RTR NET NEUTRALITY REPORT

2018

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

RTR

20
18

RTR NET NEUTRALITY REPORT

2018

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

Contents
Net Neutrality Report 2018

Figures

Tables

Abbreviations

BEREC	Body of European Regulators for Electronic Communications
CAP	content and application provider
CERT	computer emergency response team
EC	European Commission
GDPR	General Data Protection Regulation
IAS	internet access service
ISP	internet service provider
KEV	Communications Survey Ordinance (Kommunikations-Erhebungs-Verordnung)
KommAustria	Austrian Communications Authority
MNO	mobile network operator
NAT	network address translation
NN	net neutrality
NRA	national regulatory authority
RTR	Austrian Regulatory Authority for Broadcasting and Telecommunications
TCP	transmission control protocol
TKG	Telecommunications Act
TKK	Telekom-Control-Kommission
TSM Regulation	Telecoms Single Market Regulation
VoD	video on demand

01 Executive Summary

The **2018 Net Neutrality Report** is the second report by RTR on the current status in Austria relating to open internet access. The report is based on the EU's TSM Regulation, which came into force in November 2015 and includes rules on net neutrality. These rules primarily relate to equal treatment of data transmitted via the internet, independent of the sender, recipient and chosen application. Based on the first report published in 2017, this publication describes the activities or actions that the regulatory authority undertook in the year under review (1 May 2017 to 30 April 2018) to ensure open internet access. During the second year of enforcing the net neutrality rules – and of the related reporting – 'red lines' were or needed to be drawn for the first time, to contain breaches of the provisions set out in the TSM Regulation. Like the 2017 report, the current report provides information on official activities related to net neutrality, answering the questions of 'how', 'what' and 'when'.

As in the past year, a major focus of activities was to coordinate enforcement of the TSM Regulation with NRAs in other Member States under the umbrella of BEREC. Where enforcement practices vary between Member States, there is a risk of distorted competition between national markets, which in turn can have a detrimental impact in terms of the power for innovation inherent in the internet. Again in this reporting year, as an integral part of efforts to ensure net neutrality, RTR has contributed to and shaped discussions at international level on issues surrounding the enforcement of the TSM Regulation and the approaching review of the BEREC guidelines. This was all the more of a concern inasmuch as RTR, under its managing director, was and continues to chair BEREC, with one of the main responsibilities being to ensure harmonised application of provisions of law. This international involvement has had spin-off effects for the discussion taking place in various forms with all major stakeholders in Austria. As in the past, RTR continues to pursue a path of consultation, the first step of which involves providing information and advice to Austrian ISPs. We are guided by the principle that, even in cases of dispute, a solution for restoring legal compliance that involves the parties concerned is to be preferred to an official decision ordering compliance; consequently we only needed to issue binding orders in cases where it was not possible to reach an agreement with the providers concerned. By following this solution-focused approach within a clearly and strictly defined framework, we seek to maintain and nurture existing conditions, allowing providers to plan business activities and develop new products. Meanwhile, regulatory action is necessary to clearly signify that a 'level playing field' exists for all ISPs and end users and that steps will be taken with the necessary rigour in the event of any infringement of net neutrality.

A survey was taken again in 2017, entailing 15 different tests with numerous measurements to rate the degree to which providers observe transparency when transmitting data within their networks. The NRA also continues to be able to resort to other monitoring systems, including the requirement based on the TKG 2003 for providers to notify their general terms and conditions and fee provisions to the authority prior to providing services; complaints lodged by end users are also a potential source for monitoring. Indications of possible breaches of net neutrality provisions are investigated through procedures involving requests for further information and are usually considered in more detailed procedures conducted by the Telekom-Control-Kommission (TKK). The NRA's activities in the reporting year were focused on completing the pending procedures involving the five major companies and on the first actual cease orders based on the TSM Regulation, which were issued shortly before

Christmas in 2017. Accordingly, the main activities in the year under review were related to evaluations, specifically to assess whether certain services (such as video on demand) are to be classified as specialised services, and to discontinuing non-compliant traffic management practices (traffic shaping). Future enforcement of the TSM Regulation will depend on how procedures progress and specifically on the rulings handed down by the Federal Administrative Court (BVwG). Mention should be made here of an initial conclusion that has emerged regarding enforcement of the TSM Regulation: there was a clear – and positive – tendency for the ISPs involved to discontinue potential breaches 'voluntarily'. At the same time, the basis was established for a further round of review procedures, with a survey of 13 providers' products and technical practices initiated in Q1 2018.

How can open internet access in Austria be rated during the year under review? The overall picture continues to be highly positive. Companies involved in breaches of net neutrality rules generally identified constructive solutions, which were then approved by the NRA and implemented (or scheduled for implementation). Accordingly, most of the procedures initiated at the start of the current review period in October 2016 could subsequently be dropped after the ISPs involved voluntarily took corrective action. In the procedure to determine whether the VoD component of a bundled product is to be regarded as a specialised service as defined in the TSM Regulation, a final decision was taken before Christmas in 2017, after obtaining an expert's evaluation report and holding an oral hearing. In contrast to the previous reporting year, one new product was introduced, in November 2017, that directly conflicted with the provisions of the TSM Regulation. The features of the product were highly similar to a product offered in Germany under the brand name of 'StreamOn'. After the product had been brought to market in mid-November 2017, the regulatory authority had already prohibited the technical practices not complying with the TSM Regulation by 18 December 2017, thus demonstrating the intention to proceed above all quickly and with sustained effect against breaches of net neutrality. Section 5 of the report contains details of these procedures. A relevant aspect in this regard is the continued discussion of 'zero-rated' products in general. The misleading impression, conveyed by the media, that the TSM Regulation generally prohibits 'zero-rating' had to be refuted on several occasions.

Finally, a new aspect emerged towards the end of the period under review, related specifically to content-blocking of websites, where websites were subject to injunctions prohibiting access due to potential structural breaches of copyright laws. This obviously results in tension, with the requirement for free internet access and the prohibition of content-blocking as set out in the TSM Regulation potentially conflicting with the justified claims of copyright holders. While not able and by no means intending to take the place of the regular courts, the regulatory authority nonetheless has a duty as part of procedures to review such content-blocking to determine its compatibility with the TSM Regulation, which the authority is called upon to enforce. Here we need to examine primarily those cases where blocking is not based on a court order but implemented merely in response to a request by the copyright holder. In this context, a key issue relating to net neutrality and to maintaining an open internet is the question of which traffic management measures for implementing blocking are permissible based on Art. 3 of the TSM Regulation, which defines exceptions based on strict requirements for proportionality (to avoid 'overblocking').

One question is whether open internet access continues to be provided at a quality level that reflects progress in technology. Here it can be observed that the developments in the year under review were not impacted with any lasting effect by products or practices that are relevant for net neutrality. In the case of new products not conforming to the rules of the TSM Regulation, expeditious and efficient measures were taken to protect both end users and fair competition.

Thus, the experience gathered in the second reporting year – and here especially the initial procedures conducted – revealed that the intended effect of steering companies was fully achieved, by giving attention to the topic at an early stage and through the many discussions that the NRA held with companies in advance. Another proven practice is for the regulatory authority to provide an opportunity to discuss ideas for new products in advance, without prejudicing any later procedures, to review potential compatibility with the provisions of the TSM Regulation. Thus, the net neutrality rules and the guidelines building on them have from today's standpoint demonstrated their usability. From the perspective of official enforcement, immediate adaptation is needed in only a few areas.

As previously, efforts in the near future will concentrate on continued monitoring activities and on maintaining consultations and exchange between the regulatory authority and market participants within the framework of procedures and talks.

All of the major providers are expected to have achieved a state of 'net-neutrality readiness' by the end of 2018. Work in preparation for the review of the main provisions of the TSM Regulation, which the European Commission will undertake by 30 April 2019, will be another focus of activities in the next reporting year. Beyond this, RTR will closely monitor the rapid technical developments in the field of digitisation and specifically relating to the 5G standard.

Mag. Johannes Gungl

Managing Director
Telecommunications and Postal Services Division
RTR

Vienna
June 2018

02 **Introduction**

In its second Net Neutrality Report, RTR continues the practice it began last year of informing the general public about the status of net neutrality in Austria.

Providing a straightforward definition of the term net neutrality (NN) is not an easy matter. Essentially, however, NN describes the equal treatment of transmitted data, regardless of sender, recipient or chosen application. In a less technical sense, this report considers questions such as: How open is the internet in Austria? Which measures had to be adopted by regulators in the reporting year (1 May 2017 to 30 April 2018) to preserve the openness of the internet – which is and has been the driver for so many innovations we can now scarcely do without? What are the new product developments that, while potentially offering advantages for consumers, nonetheless simultaneously harbour risks for the future sustainability of the internet? Pursuing this line of enquiry, the report aims to inform readers both about the state of play and about how and when regulators act in the interests of net neutrality.

The report stems from an obligation imposed on the national regulatory authorities (NRAs) by the Telecoms Single Market Regulation (TSM Regulation)[1], which includes the objective of achieving a consistent approach to applying the provisions of net neutrality in all Member States.

This report duly complies with the guidelines[2] published by the Body of European Regulators for Electronic Communications (BEREC), which also include a section concerning reporting duties (Par. 167–183). For the purposes of clarity and readability, this report deviates in some respects from the section structure recommended by the guidelines. Interested readers can compare the structure of this report to the structure proposed by the guidelines by consulting the dedicated mapping presented in Appendix 1.

While the first report followed the strategy of providing an overview of the products offered on the market, as well as the commercial and technical practices adopted by this market, the focus in the current reporting year was on identifying potential violations of net neutrality rules. Dedicated chapters are also provided on specialised services and IAS restrictions.

As a convergent regulatory authority for media, telecoms and postal services, it is essential that RTR develops and coordinates all positions on net neutrality as an interdisciplinary activity, with involvement of the Austrian Communications Authority (KommAustria) being especially important.

---

[1] 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. L 310/1 of 26 November 2015, https://www.rtr.at/de/tk/tsm_regulation/TSM-en.pdf

[2] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, August 2016, BoR (16) 127, https://www.rtr.at/de/tk/nnnews/20160830_BEREC_Guidelines_Net_Neutrality.pdf

From the outset, the regulatory authority has oriented its practice on the following considerations: the authority's goal is to identify breaches of net neutrality provisions while raising awareness of the subject, 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. These considerations are taken into account by setting appropriate transition periods, for example.

To facilitate and guarantee harmonisation across the EU, RTR is active at European level as a member of BEREC working groups on net neutrality. This work includes discussions of cases from across the member states – on zero-rating and traffic management for example – with the aim of a uniform perspective on relevant issues.

In this report, the following section 3 provides readers with an introduction to the general context of net neutrality – namely the stakeholders, institutions and the scope of TSM Regulation enforcement. Section 4 provides a chronological view of the authority's activities in preparation for section 5, which presents (suspected) violations of the TSM Regulation together with corrective measures. Section 6 summarises the outcomes of regulatory activities during the reporting period, before section 7 then presents an outlook on the authority's activities in the future.

