POP3 and SMTP handshakes
- Testing for STARTTLS stripping
- TLS bandwidth testing for various ports

One of the findings was that requests to non-existent domains were redirected by one ISP to a Google custom search, instead of returning 'NXDOMAIN', the correct DNS response. One ISP altered the HTTP header syntax of unencrypted HTTP data packets. In the case of another ISP, TTL times for one port varied from comparable times for other ports. Yet another ISP identified zero-rated traffic for certain CAPs based on the SNI entry and not the IP address.

Of the issues identified, all those falling within the regulatory authority's scope of responsibility could be settled directly with each ISP concerned.

Besides completing transparency studies, compliance with rules of the Net Neutrality Regulation was also reviewed. This entailed, for example, the use of a 'mystery shopping' approach, in response to enduser complaints, in order to verify whether public IPv4 addresses were being assigned upon request. Any related concerns identified could usually be resolved with the ISP involved in the case.

The regulatory authority will continue with transparency studies in future.

04 Supreme court rulings

4.1 ECJ on zero-rating

In September 2020, the European Court of Justice handed down its longawaited ruling on two linked cases, C-807/18 and C-39/19.

This was the firstever instance of an ECJ interpretation of the Net Neutrality Regulation, which enshrines the openness of the internet as a fundamental principle. The ECJ examined issues relating to zero-rating, that is, nonpayable transmission of data to serve defined applications or application categories (such as chat or music services).

The case underlying the ruling involved an ISP based in Hungary that had offered internet access services with zero-rating. After users had exhausted the data volumes included in their subscriptions, the ISP tightly throttled data traffic destined for any services or applications not included in the zero-rating package. In contrast, unlimited use of included services and applications was still supported. The ECJ found that an offer designed in this way represented a breach of the net neutrality rules.

The ruling confirms the regulatory authority's previous legal interpretation and practice. Zero-rating is not prohibited in principle. Yet internet access service providers are not allowed to throttle or block individual applications or services as part of zero-rating offers.

The principle of equal treatment applies even after customers have used up included data volumes. This means that traffic management measures must not be used to treat zero-rated services any differently from all other internet services. If, as in this case, the user is not generally allowed to visit any websites after using up their included data volume, this restriction must also apply to any zero-rated services.

With the ruling, the European supreme court confirmed the legal position previously taken by the Telekom-Control-Kommission (TKK). Back in 2017, for example, its decision to enact measures in case R 5/17 prohibited any throttling of individual services in the context of zero-rating.

In addition, the regulatory authority consistently monitors zero-rating products offered in the Austrian market. The aim here is to identify any limitations to the free choice of available services, applications or content, and to stop such abuses where necessary. Periodic analyses of the observations are presented in the annual RTR Net Neutrality Report. The regulatory authority is not currently aware of any offers available in the Austrian market which would unlawfully prioritise zero-rated services once users exhaust the data volumes included in subscriptions.

4.2 Austrian Supreme Administrative Court on network blocking

The TKK also initiated six assessment procedures at the request of several ISPs in 2019. The issue to be clarified was whether ISPs are allowed to block website access or whether such blocking in the specific case would constitute a breach of the Net Neutrality Regulation. The latter permits network blocking only in very specific situations. The difference here in relation to supervisory procedures in the context of network blocking is that the websites concerned had not yet been blocked. Thus, supervisory measures would not yet have been applicable. Specifically, these assessment procedures evaluated whether circumstances qualifying for an exception existed as defined in the Net Neutrality Regulation, thereby determining whether the possibility of subsequently blocking the websites would be legitimate.

The TKK welcomed the legal interest in the assessment procedures, ruling that the website blocks under investigation would be unlawful, as there were no grounds for claims against the ISPs on the part of the copyright holder. The rights holder in the procedure responded by lodging a complaint with the Federal Administrative Court (BVwG). In the meantime, the content was subsequently removed from the domain in question and the domain put up for sale. The BVwG nonetheless proceeded with the case and overturned the TKK's decisions. The TKK responded by lodging, as an authority, an appeal with the Supreme Administrative Court (VwGH) in six cases. This was the first time that the VwGH had been asked to rule on the TSM Regulation's net neutrality provisions. The VwGH ruling, encompassing almost 50 pages, discusses in detail the issue of network blocking in relation to fundamental rights and scope. The ruling also addresses the apparent tension existing between various relevant rules.

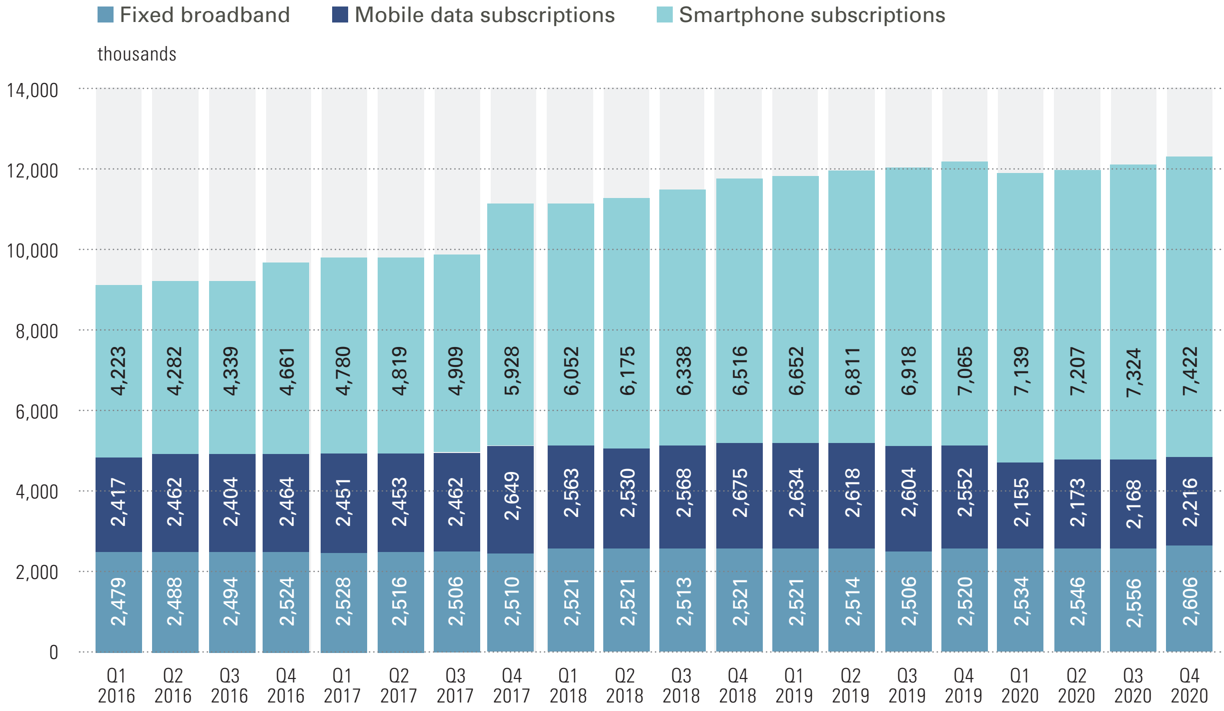
The VwGH found in favour of the TKK in all six cases, overturning the decisions handed down by the BVwG. As regards the procedure heard before the BVwG, the risk of a repeat infringement of copyright interests was not (or was no longer) present because the domain had since been made available and the content removed; the appeal case should therefore have been dropped. According to current legislation, there is no specific legal interest in determining the lawfulness of a network block before this block is put in place. A future amendment to the TKG should enshrine such assessment procedures in law. The aforementioned assessment decisions by the TKK have since become final.

05 Changes in open internet access in 2016 – 2021

The Net Neutrality Regulation requires national regulatory authorities to ensure compliance with Art. 3 and Art. 4 of the Net Neutrality Regulation and to promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology.

To offer a perspective of the changes in the past five years and to better evaluate developments, the section below refers to selected key indicators. An evaluation of continuous availability of non-discriminatory internet access services in 2020 – 2021 is provided below in Part II, section 4.3.

Figure 1: Fixed and mobile broadband connections[28]



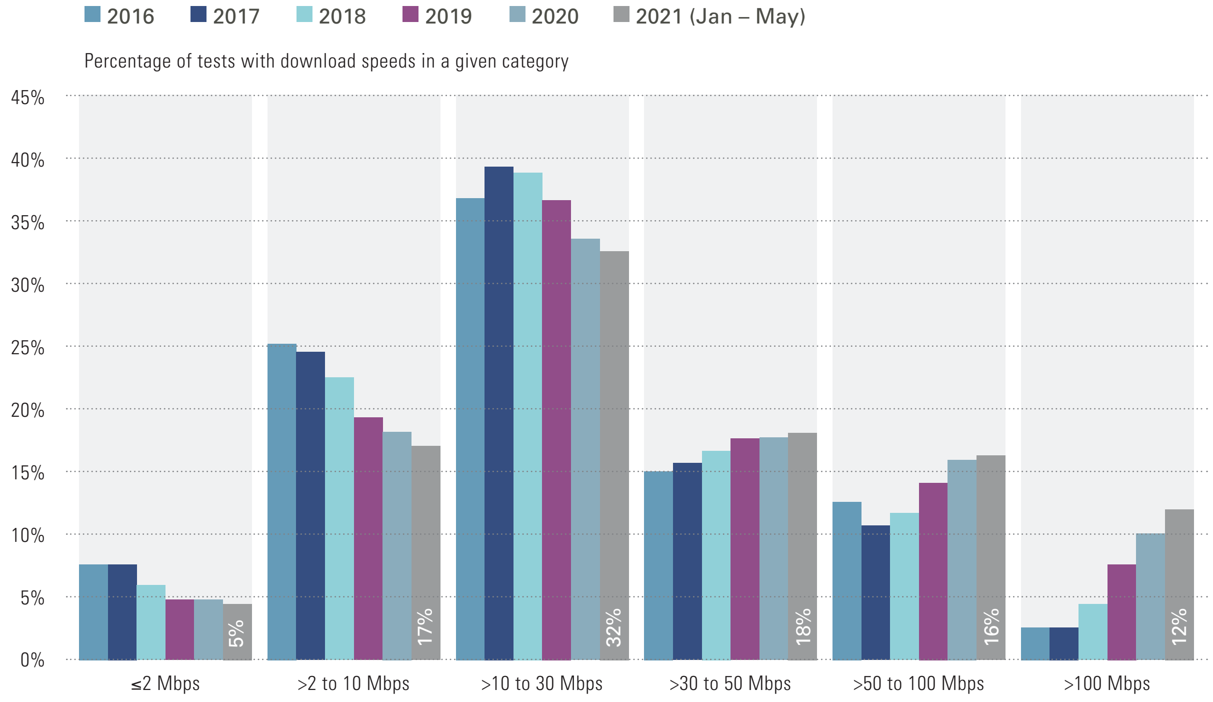
Source: RTR

[28] Data on broadband connections are collected quarterly in accordance with the Communications Survey Ordinance (KEV). M2M SIM cards are not shown in the chart. For details, see the most recent RTR Internet Monitor: https://www.rtr.at/TKP/aktuelles/publikationen/Uebersichtseite.en.html?l=de&q=&t=category%3Dinternetmonitor KEV data are available in the form of Open Data at: https://www.rtr.at/rtr/service/opendata/OD_Uebersicht.de.html

Figure 1 shows the total number of fixed and mobile broadband connections. Within mobile broadband, a distinction is made between mobile data subscriptions (without minutes and texts included) and smartphone subscriptions (with minutes and texts included). A continuous increase is seen in the number of broadband connections since 2016. The number of smartphone subscriptions in particular has risen.

Data generated with the help of the RTR-NetTest is used to assess the quality of internet access. The RTR-NetTest allows users to check the speed and quality of their internet connection, in standardised form and independently of their provider.

