RTR

RTR NET NEUTRALITY REPORT

2019

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

www.rtr.at

2019

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
web: www.rtr.at

RTR NET NEUTRALITY REPORT

2019

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

Contents

Net Neutrality Report 2019

	Contents	**4**
1	**Executive summary**	**6**
2	**Introduction**	**10**
3	**Stakeholders, institutions and the scope of TSM Regulation enforcement**	**12**
4	**Timeline of regulatory authority activities**	**14**
4.1	Timelines	14
5	**Potential violations of net neutrality and associated procedures**	**16**
5.1	Blocking of TCP/UDP ports or protocols	19
5.2	Private IP addresses and services	21
5.3	Technical discrimination and restriction / change of IAS	22
5.4	Disconnection of IP connections	22
5.5	Blocking websites due to copyright claims	23
5.6	Overview of suspected breaches of net neutrality	32
5.7	Measures in accordance with Art. 5(1)	33
6	**Other indicators and activities**	**36**
6.1	RTR conciliation procedures	36
6.2	General requests	36
6.3	Indicators of continuous availability of non-discriminatory internet access services	37
7	**Focus topic: zero-rating**	**48**
7.1	What is zero-rating?	48
7.2	A look at the consumer side	52
7.3	Wholesale level: the CAP–ISP relationship	57
7.4	Empirical econometric analysis of zero-rating in the EU	60

8 Outlook on further activities 62

9 Appendix 66

9.1 Mapping of the report to the structure of the guidelines 66

9.2 Index of figures and tables 67

9.3 Abbreviations 68

01 Executive Summary

The 2019 Net Neutrality Report is the third report by RTR on the current status in Austria relating to open internet access. This report is based on the EU's TSM Regulation, which came into force in November 2015 and sets out the most important rules concerning net neutrality. In the simplest terms, net neutrality essentially relates to the equal treatment of data transmitted via the internet, independently of the sender, recipient or chosen application. In a continuation of the practice adopted in previous reports, this report also presents the activities and measures undertaken by the regulatory authority in the year under review (1 May 2018 to 30 April 2019) to ensure open internet access. Accordingly, the report covers the 'what, when and how' of net neutrality regulatory activities. The 'who' is also worth mentioning briefly: the amendment to the Telecommunications Act 2003 (TKG 2003) in December 2018 explicitly assigns to RTR responsibility for the request-for-information procedures pursuant to Art. 5(1) the TSM Regulation, which precede the supervisory procedures (remit of the TKK).

Alongside this summary of the ongoing activities of the regulatory authorities, market developments are also presented where these are relevant to the discussion of various aspects of net neutrality. One new feature of this report stems from the regulatory authority's decision to dedicate part of it to a focus topic, so as to provide interested readers or persons affected by relevant standards with deeper insights into decisionmaking, relevant approaches or international developments. The key topic for this year's report is zero-rating.

A major focus of activities again in the year under review was to coordinate, under the umbrella of BEREC, enforcement of the TSM Regulation with NRAs in other Member States. Variations in enforcement practices among Member States entail a risk of distortions in competition between national markets. This, in turn, may have a detrimental impact on the ability of the internet to foster innovation, since content and application providers (CAPs) in particular may face differing conditions. Accordingly, RTR once again prioritised its activities aimed at contributing to and shaping discussions on enforcement of the TSM Regulation and on the forthcoming review of the BEREC guidelines at international level in the current reporting year – in particular because RTR chaired BEREC until the end of 2018, with one of the key tasks within this remit being the harmonised application of legal provisions. This international involvement also had repercussions for discussions within Austria. As in the past, RTR continued to pursue its strategy of constructive dialogue. 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. At the same time, 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.

In the year under review, the regulatory authority's national activities concentrated primarily on the processing of request-for-information procedures opened in early 2018 against 16 providers (mobile and fixed network providers) selected on account of their size. The potential violations of net neutrality thereby identified were generally similar in nature to those observed in earlier procedures (cf. table 3): Essentially, these relate to the topics of port blocking, the availability of private IP addresses and, in consequence, the (in)ability of customers to offer their own services, and the disconnection of IP connections. Very broadly, it can be said that enforcement work in recent years has continued to improve both the level of awareness and readiness to work together on these issues on the part of affected companies.