03 Stakeholders, institutions
and the scope of TSM Regulation enforcement

To improve the readability of the following sections, this section provides an introduction to the key factors in net neutrality, meaning stakeholders, institutions and applicable scope.

Broadly speaking, the provisions of net neutrality are targeted at companies that provide services for accessing the internet, known as internet service providers (ISPs). The primary goal envisaged by the Regulation is to accommodate changes in technical possibilities (such as traffic identification and control) and related new business models (or practices) pursued by internet service providers, so as to ensure that the innovative power of the internet is not impaired. The TSM Regulation accordingly identifies business practices, technical measures and obligations (such as ensuring transparency for end users, for example) that are required or prohibited in order to uphold net neutrality. Alongside ISPs, the group of stakeholders and others targeted by standards includes in particular end users (private citizens and businesses) and providers of content, services or applications (content and application providers, hereinafter 'CAPs').

Two other key aspects should also be mentioned. First, discussions about net neutrality relate in part to questions about the right approach to financing a high-performance broadband infrastructure. Can or how can CAPs, whose services are of course offered to end users via the infrastructure provided by ISPs, potentially be integrated into financing models, and which new business models might be available to ISPs? These questions have been the focus of past discussions and will continue to be a focus, considering various aspects of 5G mobile technology. After two years of enforcement of the TSM Regulation, ISPs still clearly have room for innovation and scope for products, without coming into conflict with provisions intended to uphold net neutrality. There is typically a certain tendency to 'test the limits' of such legal provisions during the introductory phase, but this in no way undermines the intended balancing of interests between infrastructure innovation and service innovation. These latter aspects constitute key goals of contemporary telecommunications policy and the resulting issues can only be resolved or answered through a cooperative approach, which is in fact planned for discussions about 5G.

A second decisive aspect relates to common practice. To be effective, a framework of rules that affects internet-driven innovation should not be created and enforced at national level but established instead on as broad a basis as possible. Correspondingly, the TSM Regulation is an EU Regulation with direct relevance for the Member States of the European Union. Its aim is to ensure that practice across the entire single market is as uniform as possible. Independent approaches taken by the various countries or regulatory authorities could have the result of disadvantaging some ISPs in relation to others. Yet it also needs to be kept in mind that market structures or, most importantly, the administrative enforcement of applicable legal provisions are all but homogeneous across Member States, and these aspects are (or could be) sufficient to account for variations in regulatory authority practice. Aside from these aspects, it has been the close coordination practised by regulatory authorities under the mantle of BEREC that has ensured the largely harmonised enforcement of the TSM Regulation. That regulatory authorities adopt a variety of points of focus in carrying out this work is entirely germane to the goal of creating precedents for harmonised enforcement as soon as possible.

This addresses another relevant group of stakeholders, namely the authorities responsible for assessing compliance with the provisions of the law (and obliged to produce an annual net neutrality report), and BEREC, whose principal role in this context is to ensure the harmonised enforcement of the provisions of the Regulation across the EU. For this purpose and in line with the TSM Regulation, BEREC adopted guidelines for the enforcement of the Regulation, making a key contribution to the first actual enforcement actions.

In Austria, the Telekom-Control-Kommission (TKK) and Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) are responsible for enforcing the TSM Regulation. Where regulatory activities in line with the TSM Regulation relate to a radio broadcasting market, responsibility is also shared with KommAustria. Pursuant to Art. 25 of TKG 2003 – and also of relevance for net neutrality – general terms and conditions as well as fee provisions must be submitted to RTR before commencement of the service. The TKK can issue an objection within eight weeks in the event of non-compliance with the TKG 2003 or ordinances issued on the basis of the TKG 2003, or Articles 879 and 864a of the Austrian General Civil Code (ABGB) or Articles 6 and 9 of the Austrian Consumer Protection Act (KSchG). This provision de facto creates a situation where all changes relevant to general terms and conditions (including those affecting net neutrality) must be submitted to the regulatory authority and reviewed for compliance with the minimum contractual content given in Art. 4(1) of the TSM Regulation. This gives the regulatory authority an efficient 'early warning' mechanism – even though violations of provisions other than those stated in Art. 4(1) of the TSM Regulation can be prohibited only ex post. Moreover, the regulatory authority can also impose reporting requirements on a company, which can help to improve estimates of the impact on the market. While a correct interpretation of Articles 115 and 117 TKG 2003 and the relevant rulings by the administrative courts allows an allocation of responsibilities between RTR and TKK, legal certainty for all market participants would be better served if, additionally, legislators were to expressly set out these allocations in a piece of legislation.

RTR is a convergent telecoms, postal and media organisation, and the Telecommunications and Postal Services division and the Media division consult with one another on all key issues relating to net neutrality. One reason why this is essential is the fact that many net neutrality topics (such as zero-rating or specialised services) exhibit an overlap with media topics (such as the procedure addressed in section 5.5). Other points of overlap arose – in relation to port-blocking – with the national representatives of the Computer Emergency Response Team (CERT), which acts as a national point of contact for IT security (such as in the event of cyber-attacks or attacks on critical infrastructure), and could potentially arise with data protection regulators (if the traffic management policies adopted were to violate the privacy of consumers, for example). The last point mentioned may become more significant in the next reporting year (entry into force of the EU GDPR on 25 May 2018).

04 Regulatory activities
chronology of events in the reporting period

4.1 Timelines

FIGURE 01:   TIMELINE OF EVENTS IN THE REPORTING PERIOD

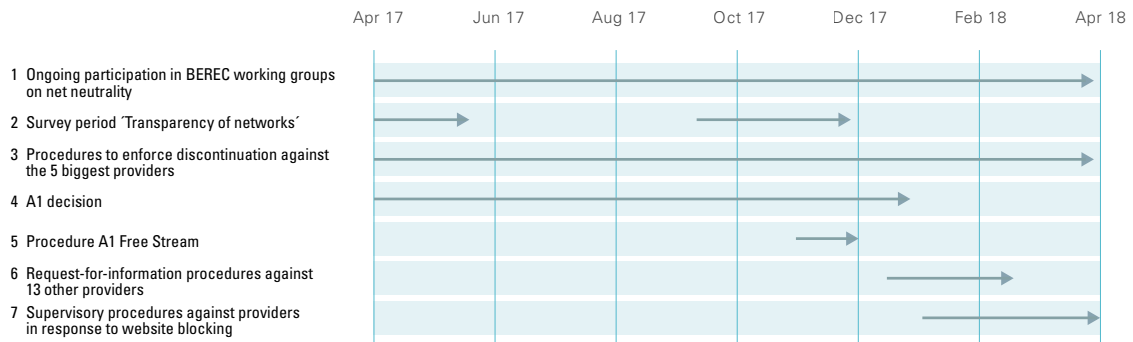|	Apr 17	Jun 17	Aug 17	Oct 17	Dec 17	Feb 18	Apr 18
1 Ongoing participation in BEREC working groups on net neutrality							
2 Survey period ´Transparency of networks´							
3 Procedures to enforce discontinuation against the 5 biggest providers							
4 A1 decision							
5 Procedure A1 Free Stream							
6 Request-for-information procedures against 13 other providers							
7 Supervisory procedures against providers in response to website blocking							

Figure 1 shows the chronological sequence of relevant events in the reporting period (05/2017–04/2018). The table below gives an overview of these events, with a brief description as well as some historical context.

TABLE 01:   TIMELINE OF EVENTS IN THE REPORTING PERIOD

		WORK IN EU BODIES
1	Current	Participation in BEREC working groups on net neutrality BEREC working groups in 2017: Implementation of Regulation 2015/2120 and Guidelines on Net Neutrality, Regulatory assessment of QoS in the context of Net Neutrality, and Net Neutrality supervision tools and methods BEREC working groups 2018: Development of a Net Neutrality measurement tool, Implementation of the Net Neutrality Regulation, Net Neutrality – input to an evaluation
		NATIONAL STATUS QUO ANALYSIS/DISCUSSION WITH PROVIDERS
2	02/2017 – 05/2017 and 09/2017 – 12/2017	The data for the study carried out in early 2017 was collected in the previous reporting year; the analysis of results and procedural implementation took place in the current reporting period. Performance of follow-up survey on network transparency (for further details, see 4.2).
		ENFORCEMENT OF TSM REGULATION
3	Since October 2016	Procedures to enforce discontinuation, initiated against the five largest providers by the TKK in October 2016. One of these cases was still open at the end of the reporting period (for further details, see 5).
4	12/2017	TKK issued a decision against A1 Telekom Austria AG (prohibiting the prioritisation of the video-on-demand component of A1 TV, extending the interval for automatic disconnection of the internet connection from 24h to 30 days and imposing an obligation to provide a free public dynamic IP address; for further details, see 5.2, 5.5, 5.6).
5	11/2017 – 12/2017	TKK decision to initiate a supervisory procedure against A1 Telekom Austria AG to discontinue a music and video streaming product (Free Stream) (for further details, see 5.4)
6	02/2018 03/2018	TKK decision to initiate request-for-information procedures against 13 other providers (for further details, see the first subsection of section 5)
7	Since 02/2018	TKK decision to initiate seven supervisory procedures against providers in response to website blocking (for further details, see 5.7)

Further details about these procedures can be found in sections 5 and 6. The next subsection presents the methods applied in the transparency survey and the results.

4.2 Network transparency survey as the 'baseline'

Two rounds of the survey commissioned by the RTR in early 2016 entitled "Transparency of Networks" were completed in the reporting period. The aim of this survey is to obtain a more detailed picture of the practices of various operators and the telecommunications networks they operate.

As with the survey in the previous reporting period, private internet connections were used for sending packets between servers and clients under controlled conditions. Performing a comparison of the packets sent and received permits changes in packet transfer to be identified and logged.

A total of five clients were used for parallel and periodic testing of the retail broadband internet access provided by seven Austrian providers. This selection included both fixed and mobile internet products. While taking measurements, the modem made available by the provider was used wherever possible. The following diagram provides a summary of the topology.