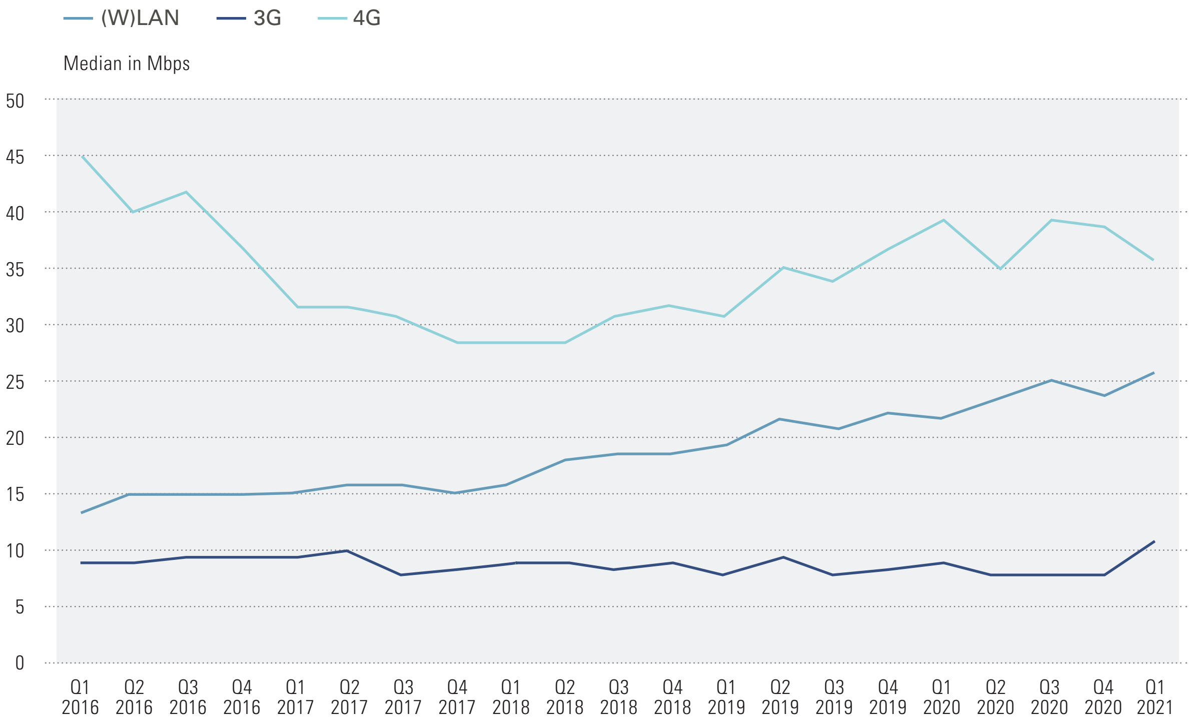
Figure 2: Distribution of download speeds



Source: RTR

Figure 2 reveals the percentages of tests with download speeds in a given category. One fact seen here is that the download speeds measured during the period under consideration range from 10 to 30 Mbps. A continuous trend is also evident, with the number of measurements below 30 Mbps receding in favour of higher bandwidths.

Figure 3: Download speed by technology



Source: RTR-NetTest

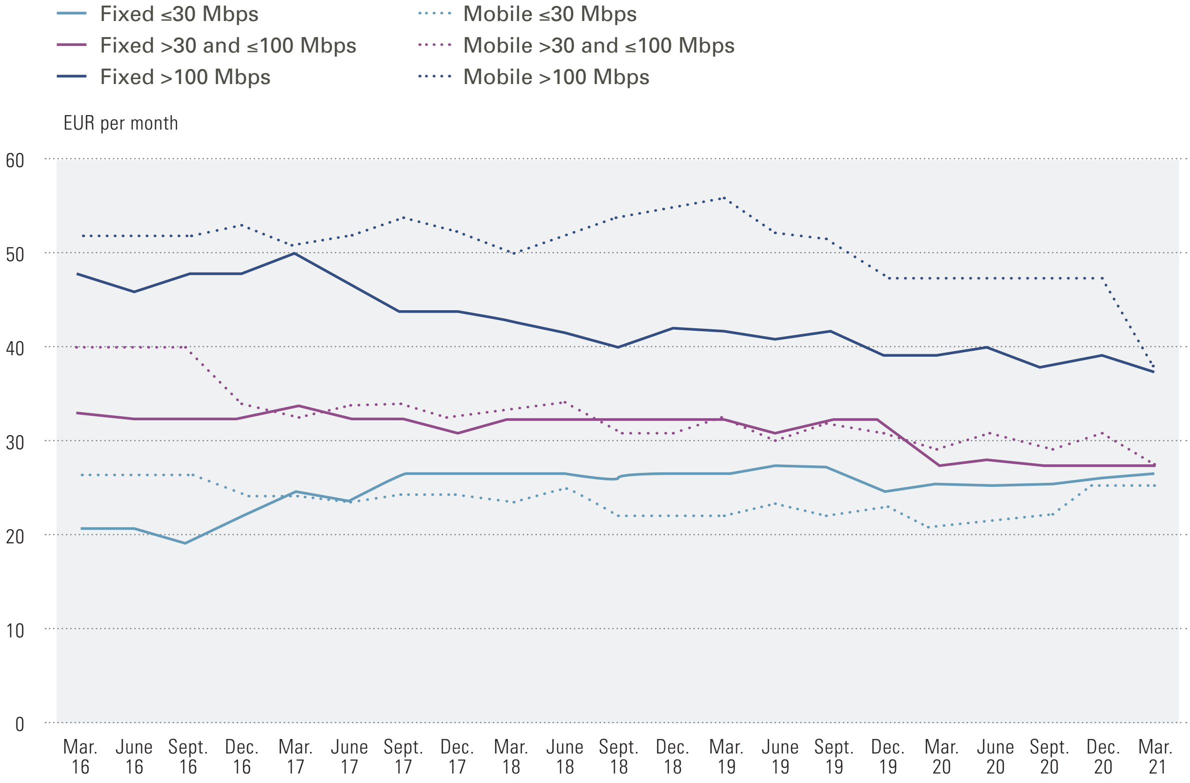
Figure 3 depicts the median[29] download speed measured with the RTR-NetTest over time, broken down by type of technology. Internet access speed depends on factors including the technology implemented. A distinction is made between 3G, 4G and various fixed and mobile network technologies. The latter were measured with the aid of a browser or app (in the case of WiFi) and have been aggregated here under the heading of (W) LAN. It can be clearly recognised that, based on median, higher download speeds can be reached with 4G mobile telecommunications technology than with (W)LAN or 3G. A continuous increase can be seen for (W) LAN, from roughly 14 Mbps in Q1 2016 to about 25 Mbps in Q1 2021. The decline in 4G download speeds, as shown in the chart, should not lead to the mistaken conclusion that connection quality has deteriorated with 4G mobile technology. Rather a cyclical component is at play here that does not contradict the global trend of higher bandwidths over time.[30] Upload speeds, broken down by technology, reveal a similar if less pronounced pattern (see figure 10, p. 58).

[29] The median is appropriate because it is located at the very centre of all (sorted) observations, i.e. 50% of measurements are above and 50% are below the median. It therefore reliably excludes the influence of outliers.

[30] With the introduction of a new mobile telecommunications technology, the capacities available at any given time generally follow a cycle that can be observed. When a new technology is introduced, there are initially free capacities available, which are then gradually utilised as a result of market competition and demand, until the next technology (often accompanied by new spectrum) in turn creates new capacities. A similar pattern is expected for 5G, while a distinction needs to be made between the stand-alone and the non-standalone versions.

Figure 4 shows price changes since the Net Neutrality Regulation became effective. This is done by contrasting three price baskets for fixed network broadband (each without TV) with three price baskets for mobile broadband (with unlimited data volumes). In both cases, the broadband categories differentiated are ≤30 Mbps, >30 to ≤100 Mbps, and >100 Mbps. The basket value is based on the least expensive product from each operator that can be included in the respective basket. A comparison of the values for March 2016 with those for March 2021 reveals a nominal rise in the price of slow fixed broadband (≤30 Mbps) while all other baskets dropped in price. The largest price decline during the period considered, of roughly 33 per cent, was seen for the basket containing mobile broadband products supporting >30 to ≤100 Mbps. A peculiar effect in Austria is the similarity in the prices of comparable bandwidths whether supplied via fixed or mobile networks. This would suggest that pressure for substitution affects both connection types equally.

Figure 4: Price baskets – fixed vs. mobile broadband



Source: RTR

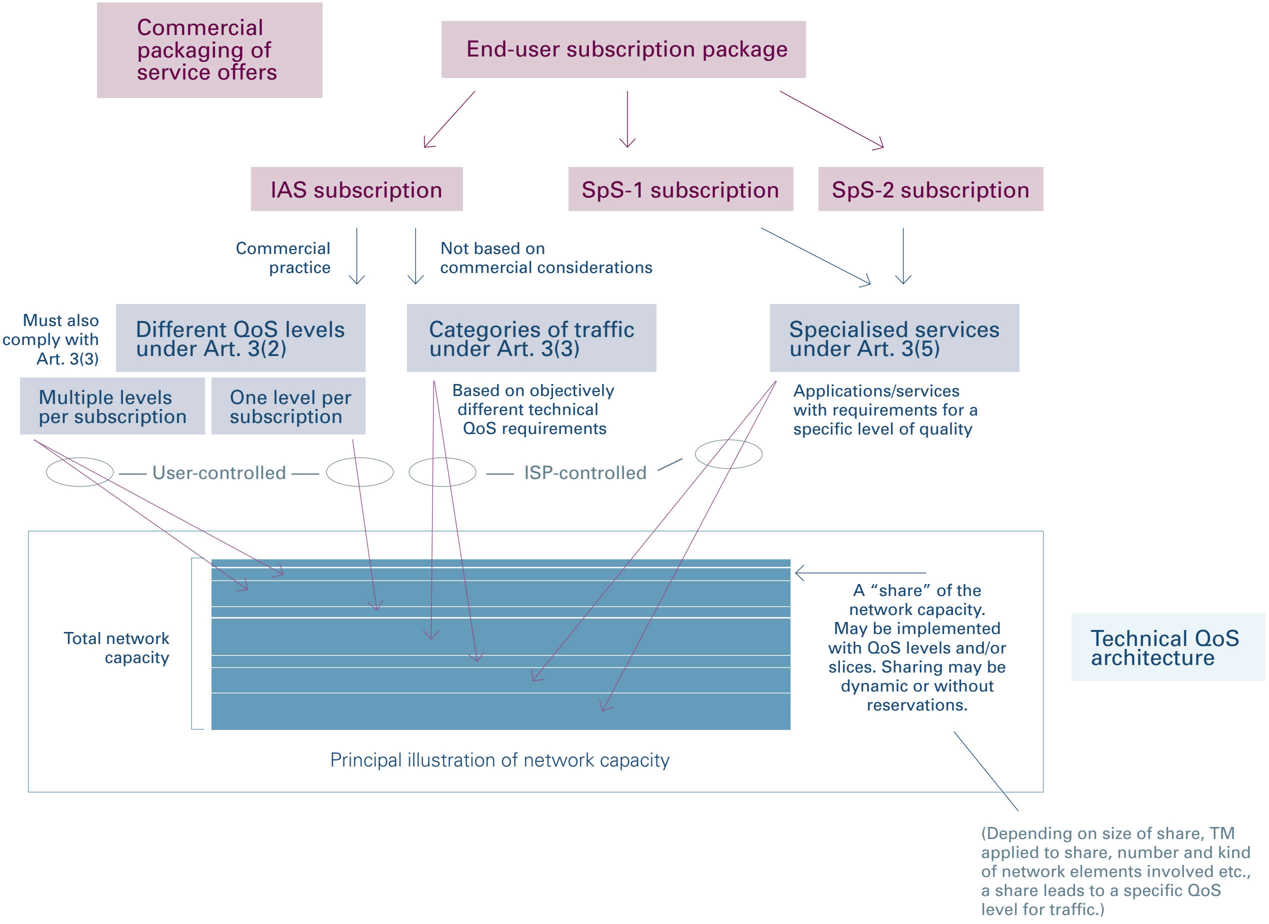
In view of the indicators above, it can be concluded that the availability of non-discriminatory internet access services at levels of quality that reflect advances in technology (requirement in Art. 5(1) Net Neutrality Regulation) was ensured in Austria over the past five years.

06 The major unknowns

6.1 QoS differentiation for a single subscription

The Net Neutrality Regulation generally obliges ISPs to treat all internet traffic equally, independently of its sender or receiver, the content retrieved or disseminated, the application or service used or provided, or the terminal equipment used. The TSM Regulation provides for several exceptions from this general rule. These are discussed in more detail below. The chart below summarises the various legal bases.

Figure 5: QoS differentiation in the TSM Regulation


Commercial packaging of service offers
End-user subscription package
IAS subscription
SpS-1 subscription
SpS-2 subscription
Commercial practice
Not based on commercial considerations
Must also comply with Art. 3(3)
Different QoS levels under Art. 3(2)
Categories of traffic under Art. 3(3)
Specialised services under Art. 3(5)
Multiple levels per subscription
One level per subscription
Based on objectively different technical QoS requirements
Applications/services with requirements for a specific level of quality
User-controlled
ISP-controlled
Total network capacity
A "share" of the network capacity. May be implemented with QoS levels and/or slices. Sharing may be dynamic or without reservations.
Principal illustration of network capacity
Technical QoS architecture
(Depending on size of share, TM applied to share, number and kind of network elements involved etc., a share leads to a specific QoS level for traffic.)

Source: BEREC Report on the outcome of the public consultation on the draft BEREC Guidelines on the Implementation of the Open Internet Regulation, BoR (20) 111.

• Applicationagnostic differentiated QoS for a single subscription

Art. 3(2) of the TSM Regulation allows a possibility for offering multiple QoS levels. ISPs are permitted to define varying technical conditions and characteristics, including price, data volume and speeds, for the various subscriptions. Similarly, ISPs can also offer multiple varying products to one and the same customer.[31] Yet this provision also allows ISPs to provide multiple varying QoS levels for one and the same subscription. This has been clearly set out in the revised BEREC Guidelines. Specifically, such products are permitted as long as the varying QoS levels are offered independently of application (on applicationagnostic terms). This means that end users must have full control over which applications transmit traffic at which QoS level. Users could do this, for example, by configuring the client application software. Another condition is that the ISP does not preselect the QoS level in which specific applications are transmitted.[32]

The RTR Telecommunications and Postal Services Division has to date not become aware of any subscriptions that have applied this differentiation. But such products apparently might be marketed in future, in the context of 5G network slicing or 4G QCI, for example.