Alongside monitoring potential net neutrality violations, a second focus in the current reporting year was the blocking of websites as a result of copyright claims. Between early 2018 and April 2019, the TKK initiated a total of 14 supervisory procedures in this context, of which 13 were concluded before the end of the reporting period. Art. 81 Par. 1a of the Copyright Act (UrhG) includes a special copyright provision, according to which providers of internet access services can be obliged to refuse to provide access to such websites. Similar provisions for other areas of the law (enforcement of state monopoly on gambling, child protection etc.) are frequently discussed. As of this writing, however, it is unclear whether or how these may result in a new remit for RTR.

A third and last point of focus for RTR at national level concerns its indepth activities related to zero-rating. Zero-rating, which refers to customers using services without the precipitated data transfers being deducted from the data volumes included in their tariff plans, is now a widespread practice within Europe and one that requires particular attention from a net neutrality perspective. This year's report includes a special section on zero-rating practices in relation to Austria. At the same time, RTR has also prepared a comprehensive comparison of empirical work on zero-rating in 15 EU Member States, in which some key concerns about zero-rating are assessed in detail.

What then can be observed in general about the state of open internet access in Austria during the year under review? The overall picture continues to be highly positive. Companies suspected of breaching net neutrality rules generally identified constructive solutions, which were then approved by RTR and implemented (or scheduled for implementation). Procedures were also dropped in a significant percentage of cases after plausible arguments were given or the case was reviewed, revealing that operators had not overstepped the mark when imposing blocks. On the other hand, it is regrettable that court decisions are still awaited on some key topics (specifically: specialised services and technical discrimination) on which the regulatory authority had already ruled in 2017.

There were no substantive changes as regards the introduction of new products or services in the year under review. In the context of the TSM Regulation, probably the most important development was in relation to zero-rating and the fact that A1 Telekom Austria had redesigned its entire core product portfolio (A1 Go product family and b.free) to make zero-rating a feature of every new private or business customer tariff. This is expected to drive a substantial increase in the customer base. However, since the offer has been made transparently and the ratio of zero-rating to overall data consumption or the volume included in the plan is relatively minor, there are no serious grounds for intervention at the moment. In addition, other domestic mobile operators are tending to withdraw zero-rated options or are not launching products with such features.

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 significantly impacted by products or practices that are relevant for net neutrality. While broadband product pricing is apparently not following any significant or obvious trend, stronger growth is being seen in the number of smartphone subscriptions, while moderate migration towards higher bandwidths is observed in general. Transfer speeds also improved, by an average of 2 Mbps for downloads and 1.3 Mbps when uploading, while latency is roughly the same year-on-year.

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. The degree of 'readiness' as regards net neutrality should also be increased in the coming year by the involvement of additional groups of providers, and a study on the transparency of data transmission in networks is also planned. A review of the main provisions of the TSM Regulation on the part of the European Commission will be another focus of activities at international level in the forthcoming reporting year, as will work on developing a tool for investigating the quality of internet access services. RTR will also be monitoring developments in relation to the 5G standard and network modifications.

Last but not least, it should be noted that the openness of the internet and its power to innovate is not decided merely by services providing access to the internet, as offered by ISPs, but is also influenced strongly by developments in user devices, operating systems, app stores and apps. This extended context has now been examined for the first time by RTR in a study published in the current reporting year (https://www.rtr.at/en/inf/OffenesInternetApps2019/). Similar studies on the broader context of open internet access are also planned for the future.

Vienna
June 2019

Johannes Gungl

Managing Director
Telecommunications and Postal Services Division
RTR

02 Introduction

With this, its third Net Neutrality Report, RTR not only provides continuity from the last issue in terms of both content and reporting structures but also includes a section dedicated to focusing in greater detail on one specific net neutrality topic: namely zero-rating. This is an approach that will continue in the future in order to help the broader public gain a deeper understanding of monitoring activities and the overall ‘state of play’ for net neutrality in Austria.

Providing a straightforward definition of the term net neutrality (NN) is not an easy matter. Essentially, however, NN refers to 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 2018 to 30 April 2019, inclusive) 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, at the same time potentially 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. Our strategy of dedicating one section to an aspect of net neutrality (zero-rating in this issue) is intended to help the interested reader gain a deeper understanding of the subject.

The present report stems from an obligation imposed on the European national regulatory authorities (NRAs) by the Telecoms Single Market Regulation (TSM Regulation)[1]. 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.

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. 182–183). Nonetheless, in the interests 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 with the structure proposed by the guidelines by consulting the dedicated mapping presented in Appendix 1.

As in the previous reporting year, monitoring activities and addressing potential net neutrality infringements dominated the current year under review. Keys points of focus in the reporting period included the blocking of websites as a result of copyright claims and more detailed investigations into zero-rating.