FIGURE 02   ARCHITECTURE FOR THE NETWORK TRANSPARENCY SURVEY
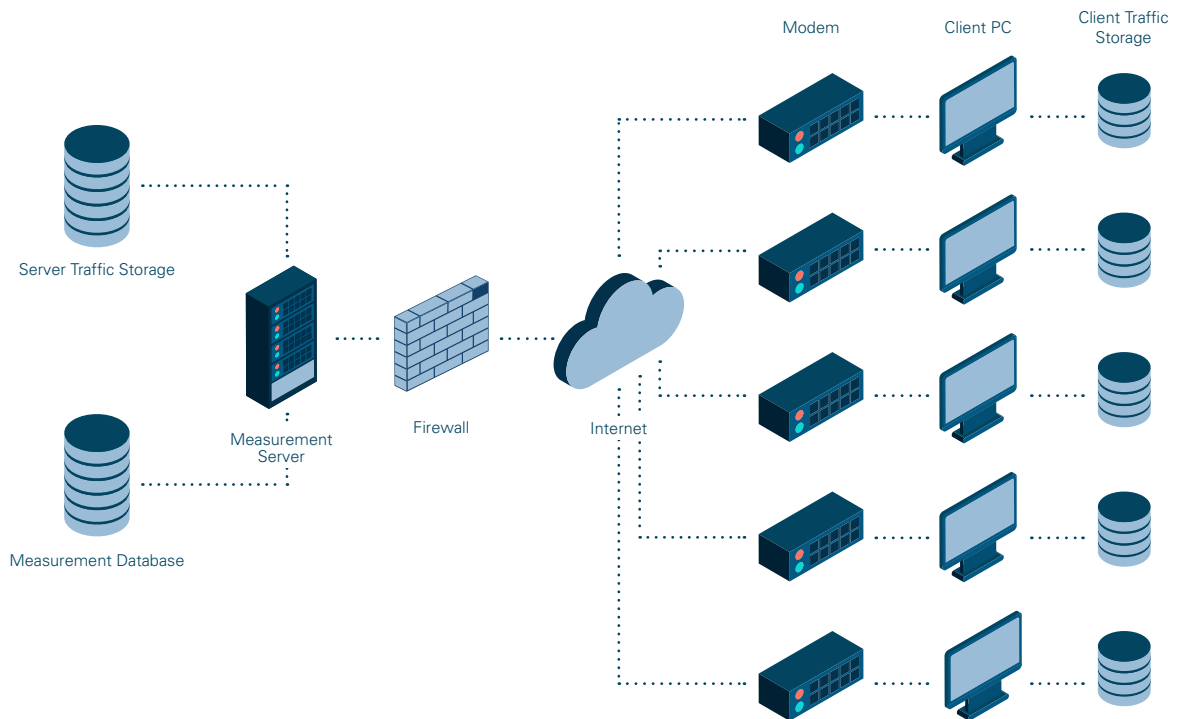
In the reporting periods of February to May 2017 and September to December 2017, over 220,000 distinct measurements were taken in total. The tests performed were grouped into 15 separate test metrics, which also remained unchanged in the follow-up survey.

These metrics are based on various layers within the OSI layer model, and are used to test potential changes to packets during the use of various protocols. These protocols included TCP, UDP, TLS, DNS, SIP, RTP, POP3 and SMTP.

No abnormalities were detected during the vast majority of measurements taken. For some metrics, isolated technical peculiarities were discovered.

- Some ISPs modify responses from their own domain name system server – so as to block websites while referring to applicable court rulings on copyright infringements, for example.
- The DNS servers operated directly by various providers vary in their behaviour when responding to queries relating to unassigned URLs. While some providers immediately return the DNS code NXDOMAIN, queries sent to other providers are queued for a few seconds and then time out.
- With one provider, the time-to-live flag for TCP ports 554 and 5060 is assigned a value that differs from the time-to-live flag for other TCP ports. No change to the TCP payload could be detected, however.
- A modification to the headers of HTTP traffic sent over TCP port 80 in the case of one provider, while existing when the previous and interim survey reports were prepared, could no longer be detected in the final survey round.

Technical modifications to traffic were not detectable with any provider. Apart from the above-mentioned exceptions, the measurements showed entirely positive results, in the sense that no manipulation, preferential treatment or other technical discrimination of internet traffic could be detected using the metrics tested.

Findings from the 2016 survey have already being used in discussions held with providers in the procedures initiated (cf. section 5) and were clarified and/or solutions identified. No new technical abnormalities were discovered in survey data collected in the reporting period: on the contrary (and as was to be expected), the incidence of problematic practices has actually decreased. In supplying input for the state of play, the survey has therefore proven its utility; there are plans to continue its use in one form or another.

05 Potential violations of net neutrality

and associated procedures

After the entry into force of the TSM Regulation on 30 April 2016 and work to confirm providers had made the necessary changes to their contract terms, the focus moved to the primary objective of reviewing compliance with the core provisions of Art. 3. Work in the first year of enforcement of the TSM Regulation therefore concentrated more on gaining an overview of the products offered on the market, as well as of the typical commercial and technical practices.

In the second year of enforcement of the TSM Regulation, the emphasis moved to taking action against potential violations of net neutrality. On a positive note, most of the procedures initiated against the largest national ISPs in October 2016 were completed by the start of this reporting period, without the need to issue a cease order under Art. 5 of the TSM Regulation. The affected ISPs themselves proposed remedies or changes to secure compliance with the TSM Regulation and implemented these following approval by the regulatory authority. As of 30 April 2018, only a single procedure is still pending against one provider, whereas the discontinuation of a potential violation of Art. 3(3) TSM Regulation (redirection of traffic via a proxy) is now already in the technical implementation phase. One may therefore be confident that all of these procedures will have been completed by the next reporting period.

As already stated in the 2017 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 and therefore needed to be investigated.

TABLE 02:   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 may render certain services unusable, which is a contravention of Art. 3(1) and Art. 3(3) TSM Regulation. A more detailed description is given in section 5.1.
2.	Private IP addresses and services	Customers are assigned private IP addresses (via NAT – network address translation). This prevents these customers from using or providing their own services; however, this right is derived from Art. 3(1) TSM Regulation. A more detailed description is given in section 5.2.
3.	Zero-rating	The data volume used by a specific application or from a specific CAP does not count towards the data volume cap included in the customer's subscription. A more detailed description is given in section 5.3.
4.	Specialised services	A specialised service is a service that is not offered via the normal internet access service (IAS) but is offered instead as a prioritised/optimised service by the ISP. To be offered as a specialised service as defined by Art. 3(5) TSM Regulation, a service must first satisfy certain conditions. A more detailed description is given in section 5.5.
5.	Technical discrimination and restriction of internet access	Traffic modification/redirection or the placing of restrictions on the IAS contravenes Art. 3(3) TSM Regulation. A more detailed description is given in section 5.4.
6.	Disconnection of IP connections	Automated disconnection of IP connections infringes the rights of the end user to use or provide their own services (Art. 3(1) TSM Regulation). A more detailed description is given in section 5.6.
7.	Blocking websites due to copyright claims	While courts of law are authorised to grant injunctions on the grounds of copyright law, 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 to verify whether an exception exists under point (a) of Art. 3(3) third subparagraph TSM Regulation (see section 5.7).

Procedures investigating practices numbered as 4 (specialised services) and 5 (restriction of IAS) formed a particular point of focus in this reporting year. In these areas (see the respective sections below for details), two procedures were also completed by the Telekom-Control-Kommission (TKK) with orders pursuant to Art. 5(1) TSM Regulation at the end of 2017. In the context of specialised services, an extensive procedure

(R 3/16)[3] to assess whether (and if so, which parts of) a service of A1 Telekom Austria AG (A1 Telekom) could be considered a specialised service was concluded in December 2017. Like the German Federal Network Agency in the case of StreamOn, RTR and the TKK were faced with a zero-rating product from A1 Telekom at the end of 2017 that simultaneously envisaged the use of traffic shaping, i.e. a reduction in bandwidth for the zero-rated content. The legal questions raised by this procedure (R 5/17)[4] were also decided shortly before Christmas 2017 by an order prohibiting the use of traffic shaping.

In terms of practice 5 in particular (see Table 2), it should be stated that RTR (as well as BEREC) were dealing with the continued activities of a satellite network operator. As in the previous reporting period, the matter concerned in-flight Wi-Fi network arrangements, implemented by a data uplink handled via a satellite connection. In this case, the provider wished to use a tiered subscription based on services (sub-internet services, i.e. packets from classes of services/applications) while simultaneously suppressing other forms of data transfer – which the regulatory authority holds to be in contravention of the TSM Regulation. The provider engaged in activities intended to convince the regulatory authorities of its view that this service-based IAS restriction was in fact appropriate traffic management, but was ultimately unsuccessful.

Towards the end of the reporting period, further intervention by the regulatory authority was required regarding compliance with Art. 3(3) TSM Regulation. This case concerned an investigation of compliance with or the applicability of point (a) of Art. 3(3) third subparagraph TSM Regulation concerning the blocking of content (websites) in response to copyright claims. While courts of law are authorised to grant such copyright injunctions, 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 to verify whether an exception based on point (a) of Art. 3(3) third subparagraph TSM Regulation exists. Whether the copyright holder has a valid claim can be considered as a preliminary issue for this evaluation.

In early 2018, as part of continued monitoring of compliance with Art. 3 TSM Regulation, a total of 13 ISPs were sent questionnaires about products and technical practices in a second round of request-for-information procedures. All responses to this survey had been received by the end of the reporting period: these will now be analysed and procedures pursuant to Art. 5(1) TSM Regulation will be initiated to handle any suspected breaches. As previously, the strategy of talking to respective providers and offering the option of resolving suspected breaches to avoid a formal procedure will also be adopted in these cases.

Alongside activities previously described as part of the stated procedures concerning existing products, general terms and conditions as well as 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). In this context, it should be noted that the minimum content pursuant to Art. 4(1) TSM Regulation is now also part of the contract terms for many small-scale providers. With respect to this minimum content requirement, no further steps towards formal procedures needed to be taken in the reporting period: the inclusion of this content is now mostly a routine matter.

---

[3] https://www.rtr.at/de/tk/R3_16_Bescheid_18122017

[4] https://www.rtr.at/de/tk/R5_17_Bescheid_18122017

5.1 Blocking of TCP/UDP ports and protocols

The request-for-information procedures revealed that all of the providers surveyed block a variety of ports in the TCP and UDP protocols, typically citing the need to maintain network security and integrity as a reason for doing so (using point (b) of Art. 3(3) third subparagraph as a legal basis). This is problematic, since it restricts end-user rights pursuant to Art. 3(3) third subparagraph.

In terms of port blocking, various circumstances have arisen as a result of procedures that have been completed or are still pending. While significant differences were identified here between fixed and mobile network operators, by no means could consistent patterns of port blocking be recognised. In most cases, the actual grounds for blocking specific ports were clarified in the course of procedures. Some ports were blocked for historical reasons or because of network expansion by the provider in question. Whether or not these ports may be legitimately blocked was and continues to be the focus of completed and current procedures pursuant to Art. 5(1). At this juncture, it must be emphatically stated 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 cannot automatically be used as a basis for assessing the legitimacy of port blocking as practised by other ISPs.

The following section offers a summary of selected case histories.

TCP port 19 (chargen)

One fixed network operator blocked the chargen protocol on TCP port 19 with the justification that the port constituted a security risk due to its age. The operator stated that the chargen protocol constituted a serious security risk since the protocol was suitable for use in DDoS attacks and indeed used to mount such attacks. In light of the fact that there is effectively no further use for the chargen protocol, this block should be considered as having very little impact.

Assessed on the basis of point (b) of Art. 3(3) third subparagraph, this block is considered to be legitimate since there is essentially no further practical use for this protocol.