• Traffic management based on category

Networks can be optimised based on objectively different technical quality of service requirements for specific categories of traffic. This option is allowed under Art. 3(3) second subparagraph of the TSM Regulation. Such measures must not necessarily be applicationagnostic, but they do, however, have to meet other conditions. They must be based on objective technical QoS requirements, not be oriented toward commercial interests and not be maintained for longer than necessary. Finally, such measures must not involve monitoring 'specific content.' The BEREC Guidelines explain the latter term in detail. Here, the Guidelines focus on the technical conditions for providing internet access service to current standards, including the use of carrier grade network address translation (CGNAT). Based on the distinction made here as well as on the OSI reference model,[33] it is possible to precisely monitor the specific content that needs to be assessed in order to provide such internet access service. 'Specific content' is accordingly defined as the 'transport layer protocol payload.' Such content is prohibited from use in traffic management. This is in distinction to 'generic content', which is interpreted as including the 'IP packet header' and the 'transport layer protocol header.' This means that classifications within the IP header such as 'DiffServ' may be used in practice.

The regulatory authority is not aware of any ISPs in Austria that make use of this type of traffic management. Aspects of this type of traffic management are currently being addressed at European level by the ECJ, in response to a referral from a German court.[34] A ruling is pending.

[31] Example: a user operates a dual SIM card device with two SIM cards from the same provider, one for data charged at a flat rate and the other for phone service.

[32] BoR (20) 112 Par. 34c.

[33] ITU-T X.200 (07/1994), https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=2820.

[34] ECJ C 34/20 (Telekom Deutschland).

6.2 Specialised services

Providers of electronic communications to the public are free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof (Art. 3(5) TSM Regulation). The optimisation must be technically necessary. In addition, other requirements must be met, including that of maintaining the general quality of internet access services.

As described above, one decision on a specialised service was issued in R 3/16. In this case, a video-on-demand service was denied recognition as a specialised service. Although network providers and equipment providers see specialised services as playing a more significant role in the context of 5G, such services based on 5G have not, to date, been a factor in practice.

6.3 New network blocks?

The legal status of the ISP, the internet access service provider, is in transition. For a long time, the apparent agreement was that ISPs merely had the job of transporting data through their networks, without bothering with content. The EU e-Commerce Directive, unamended since 2000, continues to hold access providers exempt from liability when acting as a 'mere conduit' for data traffic. Yet, some things have changed since then. While the e-Commerce Directive is expected to be replaced or supplemented by the Digital Services Act, an increasing number of EU rules now provide for network blocking. Such rules empower specified parties to approach ISPs in order to request blocking of certain types of online content. This contrasts with the Net Neutrality Regulation, which prohibits ISPs from blocking data traffic. The murky legal situation in regard to copyright law provided frequent occasions in the past for rights owners and ISPs to appeal to the high courts, petitioning for clarification of their rights and obligations. With the diverse fundamental rights of numerous parties being affected, the situation is complex. Among the issues is whether private businesses are to be allowed or required to decide the content that internet users consume. Other issues relate to controls and to designing procedures in a way that adequately considers the rights of all those involved. In certain other legal areas, provisions for network blocking exist, while in still other areas such provisions are being discussed. In light of this fact, we should address the basic issue of whether it might not be expedient to concentrate these responsibilities with a single authority, one having the necessary related competency and that is capable of ensuring a uniform approach to the issue. Network blocking directly affects net neutrality. This implies the need to develop overarching, holistic policies that take all aspects into account: the justified interests of the parties affected in ensuring expeditious, efficient removal of illegal content; and the protection of the open internet, which serves as a vital pillar of a society increasingly dependent on digital technology.

02

Part II
Reporting period
1 May 2020 – 30 April 2021

01 Stakeholders and institutions in enforcement

This *fifth* Annual Report on *Net Neutrality* from the Austrian Regulatory Authority for Broadcasting and Telecommunications addresses the same major topics as covered in last year's report, and aims to provide readers with 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 2020 to 30 April 2021, inclusive) to ensure the openness of the internet? What are the new product developments that, while potentially offering advantages for consumers, at the same time potentially harbour risks for the future sustainability of the internet?

As in the past, internet service providers (ISPs) continue to be the group primarily targeted by net neutrality provisions. The main concern of the EU Regulation is to keep pace with changing technical capabilities and support the potential new business models developed by ISPs, while avoiding any limiting of the internet's innovative power. The TSM Regulation accordingly identifies business practices, technical measures and obligations (such as ensuring transparency for end users) that are required or prohibited in order to uphold net neutrality. Besides ISPs, the Regulation both empowers and addresses in particular end users, meaning private citizens and businesses as well as providers of content, services or applications. These groups are entitled to free access to an open internet.

In Austria, the Telekom-Control-Kommission (TKK) and Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) are responsible for enforcing the TSM Regulation. 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. Another aspect, relating to net neutrality, is the continued requirement for general terms of business and fee provisions to be submitted to RTR before commencement of the service. The TKK may prohibit the application of general terms of business if they contravene the Telecommunications Act or certain consumer protection regulations. All relevant changes in contract conditions (including those that affect net neutrality) must be submitted to the regulatory authority. These 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 – even though breaches of other provisions of the TSM Regulation can only be prohibited ex post. What is more, the regulatory authority can impose reporting requirements on a company, which can help to improve estimates of the impact on the market.

RTR is a convergent telecoms, postal and media organisation, and its Telecommunications and Postal Services Division and Media Division consult both mutually and with the TKK and the Austrian Communications Authority (KommAustria) on all key issues relating to net neutrality. This is also relevant in the context of net neutrality issues (such as zero-rating or specialised services), since these may also exhibit an overlap with media topics.

The present annual report stems from an obligation imposed on the European national regulatory authorities (NRAs) by the TSM Regulation. One aim of this obligation is to achieve an approach to the application of the provisions of net neutrality that is as consistent as possible.

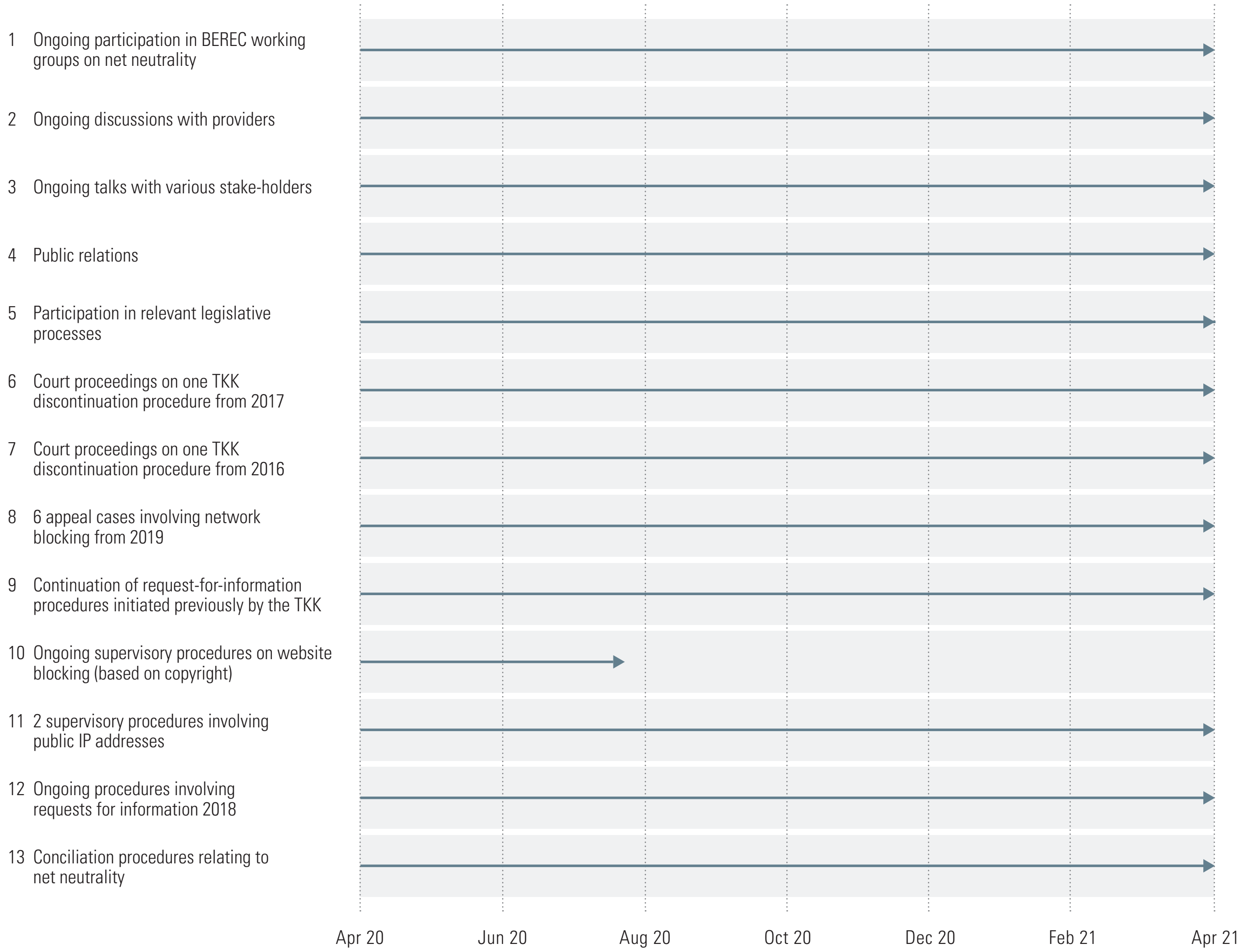
In the work it conducts with ISPs, the regulatory authority continues to uphold the principle of identifying breaches of the TSM Regulation (monitoring) while raising awareness for the topic among ISPs, so as to ultimately create a stable environment for entrepreneurial activity and innovation. Where breaches of net neutrality rules are found, the authority envisages appropriate transition periods for their resolution – which also permit companies to adjust to the new legal standards without experiencing disruptive interventions.

Furthermore, net neutrality is a topic that must always be approached in awareness of changes over time. Increasingly, questions are now arising about the implementation of net neutrality concepts in the context of the fifth-generation mobile network standard (5G). Other questions address resource distribution across virtual network elements (network slicing) and the classification of such elements within the scope of the TSM Regulation.

Section 2 presents the reader with a chronological overview of the national regulatory authority's activities, while measures to safeguard net neutrality are presented in section 3. Section 4 takes a look at other monitoring systems in relation to net neutrality and provides a set of key figures that describe the development of the internet in Austria. The last part of the report, section 5, presents a brief summary of the projects and challenges expected in the next reporting year.

02 Timeline of regulatory authority activities

Figure 6: Timeline of events in the reporting period



Source: RTR

Figure 6 shows the chronological sequence of relevant events in the reporting period (May 2020 – April 2021). The table below gives an overview of these events, with a brief description as well as some historical context. Further details about these procedures can be found in Part II section 3.

Table 1: Timeline of events in the reporting period

Work in EU bodies		
1	Current	Participation in the BEREC working group on the open internet/net neutrality Topics in 2020: Carry-over work on update to the Guidelines on the Implementation of the Open Internet Regulation, Report on the implementation of Regulation (EU) 2015/2120 and BEREC Guidelines on the Implementation of the Open Internet Regulation, NRA deployment support and sharing of practical experiences with the Net Neutrality measurement tool, Report on COVID-19 crisis Topics in 2021: Report on the implementation of Regulation (EU) 2015/2120 and BEREC Guidelines on the implementation of the Open Internet Regulation, Collaboration on the Net Neutrality Measurement tools and evolution of the regulatory assessment methodology, Report on the Internet Value Chain, Report on COVID-19 crisis
National status quo analysis/discussion with ISPs		
2	Current	Discussions with providers on the topic of net neutrality
3	Current	Talks with various stakeholders
4	Current	Public relations
5	Current	Participation in relevant legislative processes
Enforcement of TSM Regulation		
3	Dec. 2017 – Apr. 2021	One of the discontinuation procedures initiated by the TKK against the five largest providers was rejected as unfounded by the Federal Administrative Court (BVwG); the right to appeal was granted. In June 2020, the ISP appealed to the Supreme Administrative Court (VwGH), submitting a petition to recognise the suspensory effect.
4	Feb. 2019 – Apr. 2021	Continuation by the RTR Telecommunications and Postal Services Division of the request-for-information procedures initiated previously by the TKK against eleven ISPs. While most procedures were terminated by January 2020, the implementation deadline (until 2022) for one is still open (for further details, see Part II section 3).
5	April 2019 – April 2021	The TKK issues assessment decisions in order to prohibit the use of certain network blocks. In 2020 the BVwG overturns the TKK's decisions. Following appeals lodged by the TKK, the VwGH then overturns the decisions issued by the BVwG. The TKK's decisions are reinstated and are now final.
5	Since Aug. 2019	Ongoing TKK procedure from its 2018 request-for-information procedures according to Art. 5(1) of the TSM Regulation (for further details, see Part II section 3).
6	Dec. 2019 – July 2020	The TKK conducted two supervisory procedures on the topic of website blocks (copyright law) in accordance with Art. 5 of the TSM Regulation. The procedure concerned the legitimacy of blocking access to certain websites as a result of injunction claims based on copyright (see Part II section 3 for further details).
7	June 2020	The TKK issues a decision against one ISP, relating to the admissibility of access blocks for certain websites as a result of injunction claims based on copyright law. The decision is final (see Part II section 3 for details).
8	July 2020	The TKK issues a decision against one ISP, relating to the admissibility of access blocks for certain websites as a result of injunction claims based on copyright law. The decision is final (see Part II section 3 for details).
9	April 2021	The TKK drops a supervisory procedure against a provider relating to failure to assign (at least) a dynamic public IPv4 address to end users.
10	April 2021	The TKK issues a decision against a provider relating to failure to assign (at least) a dynamic public IPv4 address to end users.