[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/en/tk/nn_berec_guidelines

As a convergent regulatory authority for media, telecoms and postal services, it is essential that RTR develop and coordinate all positions on net neutrality as an interdisciplinary activity, conferring in particular with the Austrian Communications Authority (KommAustria).

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. Setting appropriate transition periods, for example, reflects these considerations. Experience has shown that in most cases, a constructive, solutionoriented approach is adequate for ensuring compliance with the substance or spirit of the TSM Regulation.

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 EU – 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, which comprises 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 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. Section 7 is dedicated to the topic of zero-rating, namely those services that are offered or used without counting the data volume included in the respective tariff plan. The last part of the report, section 8, offers a brief summary of the projects and challenges expected in the next reporting year.

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.

As in the past, internet service providers (ISPs) continue to be the group mainly targeted by net neutrality provisions; ISPs are companies that provide services for accessing the internet. 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) that are required or prohibited in order to uphold net neutrality. Alongside ISPs, the group of stakeholders and others targeted by legal provisions includes in particular end users (private citizens and businesses) and providers of content, services or applications (content and application providers, hereinafter 'CAPs'). The TSM Regulation makes no distinction per se between end users and CAPs.

Other aspects are also important, however. First, discussions about net neutrality have always needed to consider the question of how its concepts can be implemented in the fifth generation of mobile telecommunications standards (5G). One important issue here relates to the new business models that ISPs could use as differentiators in order to remain competitive in the market. For the time being, we would continue to point to the conclusions drawn in the last report – that the TSM Regulation clearly allows enough room for innovation and scope for products, without ISPs running the risk of reaching net neutrality provisions. After successfully navigating the TSM Regulation's 'roll-out phase', where the focus tended to be on 'testing the limits' of these new provisions, a dialogue has now been established that offers stakeholders a forum for discussing the future challenges to net neutrality in the context of 5G.

Common practice is the second aspect that continues to play a key role. To be effective, a framework of rules relating to 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 individual countries or regulatory authorities could ultimately disadvantage some ISPs in relation to others in other Member States. One aspect to be considered here is the challenge posed by each Member State transposing the TSM Regulation into its own system of (administrative) law, which results in differences in how procedures are organised. It has and continues to be in particular the close coordination practised by regulatory authorities under the mantle of BEREC that has ensured the largely harmonised enforcement of the TSM Regulation. In addition, work has also been proceeding for some time on a revision of the BEREC net neutrality guidelines, which is scheduled for completion in early 2020.

In Austria, the Telekom-Control-Kommission (TKK) and Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) are responsible for enforcing the TSM Regulation. This is now explicitly included as part of the December 2018 amendment to the Telecommunications Act. Supervisory procedures under Art. 5(1) of the TSM Regulation continue to be part of the TKK's remit, while the upstream request-for-information procedures pursuant to Art. 5(2) of the TSM Regulation are completed by RTR. Another aspect, relating among other things 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, as set out in Art. 25 of the TKG 2003. The TKK can issue an objection within eight weeks in the event of failure to comply with the TKG 2003 or ordinances issued on the basis of the TKG 2003, or with 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 of business (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 only be prohibited ex post. Moreover, the regulatory authority can also impose reporting requirements on a company: these can help to better assess market impact.

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 net neutrality topics (such as zero-rating or specialised services) may exhibit an overlap with media topics (such as the procedure addressed in section 5.5). Another point of contact in relation to the EU GDPR and the ePrivacy Directive is the data protection authority: collaboration here is likely to intensify as a result of the preparation and enforcement of a new ePrivacy Regulation.