TCP port 25 (SMTP)

In responding to the request for information, one fixed network operator mentioned a block on port 25 for outgoing traffic. One mobile network operator that prior to initiation of the discontinuation procedure had implemented a differing technical solution – nonetheless also contravening Art. 3(3)) – decided during the procedure to replace the solution by blocking port 25 for outgoing traffic instead. The key reason for such a block is to prevent a customer's computer from sending spam email 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.

Assessed pursuant to point (b) of Art. 3(3) third subparagraph, these blocks are considered to be legitimate since (pure) SMTP is a protocol frequently misused at retail level (for sending spam).

TCP/UDP port 53 incoming (DNS):

One provider stated that they block this port for a certain number of modems that had a firmware fault rendering them vulnerable to attacks via the port. There are plans to remove the block when the model is discontinued.

Since a manufacturer solution was not forthcoming, this block was considered legitimate pursuant to point (b) of Art. 3(3) third subparagraph for a period until the discontinuation of the model.

TCP port 67 bidirectional (DHCP):

One fixed network operator blocks this port for technical reasons based on their network topology, since port 67 is used for assigning addresses to their customers. The provider argued that a DHCP configured with malicious intent could otherwise be used to manipulate IP address assignment in the same network segment as the customer, or to redirect that customer's traffic.

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.

TCP port 69 bidirectional (TFTP):

One fixed network operator had previously blocked this port for technical reasons but removed the block entirely in the reporting period.

TCP port 123 incoming (NTP):

The block assumed to be in place on port 123 proved to be a misunderstanding. The ISP stated that the port was not blocked but, as a less intrusive option, all network traffic via this port is shaped to a particular bandwidth in order to prevent DDoS attacks. This strategy was considered legitimate pursuant to point (b) of Art. 3(3) third subparagraph.

TCP ports 135–139 bidirectional (NetBIOS):

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

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

TCP port 445 bidirectional (SMB):

Two fixed network operators block these ports since the server message block (SMB) protocol that uses these ports is, like the NetBIOS protocol, considered to be a security risk for their customers. In their opinion, there is no logical use case for SMB in a WAN, since SMB is a LAN-based network service. Further evidence submitted in support of the admissibility of such a block is the fact that the WannaCry ransomware used port 445 and SMBv1 as an attack vector.

Following an analysis pursuant to point (b) of Art. 3(3) third subparagraph, the block for incoming traffic was considered legitimate; the block for outgoing traffic was removed by the ISPs.

5.2 Private IP addresses and services

Art. 3(1) also grants end users the right to use or provide their own services. These services range from smart home servers set up for personal use (e.g. temperature monitoring) on appropriate hardware, to web servers operated by end users for third parties.

A key technical prerequisite for the self-hosting of services is therefore the direct accessibility of the server or service operated by the end user from the internet, and therefore the assignment of a public IP address to this user's internet connection.

In mobile networks in particular, it is frequently the case that customers are assigned private IP addresses (via NAT). Apart from technical aspects, reasons for this include the provider's interest in saving on IP addresses – which are already scarce in the case of IPv4.[5] 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. In the opinion of the regulatory authority, the basic right granted to the end user by the provisions of Art. 3(1) should at least be understood to mean the provision of a free public dynamic IP address – at least if the end user requests this address because they want to offer services. The end user can then utilise dynamic DNS services to enable this address to be used to provide their own services. If the assignment of a public IP address is made conditional on payment of an additional fee (such as a specific subscription model) or is reserved for certain customer segments (such as business customers), this must be considered as a contravention of Art. 3(1).

The last reporting period had shown that this problem is especially common with mobile network operators. One very positive development of note is that a solution compliant with the TSM Regulation was found in almost all procedures still ongoing at the start of this reporting period; end users can therefore now request the assignment of at least a dynamic public IP free of charge.

In one case (A1 Telekom), which was decided in December 2017, while end users were able to request the assignment of a dynamic public IP address, this required the payment of an additional charge. This practice was forbidden as being in contravention of Art. 3(1) TSM Regulation,[6] since the individual rights derived from Art. 3(1) TSM Regulation, such as self-hosted services or applications, are not available for separate monetisation.

This problem area will continue to occupy the NRA's attention, also in light of the request-for-information procedures being analysed at the end of the reporting period.

---

[5] While fewer than 2^{32} (approx. 4 billion) addresses are available using IPv4 and are now becoming scarce, IPv6 provides a little under 264 (approx. 18 trillion) subnets and therefore easily enough for the foreseeable future.

[6] Procedure R 3/16, https://www.rtr.at/en/tk/R3_16_Bescheid_18122017, the decision was appealed.

5.3 Zero-rating

A zero-rating product[7] was brought to market in the reporting period. Free Stream, a product by A1 Telekom Austria AG, offers video and music streaming from selected partner services on a zero-rated basis.[8] When the product was introduced to the market in November 2017, video traffic was restricted to 1.7 Mbps for SD content and to 3 Mbps for HD content. This breaches Art. 3(1) and (3) of Regulation (EU) No 2015/2120. The next section gives a more detailed description of the product and the associated procedure. Together with the Austrian newspapers Krone and Kurier, A1 Telekom Austria AG offers a further zero-rating product. These smartphone subscriptions include a free download of the respective versions of the e-newspapers (which are not normally free). Hutchison Drei Austria offers music streaming via Spotify as well as access to its own services – 3Cloud, 3MobileTV, 3Film and 3Kiosk (download of purchased magazines) – on a zero-rated basis. Red Bull Mobile (a brand of A1 Telekom Austria AG) has offered zero-rated access to its Red Bull TV since February 2017. This service can be used until the standard data package is used up, after which all data use is blocked. The zero-rating components of the individual products have not been a problem so far. Yet this assessment could change in the event of an alteration in the market situation (such as through a broader selection or cumulated market effects).

5.4 Technical discrimination and restrictions / modifications by IAS

Art. 3(3) third subparagraph essentially prohibits any kind of technical discrimination or modification of data traffic of end users, unless one of the exceptions listed in points (a) to (c) of the third subparagraph applies.

Some forms of technical discrimination were nonetheless identified in the case of one mobile network operator as part of requests for further information in the previous reporting period, especially with regard to self-hosted streaming and content services. Some of the operator's own services as well as the traffic for two external services/websites were essentially provided free-of-charge (i.e. zero-rated), which was provisionally deemed compatible with Art. 3(2). However, a breach of Art. 3(3) was identified based on the fact that the aforementioned services were also available without restriction once the data included in the subscription was used up – in contrast to other services. While all other services/content/applications could either not be used at all (under subscriptions blocked once the data is used up) or could only be used at a much lower speed (subscriptions throttled to roughly 128 Kbps once the data is used up), the services referred to above were still available at full bandwidth.

What is encouraging in this context is that the procedure – launched in the previous reporting period – could be dropped without an official decision. Following intensive discussions, the products in question were adjusted by the provider involved to make them compatible with the TSM Regulation. Any preferential handling of certain services, such as bandwidth measurements, was also discontinued. This also applies to the switching of data traffic to port 25, as mentioned in the previous report. In this case, the provider opted to block private and dynamic public IP addresses (cf. section 5.1).

---

[7] Zero-rated products and services are ones that can be accessed by users without this use being counted towards the data included in their contract. Consequently the data is essentially used free of charge, and it must be ensured that upon reaching the limit of any data included in the contract there is no technical discrimination of any kind among services or applications (see section 5.4).

[8] The range was expanded during the reporting period both in terms of the subscriptions and the CAPs included.

A change in mind was also achieved without an official decision in the case of another operator who used a proxy server in their network to route all unencrypted web pages retrieved (http traffic) by customers. The ISP deactivated this redirection for the majority of data traffic; as at the date of this report, the changeover was still pending for a small part of traffic, which is why the procedure is open.

In November 2017 the issue of restricting IAS or changing data traffic became very relevant again after A1 Telekom Austria AG launched Free Stream onto the market, an additional package for certain mobile subscriptions that comprises a whole range of zero-rated content services (video and audio streaming). Yet both the CAP participating in the package and the end users had to accept "traffic shaping" of the bandwidths for these services with zero-rating activated. The bandwidths were limited to 1.7 Mbps for SD content and to 3 Mbps for HD content, which for video streaming services in particular like Netflix could result in a reduction of image quality, a potential outcome that A1 Telekom Austria AG also openly admitted in the terms of use for the package.

A procedure under Art. 5(1) TSM Regulation was consequently launched on the same day the product was introduced to the market.[9] Given that the situation was largely confirmed and consequently only the legal issue involving the (non-) permissibility of traffic shaping had to be ruled on, the procedure was completed quickly. A1 Telekom Austria AG argued in detail that agreements on traffic shaping are permitted where end users are able to decide freely whether to use the product. These arguments and justification attempts ultimately came to nothing given the unambiguous formulation of the prohibition applying to ISPs as set forth in Art. 3(3) TSM Regulation: use of any traffic shaping was banned while allowing for a period of eight weeks for technical implementation, in accordance with Art. 5(1) TSM Regulation.

Interestingly, an inexplicable impression has taken hold in the Austrian media that zero-rating per se is banned by the TSM Regulation, even though the regulatory authority or BEREC has never aroused this impression or communicated anything of the sort. This made it more difficult to convey the results of the procedure at hand to the general public.

---

[9] Procedure R 5/17, https://www.rtr.at/de/tk/R5_17_Bescheid_18122017 (in German), an appeal was lodged against the decision.

5.5 Specialised services

As part of a request-for-information procedure, it was found that one of the TV and video-on-demand services offered by A1 Telekom Austria AG via the IAS bandwidth was prioritised. This means that when this service is active, the end-user device reserves a specified bandwidth, which is then no longer available for IAS.

This posed the question as to whether such constituted a specialised service within the meaning of Art. 3(5), with regard to the VoD components (video library and 'catch-up TV').[10] Subsequently, in a procedure under Art. 5(1) TSM Regulation in conjunction with Art. 3(5) as well as Par. 116 et seq. of the guidelines, the issue of the technical need for optimisation (in terms of prioritisation) had to be clarified.[11] A specialised service was assumed for the live IPTV components of the bundled product.

As part of the procedure, a technical and economic evaluation report was commissioned, which after in-depth analysis came to the conclusion that the video-on-demand service did not require data transfer prioritisation either in a technical sense, or in a commercial sense (ultimately given substitutes on the internet). Among other things, A1 Telekom Austria AG argued in detail that the bundled product should be viewed as a whole, and that it was prohibited to 'slice up' services. These arguments could not be accepted because such an approach would allow (or make it reasonable for) providers to 'bundle' specialised and non-specialised services. Following an oral hearing, a decision was ultimately reached just before Christmas 2017, ruling that the VoD service did not fulfil the specialised services requirements given the lack of any need for prioritisation, and therefore the prioritisation of this service should be discontinued. The period set for discontinuing prioritisation was three years, since the service had been provided in this form before the TSM Regulation entered into force and (presumably) in accordance with laws prevailing at that time, while the TSM Regulation provides for no additional transitional periods and the technical changeover is a large-scale endeavour for the ISP.