03 Safeguarding net neutrality and supervisory measures

On the entry into force of the TSM Regulation, the regulatory authority promptly began audits of products already offered on the market, and 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 affected ISP appealed to the VwGH in this matter, submitting a petition to recognise the suspensory effect. Another procedure has been pending with the BVwG since December 2017. In April 2021, a decision was issued against another ISP (further details in Part II, section 3.2). 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. As already stated in the 2020 report, the procedures completed in the reporting period were able to identify technical and commercial practices that were problematic in light of the provisions of Art. 3 of the TSM Regulation and therefore required investigation.

Table 2: Summary of problematic practices in light of the TSM Regulation

Type of practice	Description
1. Port blocking	Certain UDP or TCP ports are blocked for incoming and/or outgoing traffic. This might render certain services unusable, which is a contravention of Art. 3(1) and Art. 3(3) of the TSM Regulation. A more detailed description is given in Part II section 3.1.
2. 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 Part II section 3.2.
3. Zero-rating	The data volume used by a specific application or for a specific CAP is not counted towards the data volume cap included in the customer's subscription. A more detailed description is given in Part II section 3.3.
4. 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.
5. 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.
6. Disconnection of IP connections	Automated disconnection of IP connections restricts the rights of the end user to use or provide their own services (Art. 3(1) TSM Regulation).
7. Network blocks and copyright law	Even though jurisdiction for ruling on injunction claims based on copyright normally lies with the ordinary courts, the specific traffic management measures (blocks) used to implement such orders must be verified to ensure compliance with the TSM Regulation. Where such traffic management measures are implemented simply because the ISP has been asked to do so by copyright holders (and not as a result of a court order), it is also necessary verify whether an exception exists under point (a) of Art. 3(3) third subparagraph TSM Regulation. A more detailed description is given in Part II section 3.4.

In a continuation of earlier work aimed at monitoring compliance with the TSM Regulation, many smaller-scale fixed and mobile operators were audited. A total of twelve ISPs were selected, to whom questionnaires requesting information about products and technical practices were sent. This procedure was initiated some time ago, between February 2019 and July 2019. Corresponding answers from the ISPs are available for all of these procedures. On a positive note, we once again emphasise numerous ISPs' continuing readiness to cooperate, without the need for a formal supervisory procedure. As a result, only one of these procedures was pending at the end of the current reporting period. For this procedure, a longer implementation period applies for technical changes aimed at ensuring compliance with the TSM Regulation. All other request-for-information procedures had been terminated, although two only after submitting 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. By the end of the reporting period, six ISPs had taken corrective action after being notified of the relevant deficiencies (e.g. port blocks had been lifted or public IP addresses would be assigned in future; four separate procedures resulted after one MVNO had formed separate companies for their separate brand identities. One MVNO required a longer period of time to make the necessary changes and this extension was granted. 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, both operating in the lowend segment. While the two MVNOs sought in the request-for-information procedures to contest their obligation to assign public IP addresses, this was abandoned after the initiation of the supervisory procedures. One MVNO has since enabled the assignment of public IP addresses to their customers. Following a technical audit, the TKK's supervisory procedure against this MVNO was discontinued in April 2021. In April 2021, the TKK issued a decision against the second MVNO as a result of failing to assign public IP addresses to end users. Both procedures were very time-consuming, since technical audits needed to be performed on a regular basis.

In this reporting year, the regulatory authority again addressed issues involving the handling of blocks placed on domains as a result of claims made by copyright holders because the sites operated using these domains/ IP addresses were structurally in breach of copyright law. Specifically, this involved verifying compliance with point (a) of Art. 3(3) third subparagraph TSM Regulation concerning the blocking of content (websites) in response to copyright claims, or the applicability of provisions granting exceptions. Even though courts of law are authorised to issue such copyright injunctions, the specific traffic management measures (blocks) used to implement the orders must be verified to ensure compliance with the TSM Regulation. Where such traffic management measures are implemented simply because the ISP has been asked to do so by copyright holders (and not as a result of a court order), it is also necessary to verify whether an exception based on the TSM Regulation exists. Whether the copyright holder has a valid claim is a preliminary issue in this evaluation. A detailed description of these activities is provided in Part II section 3.4.

Alongside activities previously described as part of the stated procedures concerning existing products, general terms of business and fee provisions were also reviewed for compliance with the TSM Regulation pursuant to the authority's statutory role in reviewing contract terms (Art. 25 Par. 6 TKG 2003).

With respect to the minimum content of contracts as required in Art. 4(1) of the TSM Regulation, in formal procedures no immediate steps, based on the TSM Regulation, needed to be taken in the reporting period: inclusion of this content is meanwhile common practice.

3.1 Port blocking

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.

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.

The following section offers a summary of selected previous outcomes.

Port 22 (SSH)

One fixed network operator blocks this port for use by specific internet access technologies for technical reasons based on their network topology (CPE maintenance). The ISP honoured their commitment to replace the affected modem, which meant the block could be lifted.

TCP port 23 (Telnet)

One mobile operator confirmed blocking incoming traffic on TCP port 23. This action was justified by citing vulnerabilities in the hardware used by end users. The block was removed after replacing this hardware.

TCP port 25 (SMTP)

One mobile network operator and several fixed network operators stated that they block outgoing traffic 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, these blocks were considered to be legitimate – as they had been 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 IPs.

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

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

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

TCP ports 137 – 139 bidirectional (NetBIOS)

One fixed network operator 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 443 incoming (HTTPS)

One fixed network operator reported blocking incoming traffic on TCP port 443.
This block could be lifted after migration to new hardware.

TCP port 445 incoming (SMB)

One fixed network operator blocks this port for incoming traffic on account of security concerns in relation to end users. In the case of the other fixed network operator, 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 operator 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 operator 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 until early 2022 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.

3.2 Private IP addresses and services

The Net Neutrality 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, customers are occasionally assigned private IP addresses (using NAT). However, if multiple customers are required to share a single private IP address via NAT, this effectively prohibits any individual customer from providing services or content themselves. For this reason, all end users have the right to a public dynamic IP address, which is to be provided without charge.

The last reporting period had shown that this problem is especially common with mobile network operators, and especially with MVNOs. Supervisory procedures in this context were initiated against two MVNOs in August 2019. After lengthy deliberation, one MVNO finally managed to provide their customers with a public IPv4 address on request. In the case of the second MVNO, the telecommunications regulator issued a decision whereby the MVNO must now provide customers using this ISP for internet access with a public IP address (IPv4 address) on request.[35] A surcharge must not be charged for the provision of this address.

Problems in this area will continue to occupy RTR's attention in the future, since the regulatory authority continues to receive enquiries from end users in this context on a regular basis.

3.3 Monitoring zero-rating

Pursuant to Art. 5(2) of the Net Neutrality Regulation, NRAs may request information from ISPs in relation to the objectives of this regulation. In consideration of the importance of this topic for competition – also in downstream markets – and the widespread use of zero-rating, the RTR Telecommunications and Postal Services Division therefore analyses the most important key figures for zero-rating on a twice-yearly basis.

As of June 2021, three providers offer zero-rating products: A1 Telekom Austria AG (within their core brand plus the associated brands Kurier mobil, Krone mobile, Educom, Yesss! and Georg), Hutchison Drei Austria GmbH and – for the first time in this reporting period – T-Mobile Austria GmbH.

A1 Telekom Austria AG (including all of their brands) offers new customers a total of 27 separate tariff plans with bundled zero-rating products as well as 9 'extra plans' (i.e. zero-rating products that can be added to the main plan for a fee). As the customer base of A1 Telekom Austria AG brands is small in comparison with the core brand and only a small number of customers make use of the optional zero-rating products, the further analysis presented here does not examine these subbrands and extra plans separately.

A1 Telekom Austria AG offers zero-rating as part of almost all of their new plans. Excluded from the above are only those tariff plans which already include unlimited data volumes and are therefore irrelevant for zero-rating. Accordingly, A1 Telekom Austria AG offers new private customers and new business customers of their core brand a total of nine tariff plans and eight tariff plans with zero-rating, respectively. Also with previous subscription plans not including zero-rating, the option of using zero-rating also exists in the form of an add-on package. Specifically, A1 Telekom Austria AG has structured their zero-rating offer around the five zero-rated categories of music, video, chat, social media and gaming. The offer is open, meaning any of a CAP's applications that can be allocated to one of the five categories can be included in the zero-rating offer. This makes the application accessible to end users without the data usage incurred by the service being deducted from the data included in users' subscriptions. The wholesale offer of A1 Telekom Austria AG is thus basically open, which the authority rates positively. Reports to the NRA of accessibility problems affecting CAP services – and therefore downstream markets – were again absent in the 2020/2021 reporting year. No technical changes

[35] TKK 7 April 2021 R 9/19 https://www.rtr.at/TKP/aktuelles/entscheidungen/entscheidungen/R9_19.de.html

affecting service providers/CAPs were made in the reporting year. The number of business customers of the A1 core brand making use of tariff plans with zero-rating products increased by around 29 per cent from April 2020 to April 2021; the comparable share of private customers of the A1 core brand rose by around 26 per cent. In the fourth quarter of 2019, roughly 12 per cent of all smartphone plan and data subscription customers of the A1 core brand had a plan that included zero-rating; this proportion rose to 15 per cent in Q4 2020 of the year under review.

Table 3 provides an overview of the tariff plans offered with zero-rating as well as their categories. In the case of plans from A1 Telekom Austria AG, it is clear that zero-rated chat services are now offered in almost every plan with zero-rating, while zero-rated video streaming services are offered only in higher-priced plans. Unlike the 2019/2020 reporting year, the gaming category is no longer limited to plans for young people but is now available in higher-priced business plans.

Table 3: Categories included in zero-rating tariff plans[36]

Providers	Tariff plan	Music	Video	Chat	Social/ Social media	Gaming	Social and Chat
A1	Xcite S	x		x			
A1	SIMply Xcite S			x			
A1	Xcite L	x		x	x		
A1	SIMply Xcite L			x			
A1	Mobil S	x		x			
A1	Mobil L	x		x	x		
A1	SIMply S			x			
A1	SIMply L			x			
A1	5GigaMobil S	x	x	x	x		
A1	Business 5GigaMobil S	x	x	x	x	x	
A1	Business 5GigaMobil M	x	x	x	x	x	
A1	Business Mobil S	x					
A1	Business Mobil M	x		x			
A1	Business Mobil L	x	x	x			
A1	Business Mobil Pur S	x					
A1	Business Mobil Pur M	x		x			
A1	Business Mobil Pur L	x	x	x			
Drei	MyLife (SIM) M	x		x			
Drei	MyLife (SIM) L	x		x	x		
Drei	MyLife (SIM) XL	x	x	x	x		
T-Mobile	Mobile S						x
T-Mobile	Mobile M	x					x
T-Mobile	Mobile L	x	x				x
T-Mobile	Youth S						x
T-Mobile	Youth M	x					x
T-Mobile	Youth L	x	x				x

Source: RTR internet research, 11 June 2021

[36] Figures include plans with zero-rating available to new customers. In the case of changes to the zero-rating products included, the zero-rating products are reported as included at the time the survey was conducted (figures from June 2021).

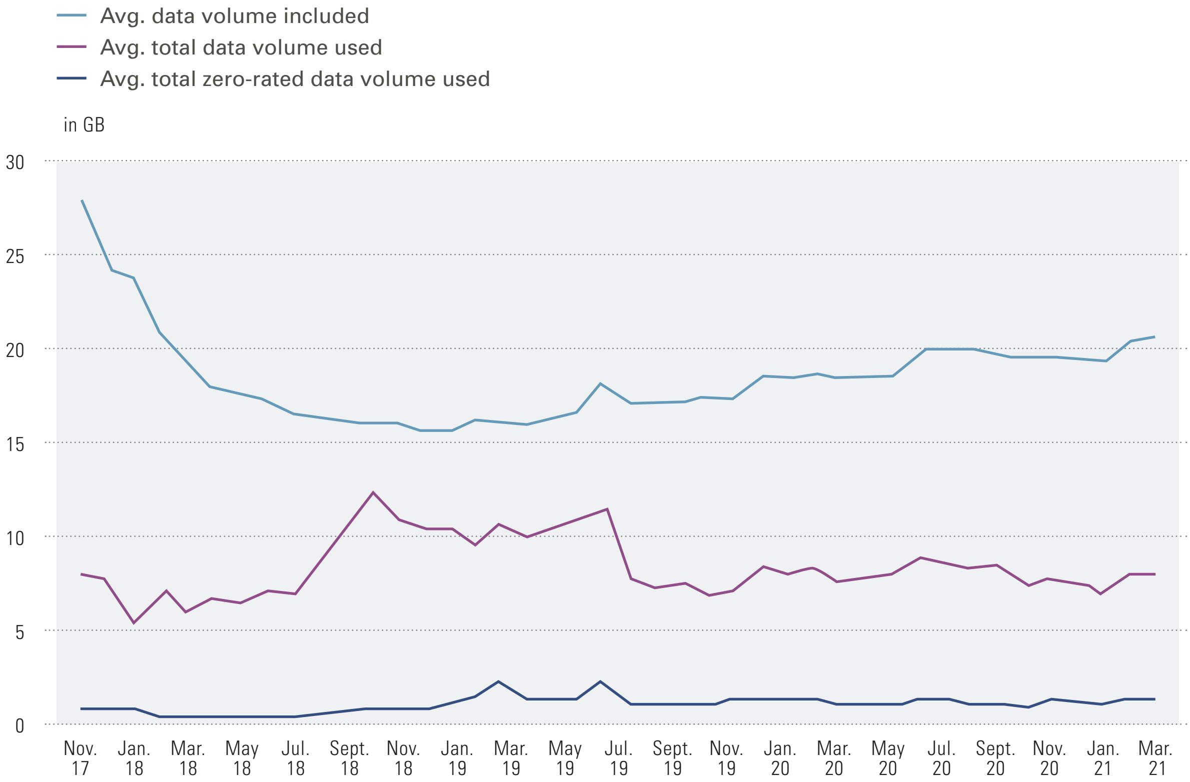
Hutchison Drei Austria GmbH was the second provider with zero-rating products and offers new customers three tariff plans (including their SIM-only versions) that include zero-rating: all of these are youth plans aimed at individuals aged 27 and under. The wholesale portfolio for tariff plans with zero-rating is essentially open – a fact approved of by the NRA. No technical changes affecting service providers/CAPs were made in the reporting year. The provider has structured their zero-rating portfolio into the four separate categories of music, video, chat and social. The chat category is zero-rated in every tariff plan, while the video category is included only in the higher-priced tariff plans. In the fourth quarter of 2020, less than 5 per cent of all smartphone and data subscription customers of Hutchison Drei Austria GmbH had a plan with zero-rating.

Hutchison Drei Austria GmbH also offers a zero-rated Spotify add-on as well as their own zero-rated services (3 Cloud and 3 Kiosk). The 3 Film product was discontinued during the 2020/2021 reporting year. The 3 TV product is included in the video category. In terms of active subscribers, customers for the additional packages offered by Hutchison Drei Austria GmbH also make up a low percentage of the overall number of subscribers to tariff plans with zero-rating and are therefore not analysed further.

As the third provider with zero-rating products, T-Mobile Austria GmbH launched tariff plans with zero-rating in the 2020/2021 reporting year. The portfolio is essentially open – a fact approved of by the NRA. As zero-rating was introduced late in 2020, no technical changes affecting service providers/CAPs were made in the reporting year. The provider has structured their zero-rating portfolio into the three separate categories of music, video, and 'social and chat.' The 'social and chat' category is provided at no charge to customers subscribing to any of the plans listed. Similarly to A1 Telekom Austria AG and Hutchison Drei Austria GmbH, the video category is included only with higher-priced tariff plans. The zero-rating portfolio from T-Mobile Austria GmbH has been available only for a few months and the proportion of subscribers was under 1 per cent in Q4 2020.

As part of the monitoring of zero-rating pursuant to Art. 3(2) of the Net Neutrality Regulation, aggregated data are collected about the use of plans with zero-rating and options. Such data enable a more precise assessment of the 'pull' created by zero-rating products, i.e. the appeal of such offers to customers. In essence this means assessing whether the offer limits consumers' freedom of choice (over the short or long term) and whether consumers retain the capability of additionally choosing other offers, thus maintaining access to future innovations and not limiting the innovation process.

Figure 7: Data volumes in plans that include zero-rating products[37]

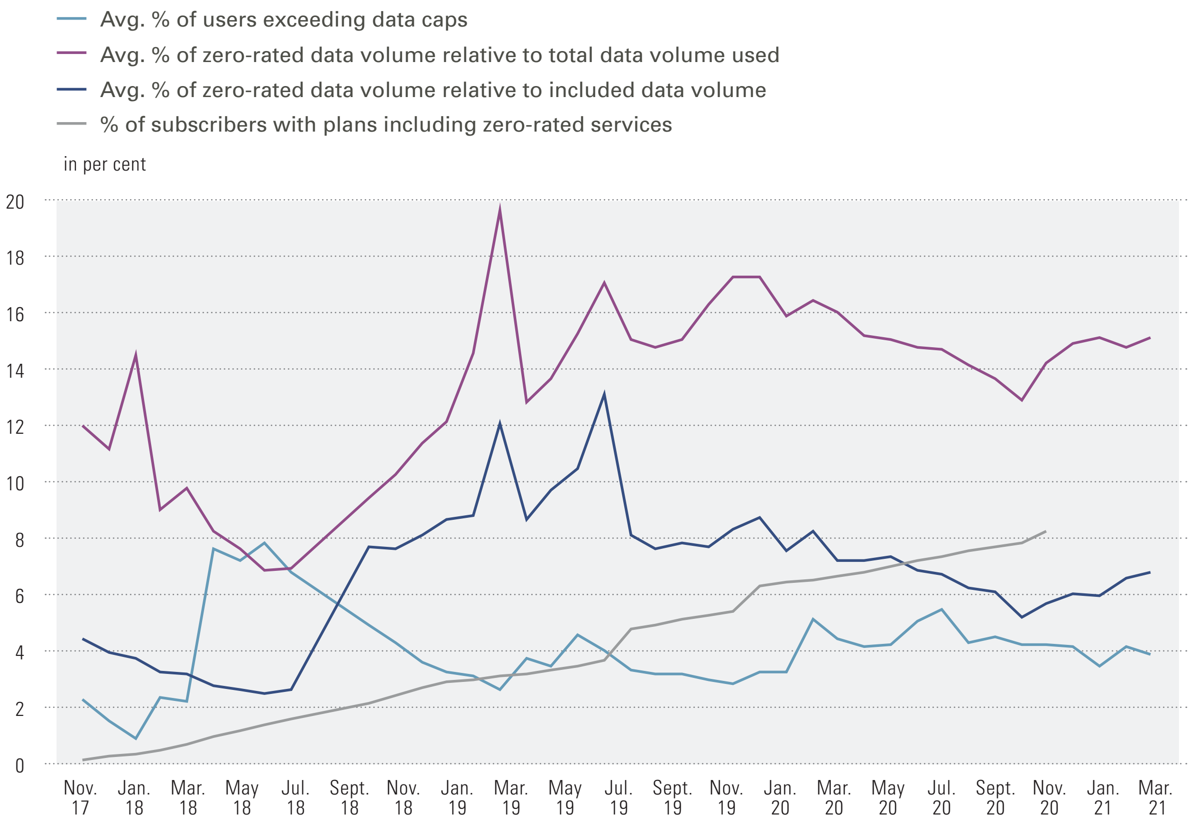


Source: RTR

Figure 7 shows the average data volume included in tariff plans with zero-rating products over time. In the 2020/2021 reporting year, this volume rose to almost 21 GB, also as a result of the introduction of higher-priced business customer plans with a higher inclusive volume, which also make the 'video' category available to customers at no charge. This is a further indication that providers, as part of an upselling strategy, can use zero-rating in the form of an add-on to distinguish themselves from competitors. Such an add-on might also be an interim step to flatrate tariff plans. The chart also shows that the average total volume of data consumed per month in the 2020/2021 reporting year was approx. 8 GB, while the average zero-rated data volume used (consumed) per month was approx. 1.5 GB. In the case of plans with a higher volume of included data, however, the latter figure did rise as high as 12 GB per month in the reporting year.

[37] The data take into account tariff plans including zero-rating that are offered under the core brands of A1 Telekom Austria AG (private and business tariff plans), Hutchison Drei Austria GmbH and T-Mobile Austria GmbH.

Figure 8: Relationships among tariff plans including zero-rating products[38]



Source: RTR survey

Figure 8 shows the proportion of subscribers to smartphone plans and data subscriptions that include zero-rating products.[39] Clearly visible is a gradual rise to approx. 8 per cent by December 2020: tariff plans that include zero-rating are now reaching more and more users. The average proportion of zero-rated data volume consumed compared with the total data volume consumed was 15 per cent in April 2021.

[38] The data take into account tariff plans including zero-rating that are offered under the core brands of A1 Telekom Austria AG (private and business tariff plans), Hutchison Drei Austria GmbH and T-Mobile Austria GmbH.

[39] These figures are based on the number of subscribers to smartphone plans and data subscriptions offered by A1 Telekom Austria AG, Hutchison Drei Austria GmbH and T-Mobile Austria GmbH.

The average zero-rated data volume consumed as a proportion of the included data volume is a key figure for assessing competition in an upstream context. This applies especially to the (transaction) costs incurred when subscribing to one of the relevant zero-rated categories: is a user able to switch from zero-rated services to non-zero-rated services outside the category without a fee or any other switching barrier? In April 2021, the average zero-rated data volume consumed as a proportion of the included data volume amounted to approx. 7 per cent. In some youth plans, however, this volume exceeded 30 per cent in the reporting year. For the majority of users, switching services is therefore a simple matter, although the user must not have exceeded or be about to exceed their data cap before the switch is made. While only 4 per cent of users exceeded their caps on a monthly basis across all plans in the reporting year (despite Covid-19), this figure was more than 25 per cent in some youth plans. Nonetheless, in proportion to the included volumes, the average volume included in each tariff plan is significantly above the average zero-rated volume consumed. In other words, when averaged over all customers, the zero-rated volumes utilised within tariff plans could also be easily covered through the data included in the plans. Ultimately, this state of affairs does not highlight any developments of concern to date that could hinder innovation.

To achieve a more nuanced view of the wholesale market for the services in these categories, the following section considers trends for average data volumes consumed in zero-rated categories in private consumer plans offered by the A1 core brand. During the 2020/2021 reporting year, average data consumption in the 'social media' category rose from approx. 2 GB in April 2020 to approx. 3.5 GB in April 2021. This category comprises the Facebook, Instagram and TikTok services – the latter being a new addition in this reporting year. Here, youth plans and plans with a higher data cap consistently exhibit a higher average level of consumption. Data consumption in the 'chat' category (comprising Facebook Messenger, SnapChat, Viber and WhatsApp) declined in the reporting year to 0.4 GB in April 2020. The categories of 'video' (comprising 20 services such as Amazon Prime Video, Netflix and Zappn) and 'music' (18 services, such as Apple Music and Spotify) remained at a similar level year on year, at 1 GB and 0.2 GB, respectively. These values depend to an extent on the popularity of the zero-rated services in the categories, conditions for entering and exiting services, and changes to the structure of a specific service (such as the increasingly data-rich use of an individual service as a result of videos and images). From a user perspective, it is certainly beneficial when the zero-rated services offered are also the services they use most often. In these dynamic markets, however, the success of individual service providers/CAPs is subject to constant and potentially disruptive change. The extent to which zero-rated services actually do distort the market (directly or indirectly) – and put services outside the category at a competitive disadvantage – may well be a topic for later investigation. In any case, such effects are mitigated by the fact that ISPs support access to categories, with ISPs serving as application-neutral platforms mediating between CAPs and end users. Accordingly, the RTR Telecommunications and Postal Services Division actively monitors category entry barriers for CAPs.

In a separate analysis, an investigation into pricing trends in private consumer plans including zero-rating products from the A1 core brand shows that the average fee (weighted by subscriber numbers) in the 2020/2021 reporting year fell slightly to EUR 38. However, the price per GB is the key figure when it comes to the potential market distortion that could end up affecting services outside the category. This held steady in the reporting year at around EUR 3 for private consumer plans in the A1 core brand. To a considerable degree, however, this value reflects older plans no longer offered to new customers, with very low volumes of included data and so a high price per GB. In youth plans, the price per GB ranges from EUR 1 to EUR 2. A systematic trend towards a higher average price per GB cannot therefore be identified.

A glance at the monthly subscription survey by the Vienna Chamber of Labour clearly reveals sufficient alternative offers for customers.[40] In addition, the three providers A1 Telekom Austria AG, Hutchison Drei Austria GmbH and T-Mobile Austria GmbH also offer several smartphone subscriptions with included data that, although mostly in the higher price segment, nonetheless typically saw a (modest) increase in subscriber numbers in the 2020/2021 reporting year. While MVNOs now also offer plans with included data volumes, they do not offer zero-rating products. This is probably attributable to the situation that MVNOs incur variable costs for the data volume that they source from their host MNOs. Further monitoring is needed to ascertain whether this will work to hinder competition in the mobile retail market.

[40] https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/FestnetzundVoIP/Die_AK-Tarifwegweiser.html

In summary, the availability of zero-rating offers in the Austrian market is continuing to increase. Yet included data volumes are not decreasing. There is no indication that zero-rating in the 2020/2021 reporting year constituted a threat to end customers, to competition or to the underlying process of innovation for services and applications. This is shown by findings including: a non-disadvantageous pricing trend, the low zero-rated data volumes as a proportion of the data cap, the low incidence of data caps being exceeded and – most importantly – the ease of access for service providers/CAPs to the categories offered by providers.