5.6 Disconnection of IP connections

Another fact limiting the right of end users to self-host services is the automatic disconnection of internet connections (IP connections) after a certain time.

Four of the network providers surveyed in 2016 revealed that the data connections of their customers were automatically disconnected after a certain time (generally 24 hours). No attention is paid in this respect to existing internet connections, in other words, the connection is always disconnected after this period, not only when it is idle. The reasons given by the providers here ranged from technical considerations regarding the assignment of IP addresses to the protection effects claimed for the benefit of user privacy. This measure is a problem mainly because dynamic public IP addresses are reassigned – 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. The frequency of the terminations ultimately means this constitutes a disproportionate restriction of the right of the end user under Art. 3(1).

---

[10] Linear television was already identified in the BEREC guidelines (Par. 113) as a specialised service under certain conditions.

[11] Procedure R 3/16, https://www.rtr.at/de/tk/R3_16_Bescheid_18122017 (in German), an appeal was lodged against the decision.

Except for A1 Telekom Austria AG, and once more without a formal decision, the period before disconnecting IP connections was increased from 28 to 30 days, so that any interference in the direct provision of services by end users was reduced to a necessary minimum.

A1 Telekom Austria AG had stipulated the disconnection of fixed internet access every 24 hours. Since the self-hosting of services or applications by end users is more likely especially with fixed internet access (such as with a private FTP server, home automation systems and similar services), this practice was prohibited in a procedure under Art. 5(1) TSM Regulation[12] and disconnection only after 30 days specified.

5.7 Blocking of websites due to copyright claims

In principle, providers of internet access services may not block, throttle, change, restrict, disrupt, impair or discriminate specific content, applications, 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 EU legislative acts or national laws or related implementing measures.

There is a special copyright provision in Art. 81 Par. 1a of the Copyright Act (UrhG) according to which providers of internet access services can also be obliged to block access to websites that structurally breach the law, if they have previously been properly warned by a rights holder.

In early 2018, the TKK instituted a total of seven supervisory procedures against providers of internet access services that had presumably denied access to particular websites. In the procedures, the providers said they had denied access to some of these websites on the basis of a court decision – such as a provisional injunction or a court ruling. Apart from that, the blocking had allegedly also been implemented based on court settlements or warnings by rights holders and without an official decision.

While courts of law are authorised to grant injunctions on the grounds of copyright law, the regulatory authority is responsible for verifying the traffic management measures to determine whether the specific implementation in the form of access-blocking is compatible with the TSM Regulation. If traffic management measures of this kind are taken by providers of internet access services after a warning by rights holders and without the respective court ruling, the exception pursuant to Art. 3(3) third subparagraph (a) TSM Regulation must also be verified.

At the request of one provider of internet access services, the TKK instituted an assessment procedure. Unlike the supervisory procedures pursuant to Art. 5 TSM Regulation as described above, the supervisory procedure here deals with websites that have not yet been blocked. The assessment procedure has to determine whether an exception exists within the meaning of Art. 3(3) third subparagraph (a) TSM Regulation as well as whether it would be legitimate to subsequently block the websites.

Both the supervisory procedure and the assessment procedure were still at the investigation stage in the reporting period.

---

[12] Procedure R 3/16, https://www.rtr.at/de/tk/R3_16_Bescheid_18122017 (in German), an appeal was lodged against the decision.

5.8 Overview of suspected breaches of net neutrality

Table 3 below provides an overview of cases involving suspected breaches of net neutrality, listing the categories, the number of cases, the status of procedures and the expected duration of procedures. More detailed descriptions of the cases can be found under the individual subsections of section 5.

TABLE 03: OVERVIEW OF CATEGORIES OF SUSPECTED NN BREACHES

KEY: Voluntarily discontinued   Procedure pending

    Procedure terminated   Discontinued by official decision

CATEGORY [13]	NUMBER OF CASES	STATUS OF PROCEDURE	PERIOD
Port blocking	14	8 ▶ 6	Q4/17
Private IP addresses and services	4	3 1	Until Q3/17
Zero-rating	0		
Specialised services (VoD)	1	1	Q4/17
Technical discrimination and restriction of internet access	2	1 1	Q3 and Q4/17
Redirection of traffic	2	1 1	Until Q3/18
No server operation possible	1	1	Q3/17
Disconnection of IP connections	4	3 1	Q3 – Q4/17
Blocking websites due to copyright claims	7 [14]	1	

---

[13] The zero-rating category, mentioned in Table 2 as a problematic practice in the context of the TSM Regulation, is not considered in this table, as zero-rating as such has yet to result in an official procedure. The limited number of products on the market is constantly monitored by the regulatory authority.

[14] Seven procedures were launched but the number of websites affected is higher.

5.9 Measures taken/applied in accordance with Art. 5(1)

With regard to compliance with the provisions of Art. 5(1) TSM Regulation, in the first reporting period (until April 2017) no measures as defined in Art. 5(1) TSM Regulation were considered necessary. This was due to dialogue being initiated with the companies early on and discussions usually resulting in constructive solutions compliant with the TSM Regulation. Nevertheless, the regulatory authority naturally monitored compliance with the provisions of Art. 3 and Art. 4 TSM Regulation on an ongoing basis.

Activity in this reporting period partially follows this trend, although in December 2017 the first two decisions on measures pursuant to Art. 5(1) TSM Regulation had to be issued. Both decisions concerned A1 Telekom Austria AG. The procedures were already mentioned in sections 5.2, 5.4 and 5.5. Both decisions issued in the reporting period were appealed before the Federal Administrative Court (BVwG). In addition, in both proceedings, a petition for suspensory effect was filed with the BVwG to suspend the enforceability of the decisions until a ruling in the main case is handed down. These petitions were not granted, so the decisions remain in force.

TABLE 04:   PROCEDURES IN ACCORDANCE WITH ART. 5(1) TSM REGULATION
IN REPORTING PERIOD

LEGENDE: ⚖ Appealed   ✓ Final

PROCEDURE	NETWORK OPERATOR	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 30 days.	2017-12-08	⚖
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.	2017-12-08	⚖

06 6 Further indicators/activities
on net neutrality in the reporting period

6.1 RTR conciliation procedures

Within the scope of conciliation procedures (Art. 122 TKG 2003), RTR's conciliation body processes requests of customers who do not agree with the services or the billing of their telecoms provider. In the reporting period for this report, a total of 1,783 conciliation requests were filed.

One important subject within conciliation procedures with regard to the TSM Regulation concerned complaints about network quality. Such complaints usually do not concern the failure to supply minimum content as required by Art. 4 TSM Regulation (such as minimum speed, maximum speed, normally available speed and advertised speed), since these parameters are already verified in the objection procedure pursuant to Art. 25 TKG 2003. The complaints concern the bandwidth available to customers in specific individual cases (upload and download speed). In most cases, these relate to an alleged 'inadequate performance' of the contract by the telecoms provider. The procedure involves compulsory verification as to whether the service is actually provided as contractually agreed. If for example a low bandwidth is agreed with the customer in the contract and the maximum speed of a mobile connection is set very low, the customer could perceive the service as being 'inadequate' but cannot enforce any claims as long as the service complies with the terms.

The number of complaints in connection with bandwidth in the current reporting period roughly corresponds to the number in the preceding reporting period (see below), and there was also a comparable number before the TSM Regulation entered into force. Thus, there was no direct increase in complaints in this area as a result of the TSM Regulation. With regard to 'quality of mobile networks', the conciliation body received a total of 112 requests in the reporting period (first reporting period: 110).

Relating to 'quality of fixed networks', there were 21 requests in the reporting period (first reporting period: 26).

6.2 General requests

RTR also receives enquiries regarding net neutrality aside from conciliation procedures. Specifically, there were enquiries regarding minimum content pursuant to Art. 4 TSM Regulation, zero-rating and port blocking.

6.3 Indicators of the continuous availability of non-discriminatory internet access services

Art. 5(1) TSM Regulation prescribes that national regulatory authorities must ensure compliance with Art. 3 and Art. 4 TSM Regulation and promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology.

To give a long-term perspective and to be able to assess progress better, we present below the development since Q1 2015. The charts are interpreted only for the reporting period, however. For some indicators, no figures were yet available for Q1 2018 when the report was compiled, but those that were available are reported.

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

- Number of broadband connections
- Distribution of download and upload speeds in the reporting period
- Median of download and upload speeds and latency over time
- Distribution of download and upload speeds by hour of day
- Hedonic price index[15] for broadband products
- Quality dimensions

---

[15] In addition to product price, the hedonic price index also integrates product features (in particular download rate and download volume) and is calculated using a regressive analysis of prices in relation to product features and time variables. Detailed information on the hedonic price index is available in the RTR Telekom Monitor.

FIGURE 03:   FIXED AND MOBILE BROADBAND CONNECTIONS[16]
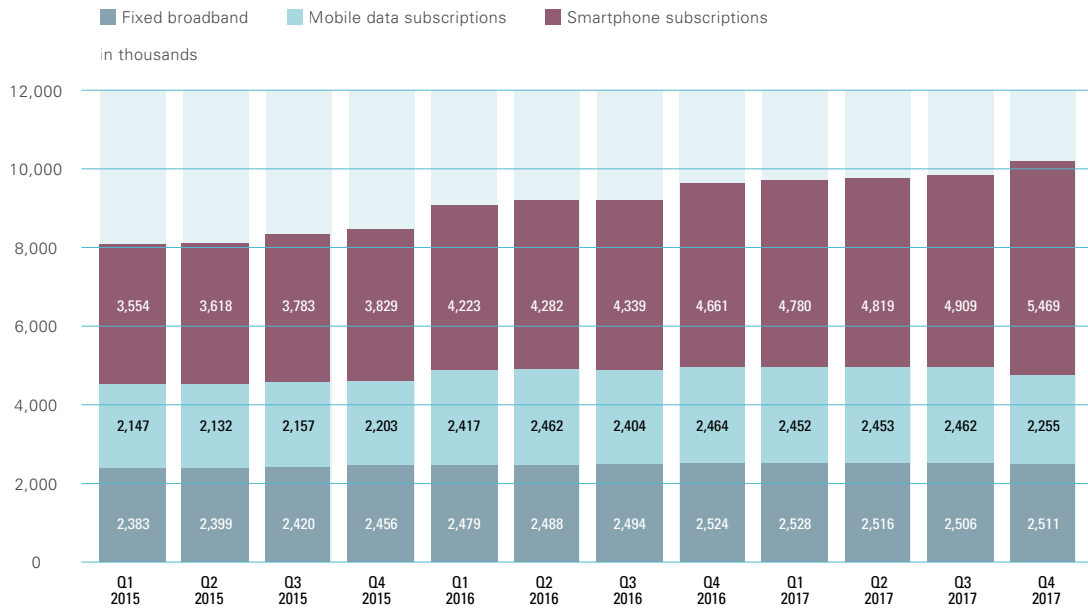
Source: RTR