3.4 Network blocking

ISPs are generally not permitted to block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services or categories of the same, subject to the exceptions set forth in the TSM Regulation. Thus, the listed measures can be taken insofar and for as long as they are necessary to comply with other specified legislation. As a result, network blocks are generally prohibited except where a specific law requires ISPs to set them.

In copyright law, there is a special provision according to which ISPs can also be obliged to block access to websites that structurally breach the law, if these sites have previously been duly warned by the rights holder (holder of copyright or intellectual property rights). A website in 'structural breach' of the law is a website that infringes copyright law, not only in isolated cases but systematically and regularly. One example of this is when website operators contribute to the mass distribution of illegal copies of copyrighted works by providing an indexed BitTorrent file to allow users to more easily locate titles of works they are looking for.[41]

Before granting to a rights holder an injunction against an ISP, various basic rights first need to be considered.[42] Assessing a claim of entitlement to network blocking entails weighing two sets of rights: on the one hand, the right of the copyright holder requesting the injunction, to protection of intellectual property and to effective enforcement of the law; and the fundamental rights of internet users, website operators and the access provider involved in the procedure, to freedom of expression, freedom of information and freedom to conduct a business.[43] Since consideration of such fundamental rights is intrinsic to the assessment of such claims, this provision therefore constitutes an exception as provided for by the Net Neutrality Regulation.[44] If an ISP sets a net block that accords with these claims, this does not violate the terms of the TSM Regulation.

• Network blocking in the period under review

In the period between early 2020 and April 2021, the TKK initiated two supervisory procedures against ISPs suspected of having already set up network blocks for certain websites. In the course of the proceedings, the ISPs stated that the network blocks had been set up in response to legal warnings from rights holders.

Even though jurisdiction for ruling on injunction claims based on copyright normally lies with the ordinary courts, the regulatory authority is responsible for verifying any traffic management measures to determine whether the specific implementation in the form of accessblocking is compatible with the TSM Regulation. Any exception pursuant to the TSM Regulation must also be verified where traffic management measures of this kind are taken by providers of internet access services after a warning by rights holders but without a corresponding court ruling. The supervisory procedures referred to here were concluded with a decision that provided a detailed assessment of the topic, including any Austrian Supreme Court (OGH) and ECJ caselaw rulings available when the particular decision was issued.

[41] OGH 24 October 2017, 4 Ob 121/17y; TKK 28 November 2018, R 1-5, 8, 9/18; 12 April 2018, R 1-6/19; 9 July 2019, R 7/19; 22 October 2019, R 8/19; 19 August 2019, p. 1-5, 8, 10, 13/19; 17 March 2020, R 11-14/19.

[42] ECJ 27 March 2014, C-314/12, UPC Telekabel Wien/Constantin Film Verleih et al.

[43] OGH 14 October 2017, 4 Ob 121/17y.

[44] TKK 28 November 2018, R 1-5, 8, 9/18; 12 April 2018, R 1-6/19; 9 July 2019, R 7/19; 22 October 2019, R 8/19; 19 August 2019, p. 1-5, 8, 10, 13/19; 17 March 2020, R 11-14/19.

In summary, it can be said that blocks set as a result of a legally enforceable court ruling based on copyright claims are binding on the national regulatory authority within the jurisdiction of the court ruling, which provides the mandatory basis for any supervisory procedure. Where the competent court does not hand down a ruling that is binding on the TKK, the actual existence of any entitlement under copyright law must, as a preliminary issue, be ascertained in the context of the procedure pursuant to Art. 5 of the TSM Regulation.

In the six procedures completed, the placing of access blocks to the websites that were the subject of the procedures was in accordance with the legitimate rights of the rights holders. The traffic management measures adopted, typically by setting up DNS blocks, were also identified as being appropriate to the situation and as observing the principle of proportionality.

As requested by a number of ISPs, the TKK initiated seven assessment procedures in the period from early 2019 to April 2020. Unlike the supervisory procedures pursuant to Art. 5 of the TSM Regulation as described above, the supervisory procedures here dealt with websites that have not yet been blocked. The assessment procedures determined whether an exception existed as defined in the TSM Regulation and whether it would be legitimate to subsequently block the website.

One procedure ended with the complete withdrawal of the request by the applicant parties in the procedure. For the remaining six, the TKK ascertained that an access block to the website being examined in the procedure would not be admissible in the absence of an injunction claim based on copyright and that such a block would breach the provisions of the TSM Regulation.[45] One party involved in these procedures filed with the BVwG an appeal against the decisions. As of this writing, the unlawful content had been removed and the domain that had been the object of the block was again available and offered for general sale.

The BVwG found such assessment procedures to be impermissible in the absence of an explicit legal provision and due to a lack of a legal interest on the part of the ISP. Although content was no longer accessible at the domain, the BVwG did not drop the respective procedures. The regulatory authority lodged an appeal with the Supreme Administrative Court in all procedures. The VwGH overturned the decisions issued by the BVwG and, in its own ruling, noted that the procedure should have been dropped by the BVwG since the contested content had been removed and the domain was again offered for general sale. The court also noted that the current legal situation authorises the regulatory authority to intervene only once the network block has been set up – and not before. The BVwG accordingly dropped the procedure. As a result, the TKK's decisions became final.

In light of the multi-year procedures held before ordinary courts as well as the Constitutional Court and Supreme Administrative Court, an explicit legal provision for an elective assessment procedure judged by the regulatory authority would be certainly be beneficial in this context. This would be particularly expedient to safeguard the right of all internet users to a free and open internet, and to enhance legal certainty for all stakeholders.

[45] TKK 19 August 2019, p. 5-8, 10, 13/19.

3.5 Supervisory measures

In the fifth reporting period (ending in April 2021), only one decision to ensure compliance was necessary. This was because dialogue was initiated with companies early on and discussions usually resulted in constructive solutions compliant with the Net Neutrality Regulation. Various request-for-information and supervisory procedures were initiated but then dropped without an order by official decision (e.g. because of the voluntary resolution of the issue by the ISP); such cases are not listed here. 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 (in R 3/16 and R 5/17) remain valid. The BVwG has in the meantime handed down a ruling on the appeal in R 3/16. The decision issued by the regulatory authority was confirmed on all points. The court's decision was not yet final at the end of the reporting period. A ruling by the BVwG on the appeal in R 5/17 is pending.

Table 4: Pending and decided supervisory procedures pursuant to Art. 5(1) of the TSM Regulation

Key: ⚖ 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 breach 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 breach of Art. 3 TSM Regulation identified	2018-11-26	☑

PROCEDURE	ISP	BRIEF DESCRIPTION	DATE OF DECISION	STATUS
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 breach 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 breach of Art. 3 TSM Regulation identified	2018-11-26	☑
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 breach 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 breach 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 breach 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 breach of Art. 3 TSM Regulation identified	2019-04-12	☑

PROCEDURE	ISP	BRIEF DESCRIPTION	DATE OF DECISION	STATUS
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 breach 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 breach 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 breach 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 breach of Art. 3 TSM Regulation identified	2019-04-12	☑
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 breach 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 breach 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 breach of Art. 3 TSM Regulation identified	2019-10-22	☑

PROCEDURE	ISP	BRIEF DESCRIPTION	DATE OF DECISION	STATUS
R 11/19	Hutchison Drei Austria GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no breach 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 breach 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 breach 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 breach 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 breach of Art. 3 TSM Regulation identified	2020-06-23	☑
R 1/20	Mass Response GmbH	Supervisory procedure pursuant to Art. 5 TSM Regulation on the auditing of access blocks for certain websites due to injunction claims based on copyright. Procedure dropped; no breach 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	Not yet final

04 Other indicators and activities

4.1 RTR conciliation procedures

A sharp rise was seen in complaints relating to the contractually agreed quality of internet access. Working from home and distance learning has highlighted the importance of this essential infrastructure. Notably, virtually all of the current reporting period was contemporaneous with the ongoing Covid-19 pandemic and its associated lockdowns. Anyone needing to be online around the clock for their job, studies or schoolwork naturally has more demanding requirements than someone simply using the internet during their free time. The situation is made more difficult by the simultaneous use of one internet connection by family members, for example.

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

Conciliation procedures	05/20 to 04/21	05/19 to 04/20
Mobile network quality	162	100
Fixed network quality	85	32

Transparency in relation to the contractually agreed and obligated performance for mobile internet connections continues to be a problem. The TSM Regulation has not achieved significant improvements in this area. The estimated maximum bandwidth that must be achieved once a day (which means that 4 a.m. is perfectly adequate) is a poor yardstick of quality, without any relevance for actual periods of internet usage. In addition, this estimated maximum bandwidth is in many cases itself set so low as to make its relationship to the bandwidth advertised for the tariff plan nonsensical (e.g. estimated maximum bandwidth 10 Mbps for an advertised bandwidth of 150 Mbps). The TSM-specific rules designed to identify non-contractual performance often prove to be a paper tiger in relation to mobile internet access. Although the bandwidth normally available to an end user is harder to define in a mobile context for technical reasons, a set of more hard-and-fast parameters would nonetheless be desirable here. At the same time, there is also the question of the interpretation of bandwidth as advertised. From a customer perspective, it would be better if adverts included clear and specific details of situations where ‘real-world’ usage could differ.

4.2 General requests

RTR’s Telecommunications and Postal Services Division also handled net neutrality enquiries outside the context of conciliation procedures. Specifically, there were enquiries regarding minimum content pursuant to Art. 4 TSM Regulation, forced disconnection of internet access, free choice of router and zero-rating. Beyond this, questions were also raised in relation to the right to request a public IP address. Overall, Austrian providers can be said to be fulfilling their obligations in this regard. During the reporting period, supervisory procedures were initiated against only two smaller ISPs.

4.3 Indicators for continuous availability of open IAS

The Net Neutrality Regulation allots national regulatory authorities the task of assessing the continuous availability of non-discriminatory internet access services at a certain level of quality.

The information presented below is also intended to account for longerterm trends. Reference is therefore also made to the figures in Part I section 5. The charts below are nonetheless interpreted only for the 2020 – 2021 reporting period.

The following indicators were deemed relevant to depict the continued availability of non-discriminatory internet access services (IAS) at levels of quality that reflect advances in technology:

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

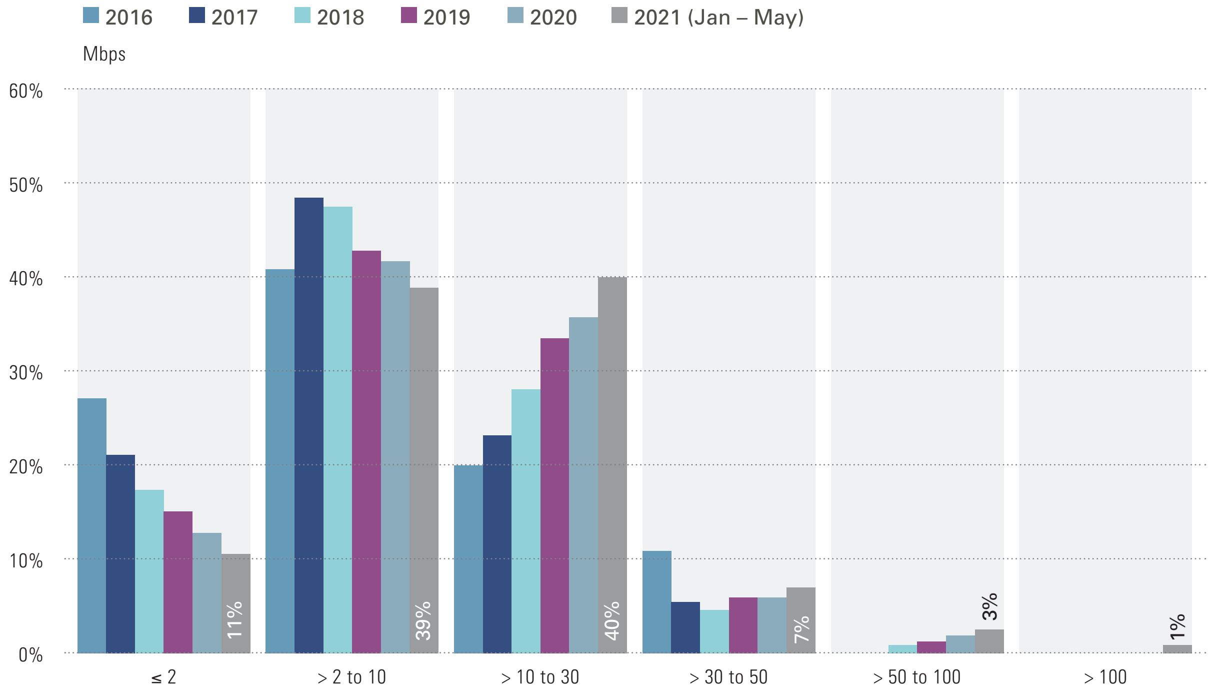
Figure 1 on page 24 shows the total number of fixed and mobile broadband connections. Within mobile broadband, a distinction is made between mobile data subscriptions (without minutes and texts included) and smartphone subscriptions (with minutes and texts included). M2M SIM cards are not shown in the chart. In terms of the number of mobile data subscriptions, one provider issued a correction: the figure is 2.2 million for the fourth quarter of 2020. The number of fixed broadband subscriptions rose from 2.5 million in Q4 2019 to 2.6 million in Q4 2020. The strongest growth was seen in smartphone subscriptions, which rose by around 5 per cent from 7.1 million in Q4 2019 to 7.4 million in Q4 2020. Overall, total internet connections rose by roughly 1 per cent from 12.1 million in Q4 2019 to 12.2 million in Q4 2020.

In the following, data from RTR-NetTest are used to assess developments in relation to quality during the reporting year. In 2020 RTR-NetTest was used to carry out more than 1.4 million measurements[46] (with a location accuracy of less than 2 km). In 2019 this number was still only 990,000. These data form the basis for figures 2, 3 and 9 to 12.

Figure 2 on page 25 shows the percentage of tests with download speeds in a given category. As can be seen, the category of 10 to 30 Mbps recorded the largest number of download speed measurements during the years 2019, 2020 and 2021 (in the months of January to May). Since then, this proportion has declined slightly to about 32 per cent from January to May 2021. The proportion of measurements in the category 2 Mbps or lower fell to around 5 per cent from January to May 2021. Measurements in the over 100 Mbps category have risen steadily from 7 per cent in 2019 to 12 per cent in January to May, marking the strongest growth in the speed categories considered during this period.

[46] Repeat measurements are not included.

Figure 9: Distribution of upload speeds

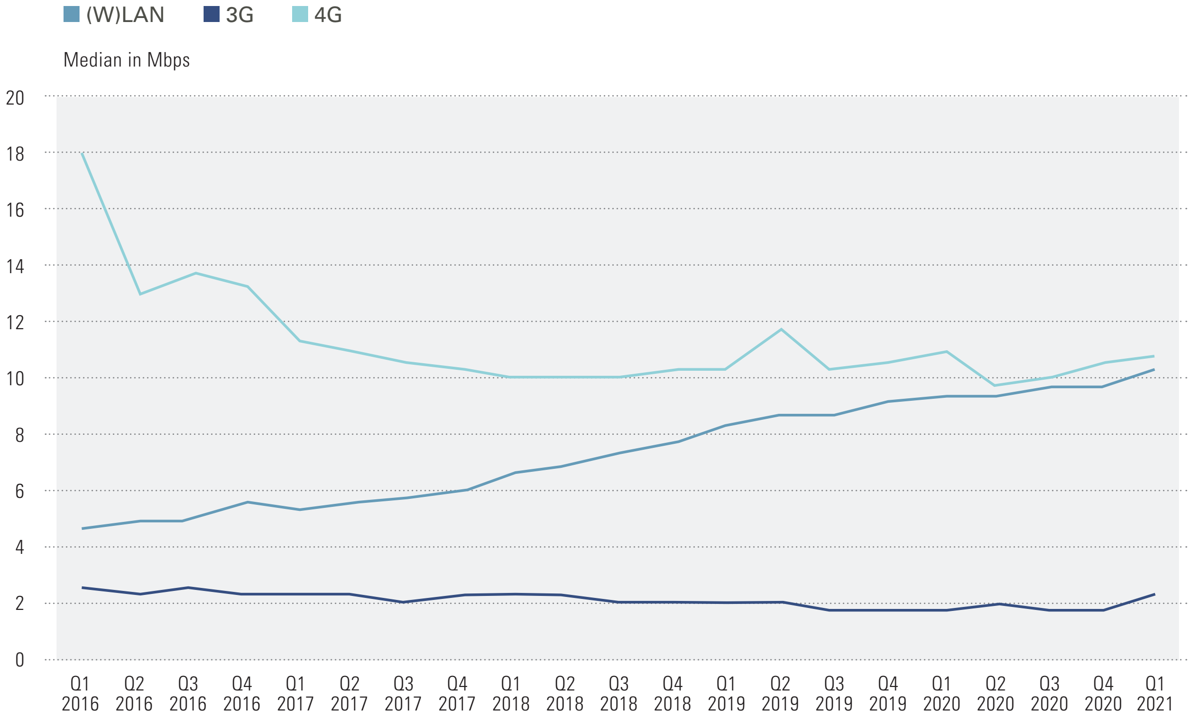


Source: RTR-NetTest

Figure 9 depicts the percentage of tests with upload speeds in a given category. In 2019 and 2020, most of the tests showed an upload speed of 2 to 10 Mbps. In the period January to May 2021, technical progress meant that the 10 to 30 Mbps category recorded the largest number of tests for the first time. The percentage of tests with an upload speed of less than 2 Mbps can also be seen to have fallen sharply since 2019, whereas the percentage of tests with an upload speed of 10 to 30 Mbps has risen by roughly 6 percentage points. The percentage of tests with speeds of 50 to 100 Mbps has increased since 2019 and averaged about 3 per cent in January to May 2021. The percentage of tests with speeds greater than 100 Mbps is still very small, but has increased slightly since 2019.

Figure 3 on page 26 depicts the median download speed measured with the RTR-NetTest over time, broken down by type of technology. Internet access speed depends on factors including the technology implemented. Download speeds achieved by 4G mobile services have fluctuated since Q1 2019. During Q2 2020, at the time of the first restrictions on movements imposed due to the Covid-19 crisis, a drop in 4G speeds to around 34 Mbps can be identified. After this, the median download speed for 4G mobile services then rose again to about 39 Mbps in Q3 2020. Another slight decline in the median speed has since revealed itself, with the figure being around 36 Mbps for Q1 2021. The speeds for 3G mobile telecommunications technology tend to be low and in Q1 2021 reached roughly 11 Mbps. Speeds in (wireless) LANs have fluctuated, with the median in Q1 2021 being 25 Mbps.

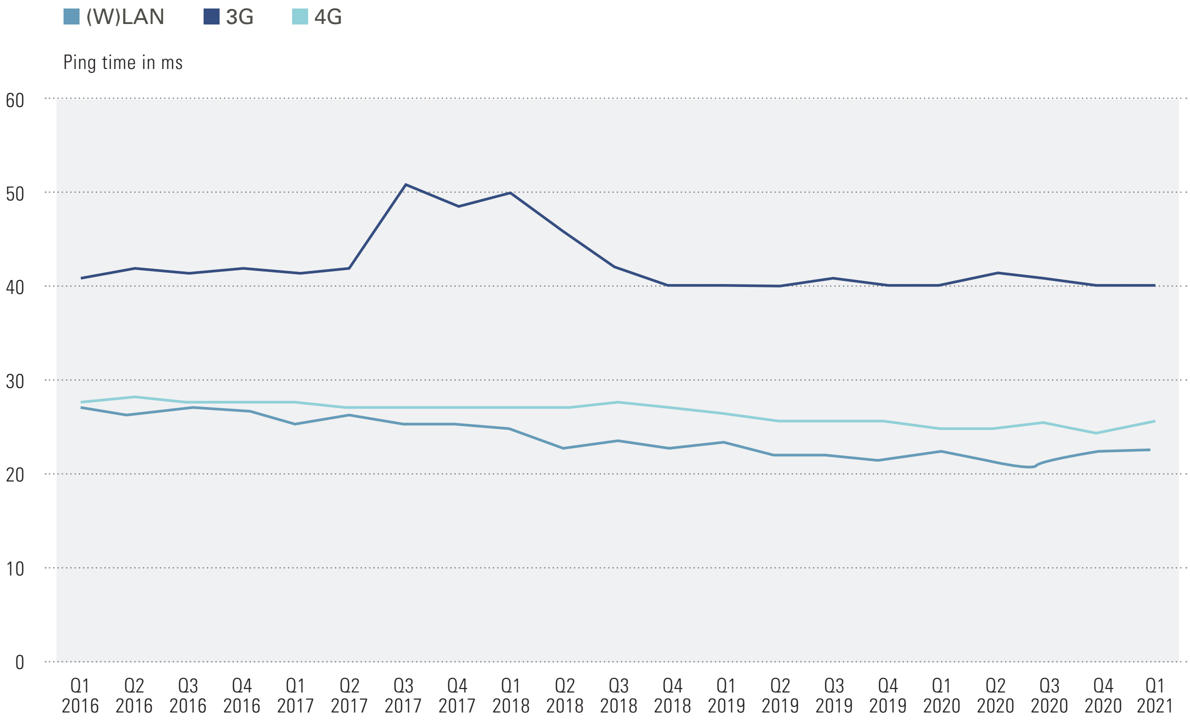
Figure 10: Upload speed by technology



Source: RTR-NetTest

Figure 10 depicts median upload speed broken down by technology. Once again, it is clear that the highest upload speeds are achieved with 4G mobile networks. Values fluctuated during the reporting period, with the figure being around 11 Mbps for the first quarter. The upload speed measured for (W)LAN has risen relatively constantly and was around 10 Mbps at the end of the reporting period. The upload speed for 3G mobile connections fluctuates and was about 2 Mbps in Q1 2021.

Figure 11: Latency (ping) by technology[47]

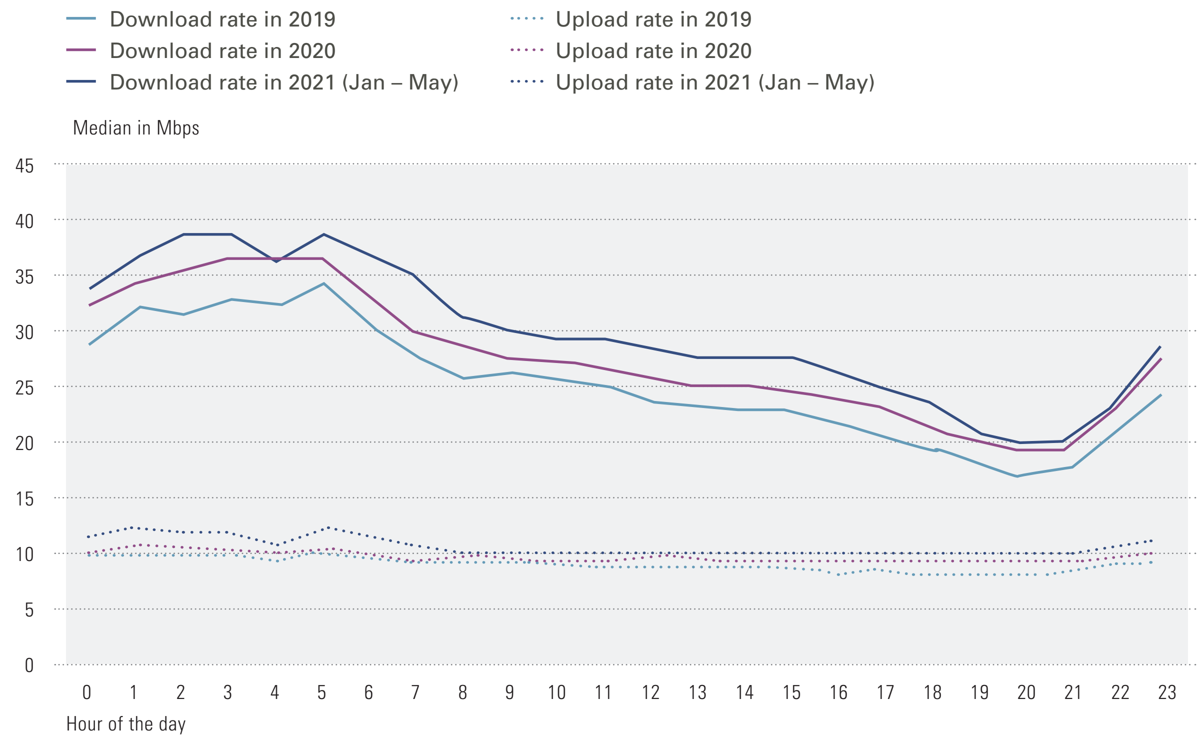


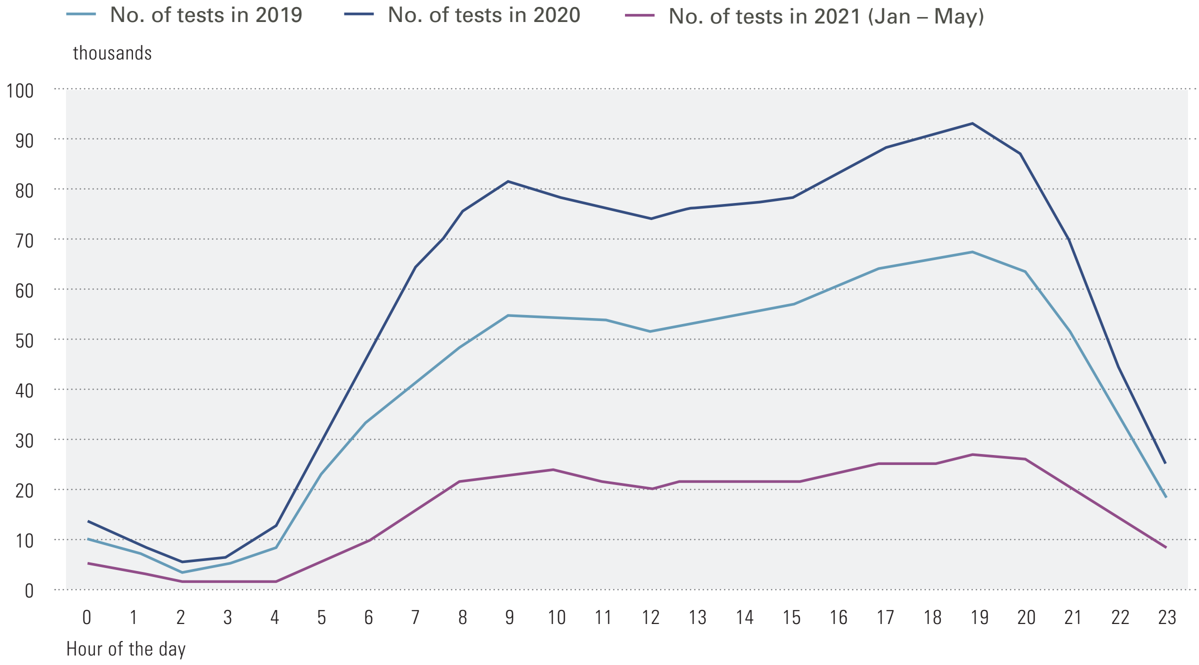
Source: RTR-NetTest

Figure 11 depicts median latency. Comparable latency measurements are potentially achieved using 4G mobile technology and (W)LAN. In the first quarter of 2021, ping time for 4G was 25.1 ms and 22 ms for (wireless) LAN. The figures are relatively constant for (W)LAN, 4G and 3G in the reporting period. With 3G mobile telecommunications technology, however, latency is consistently much higher at around 40 ms.