Figure 3 shows a continuous increase in the number of broadband connections since 2015. The number of smartphone subscriptions in particular has risen. In terms of the reporting period this means that the number of smartphone subscriptions rose (not least due to an amendment in the Communications Survey Ordinance (KEV), see footnote 15) from 4.82 million to 5.47 million between Q2 2017 and Q4 2017. The number of mobile data subscriptions fell from 2.45 million in Q2 2017 to 2.26 million in Q4 2017. The number of fixed broadband tariffs remained almost unchanged (2.52 million in Q2 2017 compared with 2.51 million in Q4 2017).
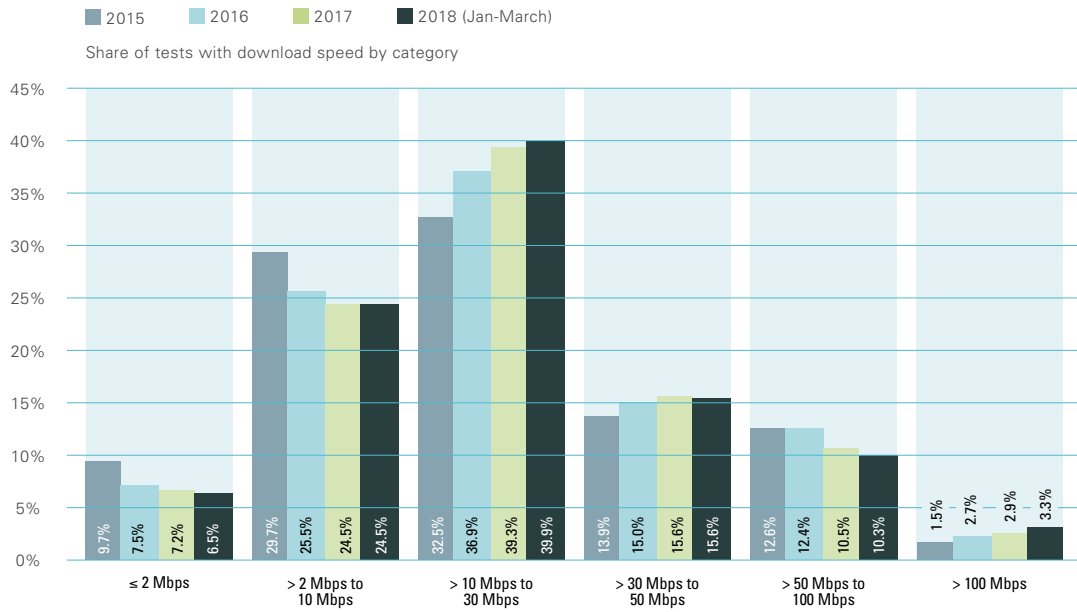
Data (Open Data)[17] generated with the help of the RTR-NetTest[18] is used to assess the quality of internet access. The RTR-NetTest allows users to check the speed and quality of their internet connection, reliably and independently of their provider. From Q2 2017 up to and including Q1 2018, the RTR-NetTest was used for unrepeated measurements over 786,000 times in Austria (with a location accuracy of less than 2 km). More than 215,000 of the tests were mobile service measurements.

[16] Data on broadband connections is collected quarterly in accordance with the Communications Survey Ordinance (KEV) but was not yet available when this report was prepared for Q1 2018. In comparison with the net neutrality report of the previous year, the definition of mobile broadband connections was revised from Q4 2017 under the amendment to the KEV. Specifically, from the fourth quarter post-paid connections are only counted if the internet was accessed at least once in the quarter. This explains the fall in the category of mobile data subscriptions from the third to the fourth quarter of 2017. Until Q3 2017, smartphone subscriptions were only counted if they were post-paid contracts. From the fourth quarter of 2017, all subscriptions regardless whether they are post-paid or pre-paid are considered smartphone subscriptions if both data as well as minutes and text messages are included.

[17] The Open Data of the RTR-NetTest is available at https://www.netztest.at/en/Opendata.html.

[18] Available as a mobile app (Android, iOS) and as a browser test. For details see https://www.netztest.at/en/.

FIGURE 04:   DISTRIBUTION OF DOWNLOAD SPEEDS OVER REPORTING PERIOD

■ 2015   ■ 2016   ■ 2017   ■ 2018 (Jan-March)

Share of tests with download speed by category

	≤ 2 Mbps	> 2 Mbps to 10 Mbps	> 10 Mbps to 30 Mbps	> 30 Mbps to 50 Mbps	> 50 Mbps to 100 Mbps	> 100 Mbps
2015	9.7%	29.7%	32.5%	13.9%	12.6%	1.5%
2016	7.5%	25.5%	36.9%	15.0%	12.4%	2.7%
2017	7.2%	24.5%	39.3%	15.6%	10.5%	2.9%
2018	6.5%	24.5%	39.9%	15.6%	10.3%	3.3%

Source: RTR-NetTest

Figure 4 reveals the proportions of tests with download speeds in a given category. It is clear that back in 2015 most of the measurements display download speeds of 10 to 30 Mbps; this share increased in the subsequent years. The ratio of measurements under 2 Mbps dropped between 2015 and 2018, while the proportion of measurements in excess of 100 Mbps rose over the same period.

FIGURE 05: DISTRIBUTION OF UPLOAD SPEEDS OVER REPORTING PERIOD

■ 2015 ■ 2016 ■ 2017 ■ 2018 (Jan-March)

Share of tests with upload speed by category
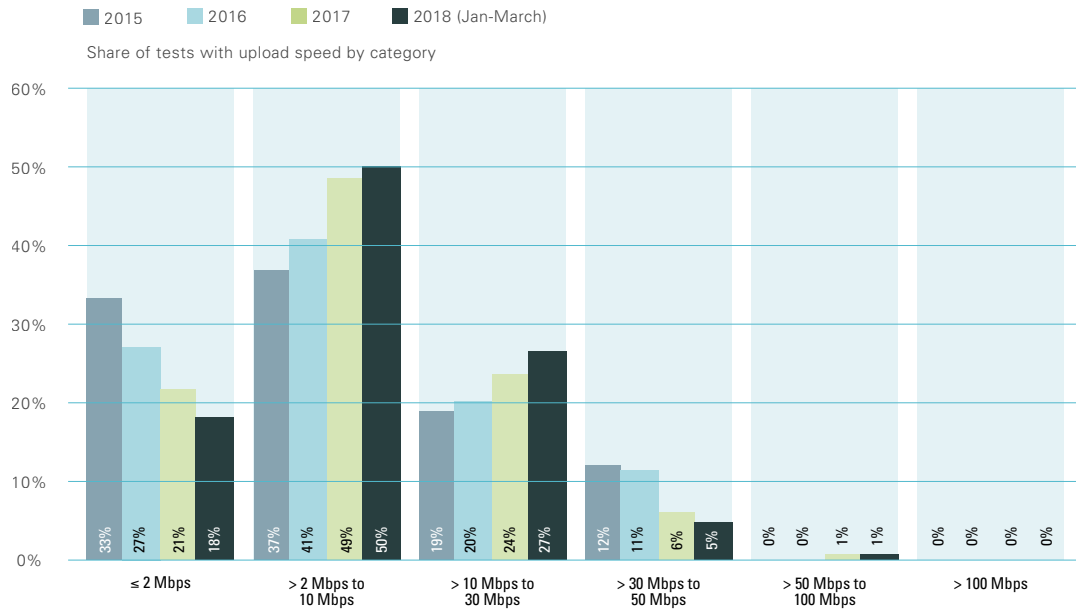
Source: RTR-NetTest

Figure 5 depicts the ratios of tests with upload speeds in a given category. Back in 2015, most of the tests showed an upload speed of 2 to 10 Mbps, and this figure has risen sharply over the years. It is also clear that the proportion of tests with an upload speed of less than 2 Mbps has fallen sharply. Interestingly, the proportion of tests with an upload speed of between 30 and 50 Mbps has dropped since 2015.

FIGURE 06:   DOWNLOAD SPEED BY TECHNOLOGY

■ (W)LAN ■ 3G ■ 4G

Median in Mbps
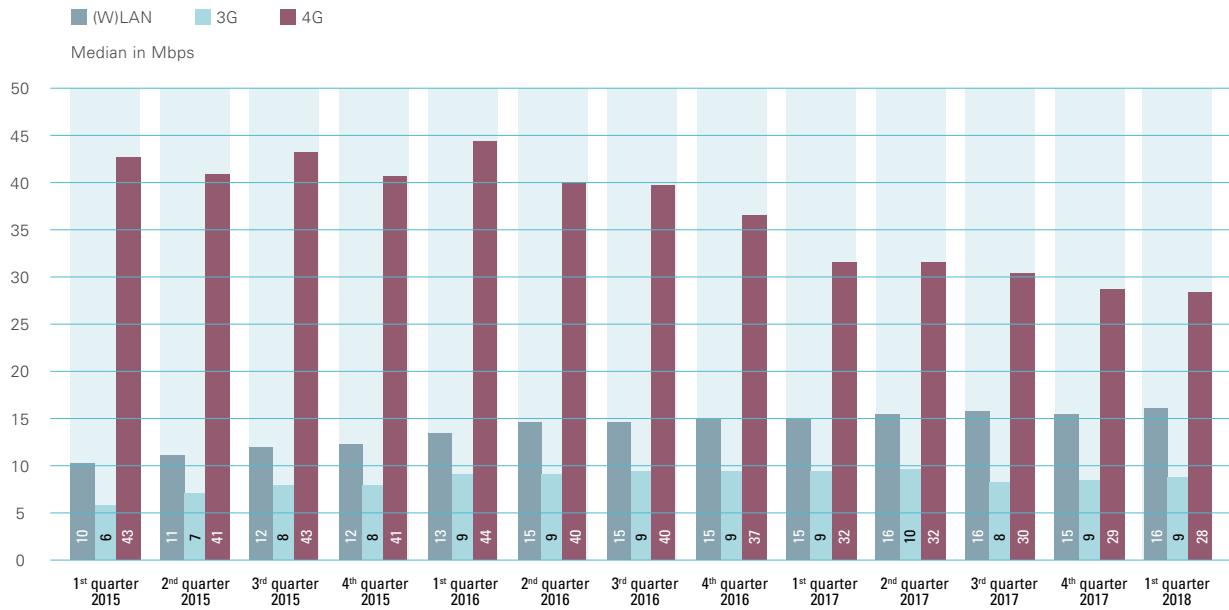
Data: RTR-NetTest

Figure 6 depicts the median[19] download speed measured with the RTR-NetTest over time, broken down by type of technology. It is clear to see that far higher download speeds can be reached on average with 4G mobile telecommunications technology than with (W)LAN or 3G. However, the download speed for 4G has fallen continuously since the start of 2016. This trend continued in the reporting period as well. As reported last year there has been a sharp increase in the number of customers using 4G. This may be one reason for the decline in download speed.[20] 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 'occupied' through competition on the market until the next technology (often associated with new spectrum) creates in turn new capacities. Consequently, it cannot be concluded from the figure that the quality of connections has deteriorated, and furthermore there is no connection here to net neutrality. Of all the technologies assessed, the lowest download speeds were achieved with 3G. In light of the low data transmission rates possible, 2G connections are not included in this and subsequent assessments. The download speed for (W)LAN was relatively constant or rose slightly in the reporting period.

---

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

[20] See: https://www.rtr.at/de/inf/TK_Monitor_Q3_2017/RTR_Telekom_Monitor_Q3_2017.pdf (in German)

FIGURE 07:   UPLOAD SPEED BY TECHNOLOGY
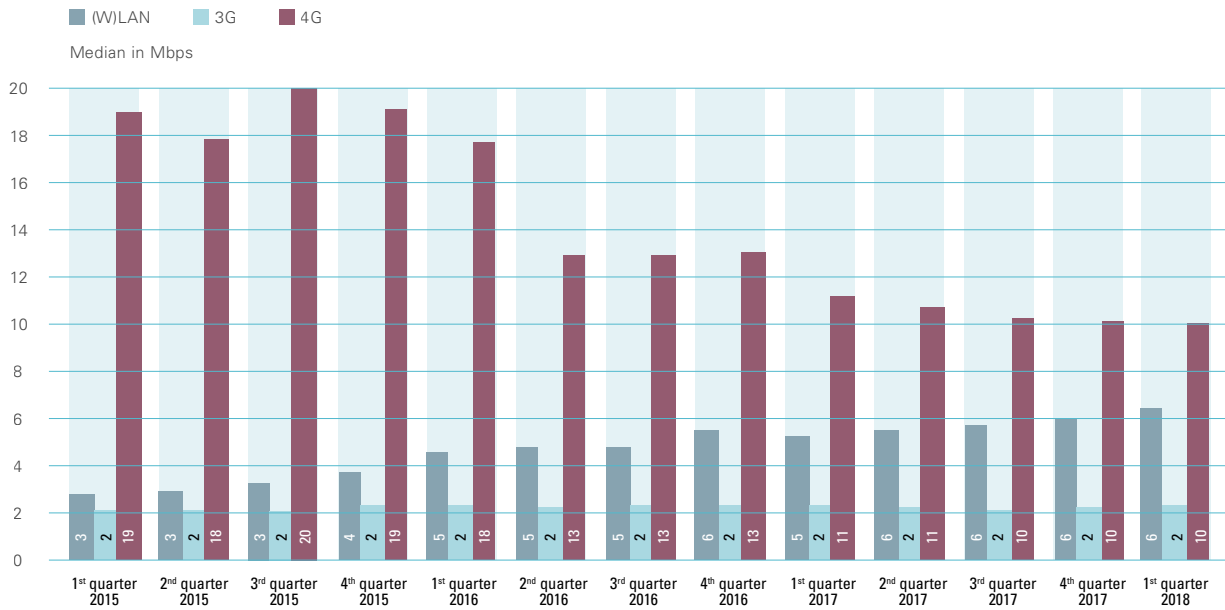
Data: RTR-NetTest

Figure 7 depicts the median upload speed. Again it is seen here that 4G mobile technology allows the fastest upload speeds to be reached, though a decline since 2015 is also recognised which continued through the reporting period (see above). The uplink speed for (W)LAN measurements has risen constantly. The uplink speed for 3G mobile connections is relatively constant.

FIGURE 08:   LATENCY (PING) BY TECHNOLOGY[21]

■ (W)LAN   ■ 3G   ■ 4G

Ping in ms
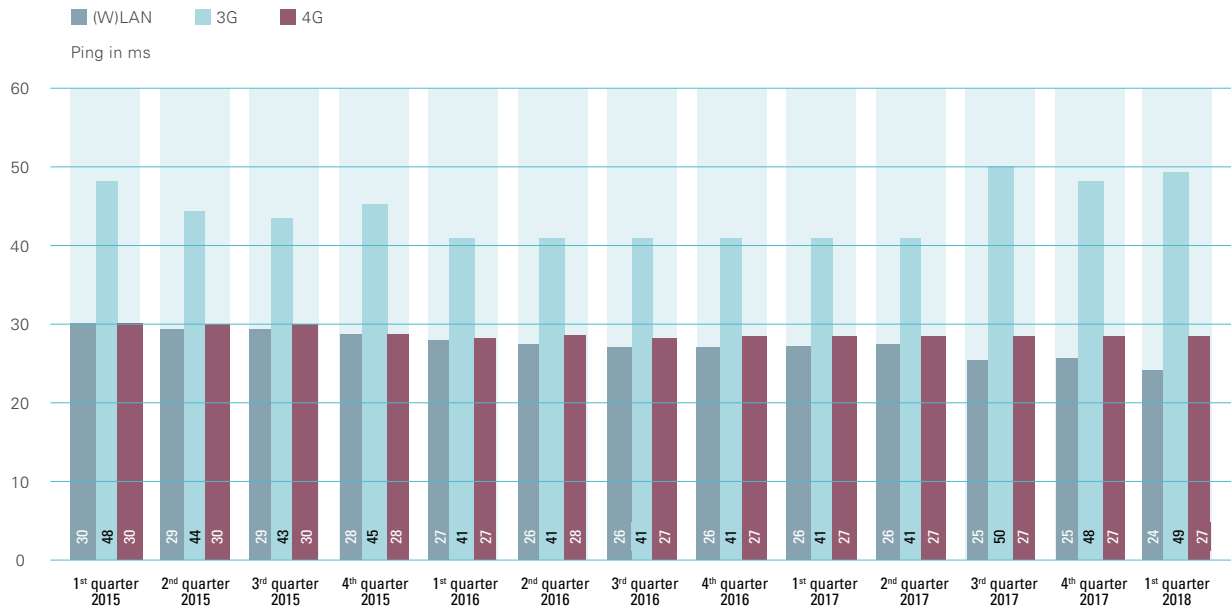
Data: RTR-NetTest

Figure 8 depicts the median latency. Roughly the same figures are achieved using 4G mobile technology and (W)LAN. The figures are relatively constant in the reporting period. With 3G, however, the latency is much higher, and has risen sharply since Q3 2017.

---

[21] 'Ping' (or 'latency', to give it the technically correct term) is the time needed by a small data packet to make its way from a user device (such as a mobile or laptop) to an online server and back. The ping time is measured in milliseconds (ms). The ping time is a key indicator for online games, but the ping time can also have a significant impact on the 'sluggishness' of access when normally surfing in the internet. The delay can be markedly influenced both by the technology applied to access the internet and its level of utilisation.

FIGURE 09:   DOWNLOAD AND UPLOAD SPEEDS BY TIME OF DAY IN 2017
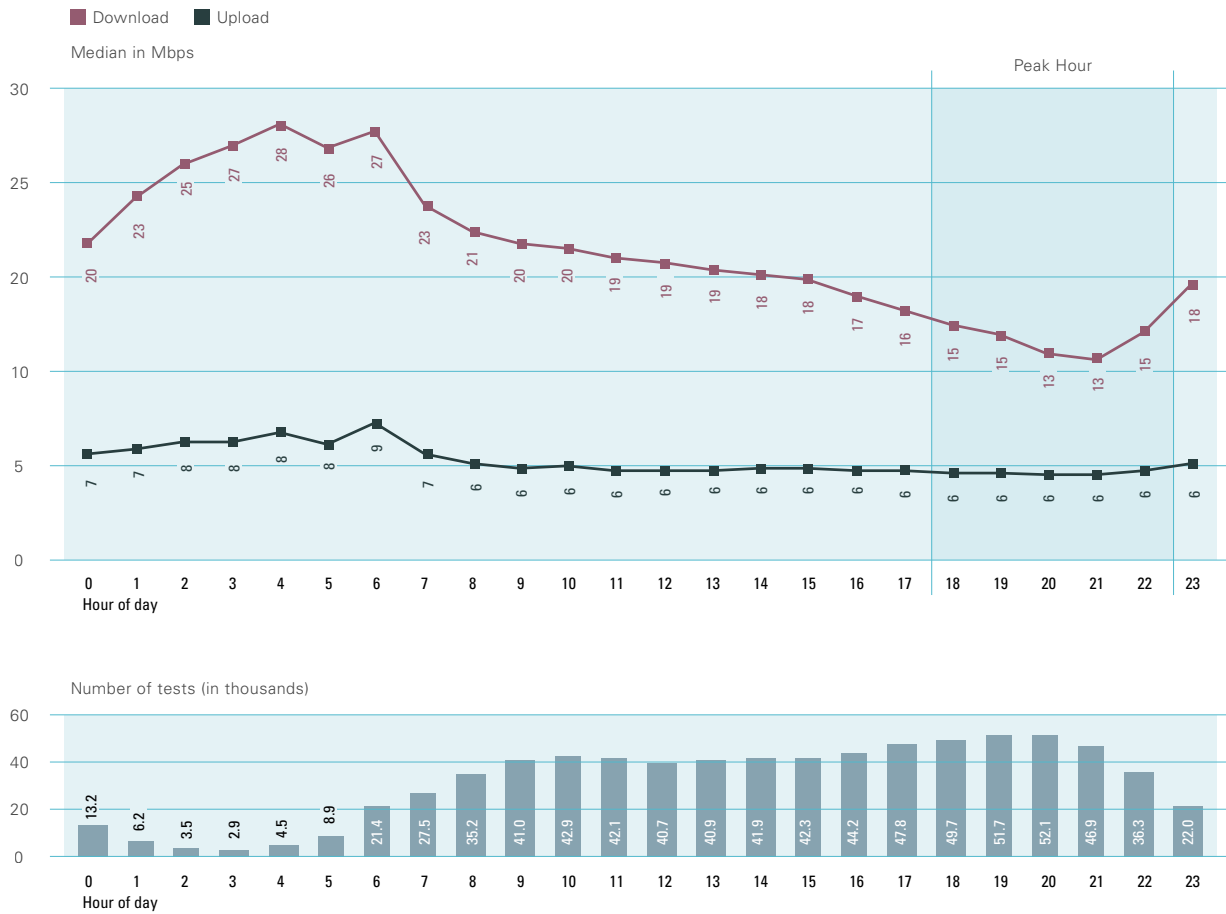
Data: RTR-NetTest

Figure 9 shows that the median download speed in peak hours, which here means between 17:30 and 22:30, has fallen sharply, but the median upload speed is less affected. During early morning hours between 4:00 and 6:00 the download speed is the highest at roughly 28 Mbps. In the course of the day the median download speed drops continuously to only 13 Mbps between 21:00 and 22:00. The median upload speed during the day is relatively steady at about 6 Mbps.