[47] 'Ping' (or more precisely 'round-trip latency') is the time a small data packet needs to make its way from a user device (such as a mobile or laptop) to an online server and back. Ping time is measured in milliseconds (ms). While ping time is a key indicator in relation to applications such as virtual and augmented reality and online gaming, ping time can also have significant bearing on how 'sluggishly' an internet connection responds during 'normal' internet surfing. Both the technology used to access the internet and the extent to which access is utilised significantly affect latency.

Figure 12: Download and upload speeds by time of day





Source: RTR-NetTest

Figure 12 shows the median download and upload speeds by time of day in 2019, 2020 and 2021 (Jan – May). The figure reveals that the median download speed is considerably lower between 18:00 and 22:00 than at other hours of the day, although no similar pattern is discernible for the median upload speed. During early morning hours between 1:00 and 6:00, the download speed is the highest, at roughly 37 Mbps in 2021 (Jan – May). In the course of the day the median download speed drops continuously and in 2021 (Jan – May) was only about 20 Mbps during the peak hour between 20:00 and 21:00. The median upload speed during the day was between 9 and 13 Mbps in 2021 (Jan – May). One positive finding is that both upload and download speeds were consistently higher in 2021 (Jan to May) than in 2020.

The number of RTR-NetTest measurements varies considerably over the course of the day. Only a few tests are performed during night hours. In 2019, 2020 and 2021 (Jan to May) most measurements were conducted between 19:00 and 20:00. During 2020 more than 93,000 measurements were made during this hour of the day.

Figure 4 on p. 27, finally, shows the three price baskets for fixed broadband (each without TV) and the three price baskets for mobile broadband (with unlimited data volume) over time. In both cases, the broadband categories differentiated are ≤30 Mbps, >30 to ≤100 Mbps, and >100 Mbps. The basket value is based on the least expensive product from each ISP that can be included in the respective basket (excluding subscription plans for young persons). From March 2019 to March 2021, prices rose in both ≤30 Mbps categories and for >30 to 100 Mbps fixed broadband, while prices instead fell in both >100 Mbps categories and for >30 to 100 Mbps mobile broadband. The strongest increase in this period, from EUR 20.70 to EUR 25.30, was seen in the ≤30 Mbps mobile broadband category. The biggest drop in price was recorded in the >100 Mbps mobile broadband category, which fell from EUR 46.90 to EUR 37.50.

Internet Monitor data can also be used to track the growth in data volumes consumed by tariff plan type.[48] Such an analysis reveals that the average volume of data consumed per fixed broadband connection between Q4 2019 and Q4 2020 rose from approx. 138 GB to 175 GB, which is equivalent to growth of around 27 per cent. The average volume of data consumed per mobile data subscription also increased, from 77 GB in Q4 2019 to 108 GB in Q4 2020, which is equivalent to growth of around 40 per cent. Growth of roughly 37 per cent was recorded in the average data volume consumed by smartphone subscriptions – rising from approx. 5 GB in Q4 2019 to more than 7 GB in Q4 2020.At least part of this increase can probably be ascribed to the Covid-19 crisis. Whether or not this develops into a trend towards everincreasing data consumption is a question to be answered at a later date.

[48] For details, see the most recent RTR Internet Monitor: https://www.rtr.at/TKP/aktuelles/publikationen/Uebersichtseite.en.html?l=de&q=&t=category%3Dinternetmonitor KEV data are available in the form of Open Data at: https://www.rtr.at/rtr/service/opendata/OD_Uebersicht.de.html

05 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 and being available as a partner to ISPs, internet users and all other stakeholders to consult on net neutrality issues. Optimal conditions for meeting this commitment are given through newly established organisational structures, including a dedicated ‘Net Neutrality and Customer Contracts’ team.

Specifically, the activities described below are currently planned for 2021/2022 or by the end of the next reporting period in April 2022.

I. Monitoring

1. **Transparency investigation.** Another investigation already planned for the coming reporting year will evaluate the status of transmission transparency (whether traffic is modified). This activity has been postponed to the following period as a result of the Covid-19 crisis. An investigation of this kind should certainly be conducted and further procedural steps should then be initiated in cases where there is evidence that data has been manipulated.

2. **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.

3. **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 accordingly.

4. **Ongoing review of general terms of business.** The regulatory authority’s work reviewing general terms of business also involves checking to confirm 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 significantly involve net neutrality issues (such as zero-rating or the provision of specialised services), the regulatory authority will set up monitoring teams as appropriate.

5. **Data from market observation and RTR-NetTest.** The regulatory authority periodically collects data (via the KEV, ZIB and ZIS)[49] 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, Telecoms Monitor). Another important system that is used to provide information about the structure and development of the internet is RTR-NetTest.[50] 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 developed on an ongoing basis.

6. **Certified monitoring mechanism.** A longstanding RTR measurement tool, RTR-NetTest was first deployed in conciliation and court proceedings in November 2018 with the aim of providing evidence for an ISP’s compliance or lack of compliance with a contractually agreed service level. This is considered a type of certified monitoring mechanism within the meaning of Art. 4(4) of the TSM Regulation.

[49] KEV is the Communications Survey Ordinance (Federal Law Gazette II No. 365/2004, as amended in 2017); ‘ZIS’ designates the Single Information Point for Infrastructure Data. The ZIS is a register of all existing infrastructure as usable for telecommunications purposes as well as planned construction projects. The ZIB is the Single Information Point for Broadband Coverage.

[50] See https://www.netztest.at/en/

7. **Network blocks are a topic of increasing significance.** In early 2021, the TKK's remit was further expanded by the Cooperation of Consumer Protection Cooperation Act (VBKG), and basic blocking principles are also being duly considered in other areas of law. The regulatory authority expects to see network blocks being afforded a due degree of attention on account of the need to weigh up one basic right against another in this context, which can also impact business models.

8. **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. There has been a greater national and international focus on topics in this area since the publication of the draft Digital Market Act (DMA) by the European Commission in December 2020. The regulatory authority is concentrating efforts here on the continuous monitoring of developments in applications and groups of application within the Austrian market.

II. International cooperation

1. **Aimed at a harmonious implementation of net neutrality provisions,** international exchange among regulatory authorities will continue. This takes the form of ongoing procedures as well as joint discussions and analysis of relevant products, within the framework of BEREC but also bilaterally. 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 2021 the "Outline for BEREC Work Programme 2021"[51] 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 2021. The report will be based on the reports on net neutrality that are to be prepared by the NRAs by 30 June 2021 and on the BEREC data survey carried out in June 2021.[52]

4. **Work on the DMA and the internet value chain.** Preliminary work on the DMA, which BEREC had itself initiated by the publication of the consultation document on a draft Digital Services Act in June 2020, was completed in March 2021 with the submission of a detailed expert opinion.[53] The first months after the end of the present reporting period were spent in consultations conducted with European institutions and on analysis work aimed at fleshing out individual topics. Supplementing and parallel to the RTR's engagement in the form of analyses relating to the DMA, the RTR Telecommunications and Postal Services Division has also been contributing to work on internet value chains that addresses both topics at network level (IP core, IB interconnection, IPv6) as well as the internet as an ecosystem.

[51] https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes /8977-outli

[52] https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/

[53] https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/9879-berec-opinion-on-the-european-commissions-proposal-for-a-digital-markets-act

5. **International work fosters knowledge transfer.** Work at international level not only creates a space for dialogue and discussion of the issues at hand. It also offers the opportunity of following the work of other regulatory authorities on the topic of net neutrality, reviewing its relevance for Austria and adopting suitable approaches where appropriate. Topics currently of particular importance internationally include network slicing, quality differentiation, specialised services and – last but not least – 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 at the start of this section – namely to promptly and constructively discuss, as part of an open dialogue with the sector or individual companies, any new issues, as a means of identifying solutions. Essentially, this lays the groundwork for all regulatory activities on net neutrality, since the details of any undertaking must in many cases be understood in full before regulatory recommendations can be proposed or conclusions drawn.

2. **Marking five years of the Net Neutrality Regulation.** In an event planned for July 2021, the RTR Telecommunications and Postal Services Division will look at past and future developments following the entry into force of this legislation. A retrospective will address difficulties, achievements, the role of the NRA and practicalities in relation to enforcement. An outlook will focus on future requirements, such as will transpire as a result of 5G and enforced quality differentiation. US insights drawn from the presence and absence of net neutrality legislation will also be discussed and compared with the EU experience. Speakers at the event will include Prof. Barbara van Schewick (Professor of Law at Stanford Law School), Rudolf Schrefl (CEO Hutchison Drei Austria) and Klaus M. Steinmaurer (Director of the RTR Telecommunications and Postal Services Division).

3. 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.[54] Alongside other activities, the Net Neutrality and Customer Contracts Team 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.

4. Last but not least, the **RTR Net Work Digital** event programme also plans to include an event dedicated to current issues and decisions in relation to net neutrality. Current candidates for topics include relevant EU rulings on net neutrality as well as recent developments in relation to areas including network blocks and quality differentiation. Further details of an event of this kind – planned for early 2022 – will be offered for comment as part of the budget consultation to be published later this year.

[54] See:
https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/Netzneutralitaet.en.html

Appendix 1: Mapping of the report to the structure of the guidelines

Here, as described above in the introduction, interested readers can view 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"	Part II section 1
"description of the monitoring activities carried out by the NRA"	Part II section 3 and section 4
"the number and types of complaints and infringements related to the Regulation"	Part II section 3 and section 4
"main results of surveys conducted in relation to supervising and enforcing the Regulation"	Part II section 3
"main results and values retrieved from technical measurements and evaluations conducted in relation to supervising and enforcing the Regulation"	Part II section 3 and section 4
"an assessment of the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology"	Part II section 4.3
"measures adopted/applied by NRAs pursuant to Article 5(1)"	Part II section 3.5

Appendix 2: Index of Figures and Tables

Figures

Figure 1: Fixed and mobile broadband connections 24
Figure 2: Distribution of download speeds 25
Figure 3: Download speed by technology 26
Figure 4: Price baskets – fixed vs. mobile broadband 27
Figure 5: QoS differentiation in the TSM Regulation 28
Figure 6: Timeline of events in the reporting period 34
Figure 7: Data volumes in plans that include zero-rating products 43
Figure 8: Relationships among tariff plans including zero-rating products 44
Figure 9: Distribution of upload speeds 54
Figure 10: Upload speed by technology 55
Figure 11: Latency (ping) by technology 56
Figure 12: Download and upload speeds by time of day 57

Tables

Table 1: Timeline of events in the reporting period 35
Table 2: Summary of problematic practices in light of the TSM Regulation 36
Table 3: Categories included in zero-rating tariff plans 41
Table 4: Pending and decided supervisory procedures pursuant to Art. 5(1) of the TSM Regulation 48
Table 5: Sections of this report as mapped to the BEREC Guidelines 64

Appendix 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
GDPR:	General Data Protection Regulation
EC:	European Commission
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
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 2003:	Telecommunications Act 2003 (Telekommunikationsgesetz 2003)
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; Net Neutrality Regulation; officially: Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

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
(Rundfunk und Telekom Regulierungs-GmbH)
Mariahilfer Strasse 77 – 79, 1060 Vienna, Austria
Tel.: +43 (0)1 58058-0; fax: +43 (0)1 58058-9191; e-mail: rtr@rtr.at
www.rtr.at

Responsible for content
Dr. Klaus M. Steinmaurer (Telecommunications and Postal Services Division)

Conceptual design and text
Austrian Regulatory Authority for Broadcasting and Telecommunications

Graphic design and layout
Westgrat – Agentur für Kommunikation
cibus Kreativagentur

While all contributions to the 2021 Net Neutrality Report have been reviewed with the utmost care, errors cannot be ruled out. No guarantee of accuracy can consequently be provided for this information.

RTR

Austrian Regulatory Authority for Broadcasting and Telecommunications

(Rundfunk und Telekom Regulierungs-GmbH)
Mariahilfer Strasse 77 – 79 | 1060 Vienna | Austria
t: +43 1 58058-0 | f: +43 1 58058-9191 | m: rtr@rtr.at
www.rtr.at