FIGURE 10:   BROADBAND PRICE INDEX (HEDONIC)

Index points (base year = 2010)

■ fixed   ■ mobile   ■ fixed and mobile
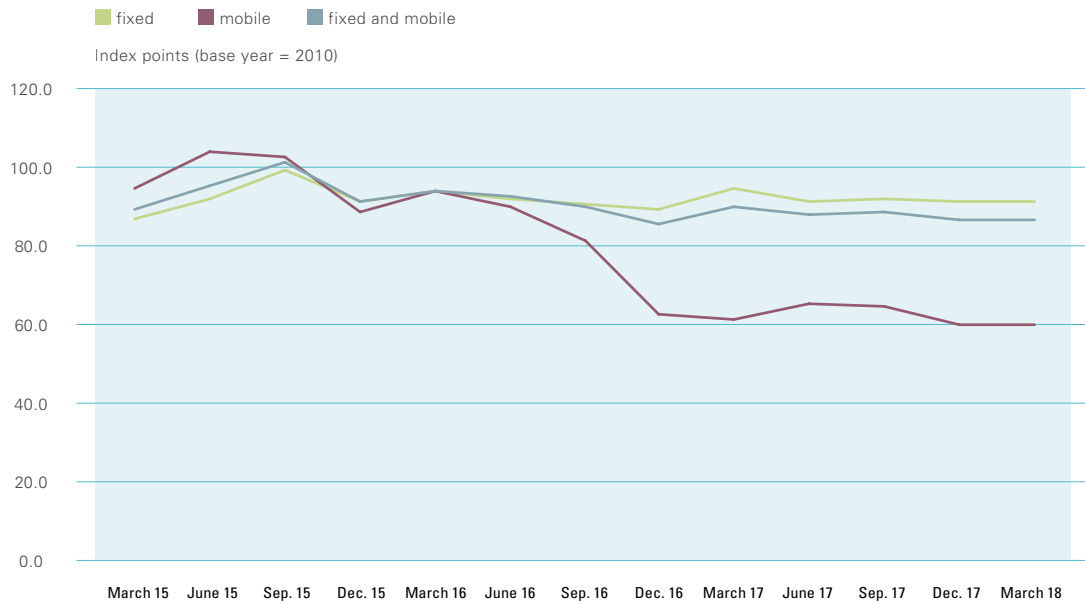
Source: RTR

The hedonic price index for fixed and mobile broadband products remained almost unchanged from April 2017 to March 2018, and the same applies when the changes in fixed and mobile broadband products are viewed individually. Nonetheless, the mobile price index reveals greater fluctuations over the year. This can be attributed to the fact that hardly any changes in prices or product features were seen, apart from the increase in service charges by one large network operator. If we compare the levels of the fixed and mobile price index, it is interesting that the price index for fixed broadband products is roughly 30 index points higher than that for mobile broadband products.

FIGURE 11:   QUALITY OF SERVICE TEST (RTR-NETTEST)

Quality of Service		
Web page	■■	1/1 - details
Unmodified content	■■	2/2 - details
Transparent connection	■■	5/5 - details
DNS	■■	33/33 - details
TCP ports	■■	16/18 - details
UDP ports	■■	11/13 - details
Traceroute	■■	1/1 - details

Source: RTR-NetTest – Open Data from quality test

Figure 11 shows an example of a result from the RTR-NetTest quality of service test. A green light depicts a positive result for a test. Next to the light, the number of positive tests carried out in the given category is shown relative to the total number of tests. A precise description of the test can be found at https://www.rtr.at/en/tk/netztestfaq_qos. Using the QoS tests, end users can determine how well they can use their internet access. A red light indicates possible restrictions with certain uses. With the test referred to above as an example, two TCP and two UDP port tests failed. The actual results of the failed tests can be viewed under 'details'. In this case the end user had a private IP address, which does not allow incoming connections to the user. The end user in this example would not be able to operate an online server.

If we take a look at the indicators above, it can be concluded that the availability of non-discriminatory internet access services in Austria was ensured over the reporting period. There is no evidence that the fluctuations are connected to net neutrality. What is encouraging, though, is that broadband subscriptions did not become more expensive in the reporting period and no notable declines in download and upload speeds were identified. No negative impact on access to non-discriminatory internet access services has yet been observed due to the presence of zero-rating products on the market. However, should the number of customers using these products rise in the future, or should the market change, these products will need to be evaluated again.

07 **Outlook**
on further activities

The Austrian NRA began to deal very early on with the issue of net neutrality, and was therefore able to exert an influence on the legal development and the design of the guidelines. Furthermore, companies in the sector were given valuable information at a very early stage and the authority was available for product development as an expert partner.

This proactive approach that was also the guiding principle of the second reporting period is to be maintained in the future. Specifically, the following activities are planned for 2019 and until the preparation of the next report in June 2019:

Monitoring activities

1. **Continuation of network transparency study and implementation of further surveys.** Further studies are planned in the coming reporting year on the transparency status of transmissions (whether traffic is modified). As in the past, requests for further information and additional steps will be launched if need be in the event the corresponding evidence is found.

Section 5 referred to these other official tools to verify conformity with the provisions of the TSM Regulation:

2. **Additional requests for information.** As presented in the timelines in section 4.1, surveys at another 13 network operators were started in February/March of this year. The request-for-information procedures were still ongoing when this report was prepared and will continue to preoccupy the authorities in the coming reporting year.

3. **Customer complaints as a source of information.** Customer complaints are considered a further source of information for any breaches of the TSM Regulation provisions. Discussions will be held and procedures launched in the event of any peculiarities, repeated complaints or similar developments.

4. **Ongoing review of general terms and conditions.** The fourth instrument relates to the powers under Art. 25 TKG 2003, according to which all general terms and conditions must be submitted to the regulatory authority and can also be contested by the TKK – where any provisions of Art. 4(1) TSM Regulation are breached. This supports the monitoring of compliance with TSM Regulation provisions. RTR will monitor any significant products that touch on net neutrality issues but are in principle permitted by the TSM Regulation; such issues include zero-rating within the data cap, development of the internet in general and proliferation of specialised services.

5. **Information from ongoing market observation.** Under the KEV[22] the regulatory authority periodically collects information on the development of the internet access markets, product data transmissions, implemented technologies and other items, and makes this available along with analyses derived from that information (such

---

[22] Communications Survey Ordinance (KEV), 2004, as amended in 2012.

as hedonic prices and the mobile price index). Additionally, the continuous further development of the RTR-NetTest provides a significant instrument to measure quality and data transmission speeds. On the whole, this provides a foundation for further RTR indicators and analyses. All of the relevant information is published in RTR's quarterly Telekom Monitor, and can be downloaded as Open Data[23] by interested parties. In the course of 2018 more information about the development of the internet in Austria (and internationally) is to be offered, and made available to the public in a new product.

International cooperation

The special significance of international cooperation in the context of net neutrality was highlighted in the executive summary and in section 3. Collaboration at this level will continue in the coming reporting year (05/2018 to 04/2019) with the following priority areas: [24]

1. The international exchange about ongoing procedures among regulatory authorities, aimed at a harmonious implementation of net neutrality provisions (within the framework of BEREC but also bilaterally), will continue in 2018/2019 as well as the joint discussion and analysis of relevant products.

2. A BEREC report on implementing the TSM Regulation will be compiled and published towards the end of 2018. The report will be based on the national reports on net neutrality to be released by 30 June 2018 and on the BEREC data survey to be carried out in June 2018.[25] Work is also under way on a BEREC opinion assessing net neutrality regulation. As part of this work there was a public consultation in spring 2018, the results of which (consultation report) are also to be published at the end of this year.

3. Another focal area as part of BEREC's international activities for 2018 concerns the development of a tool to check the quality of internet access services (in light of the objectives set forth in Art. 4 and Art. 5 TSM Regulation). The tender procedure was still under way at the time this report was published. Once the contract is awarded, development of the tool is to begin in the second half of 2018 and be completed by the end of 2019. In the form of an app and a browser app, this tool will directly enable end users to measure quality criteria relating to their internet access service and identify any potential breaches of net neutrality. As the basis for this, an expert group within BEREC coordinated and consulted on a uniform technical specification

---

[23] See Open Data Portal of the RTR, https://data.rtr.at

[24] The following details are based largely on the BEREC Work Programme 2018: https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/7528-berec-work-programme-2018. The 2019 Work Programme is currently being drafted and should be finally adopted in late 2019.

[25] BEREC Report on the Implementation of the Net Neutrality Regulation.

of various test metrics, which was published as a document.[26] This describes, for example, techniques for identifying internet speed, the availability of blocked ports or the discrimination of streaming traffic. Another document was published at the same time,[27] which presents how these metrics can be implemented in the future tool while applying the Open Source and Open Data principles. As the regulatory authority holding the BEREC chairmanship in 2018, RTR has played an instrumental role in these activities.

4. Since the 2019 Work Programme is just being drafted at international level, we cannot take any further look ahead at this point. However, the items that will be crucially important in activities until April 2019 obviously include: work on reviewing the TSM Regulation (Art. 9 TSM Regulation requires the European Commission to review the Regulation by 30 April 2019) and the accompanying guidelines, and the focal area of '5G – net neutrality'.

Cooperation with network operators

After a range of events and discussions in the context of adopting the TSM Regulation and the BEREC guidelines, the current reporting year was characterised by procedures and discussions on how to resolve certain practices deemed problematic from a net neutrality perspective can be resolved. Elsewhere in this report we explained how certain practices were transparent for and tolerated by the authority in certain cases, while solutions were found in many other cases in consultation with the network operator. As previously, the regulatory authority continues to encourage all network operators, interested institutions and other stakeholders to take part in an open dialogue about any issues that might arise as well as new developments and concerns about net neutrality.

Information for the public and further considerations

Provided related information is permitted to be made publicly available, the activities mentioned will be accessible on the RTR website, and links to further content on the websites of BEREC and other institutions will be provided.[28]

Alongside the product mentioned above, which will appear for the first time in the course of 2018 and include significant statistics on the internet and developments in this area in Austria, RTR is planning further activities related to the internet and broadband in the coming reporting year.

Finally, it should be pointed out that the statutory rules on penalties for non-compliance with the provisions of the TSM Regulation were required to be implemented by 30 April 2016, in accordance with Art. 6 of the Regulation. The preparation of the legislation was under way at the time of this report, but not yet completed.

---

[26] BoR (17) 178 (https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_
bestpractices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology

[27] BoR (17) 179 (https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7296
-net-neutrality-measurement-tool-specification)

[28] See following link: https://www.rtr.at/en/tk/Internationales

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

Here, as described 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 05:   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"	Executive Summary
"description of the monitoring activities carried out by the NRA"	Section 5 and section 6
"the number and types of complaints and infringements related to the Regulation"	Section 5 and section 6
"main results of surveys conducted in relation to supervising and enforcing the Regulation"	Section 4.2, section 5
"main results and values retrieved from technical measurements and evaluations conducted in relation to supervising and enforcing the Regulation"	Section 4.2
"an assessment of the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology"	Section 6.3
"measures adopted/applied by NRAs pursuant to Article 5(1)"	Section 5.9

Publishing information

Owner and publisher

Responsible for content

Conceptual design and text

Graphic design and layout

While all contributions to the 2018 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