04 Regulatory authority activities

Timeline of regulatory authority activities

4.1 Timelines

FIGURE 01: TIMELINE OF EVENTS IN THE REPORTING PERIOD

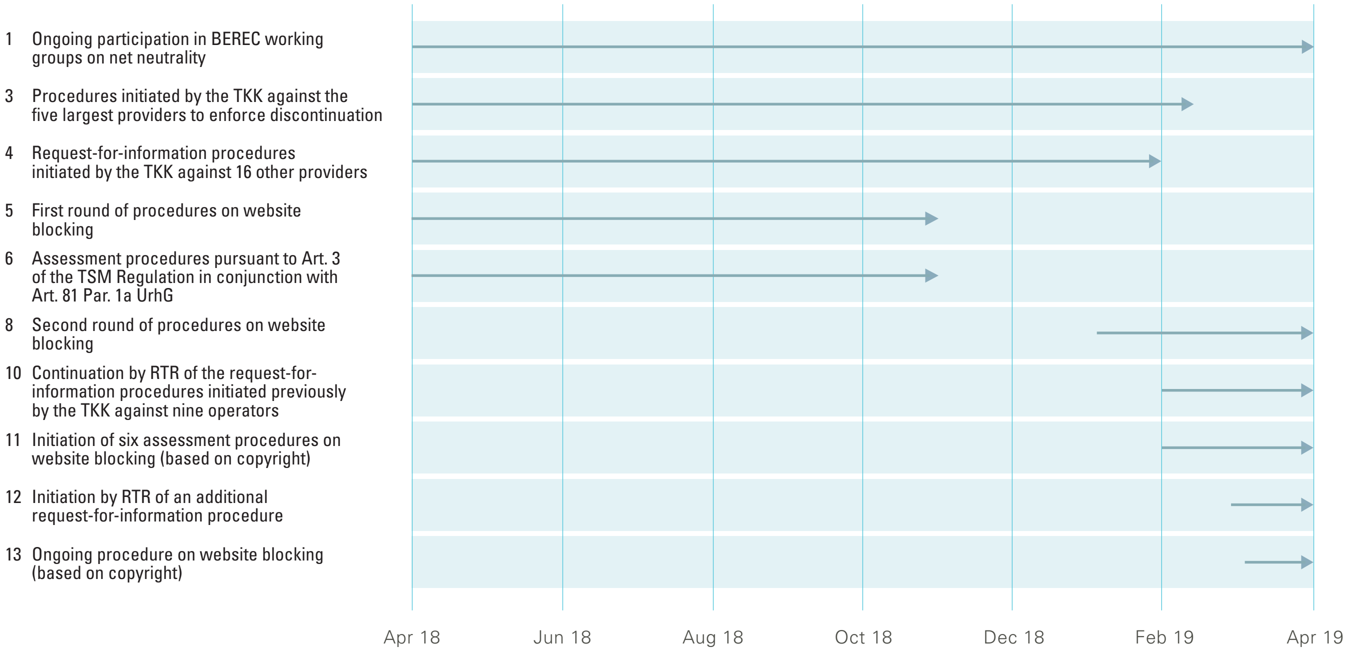


Figure 1 shows the chronological sequence of relevant events in the reporting period (May 2018–April 2019). The table below gives an overview of these events, with a brief description as well as some historical context. Further details about these procedures can be found in section 5.

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 2018: Development of a Net Neutrality measurement tool, Implementation of the Net Neutrality Regulation, Net Neutrality – input to an evaluation BEREC working groups 2019: Update to the Guidelines on Net Neutrality, Report on the implementation of Regulation (EU) 2015/2120 and BEREC Net Neutrality Guidelines, Carry-over work on BEREC Net Neutrality measurement tool
		NATIONAL STATUS QUO ANALYSIS/DISCUSSION WITH PROVIDERS
2		No transparency study was completed in the current reporting period.
		ENFORCEMENT OF TSM REGULATION
3	Oct 2016 – Mar 2019	Procedures by the TKK to enforce discontinuation, initiated against the five largest providers by the TKK in October 2016. The last ongoing procedure in this round was dropped in March 2019 (see section 5 for further details).
4	Jan 2018 – Feb 2019	Request-for-information procedures initiated by the TKK against 16 other operators; six procedures were dropped in the reporting period without initiating a supervisory procedure. Procedures against nine of these operators were transferred to RTR in Feb 2019 through the change in responsibility resulting from the amendment to the TKG 2003 (FLG I No. 78/2018) (see section 5 for further details).
5	Feb 2018/ Apr 2018 – Nov 2018	Seven procedures initiated by the TKK pursuant to Art. 3(3) of the TSM Regulation against eight operators (six following merger of T-Mobile and UPC). The procedure concerned the legitimacy of blocking access to certain websites as a result of injunction claims asserted by copyright holders (see section 5.5 for further details).
6	Apr 2018 – Nov 2018	Introduction and informal dropping of an assessment procedure (as a result of all parties to the procedure withdrawing their submissions) pursuant to Art. 3 of the TSM Regulation and Art. 81 Par. 1a UrhG (see section 5 for further details)
7	Nov 2018	The TKK issues decisions versus A1 Telekom Austria AG, LIWEST Kabelmedien GmbH, kabelplus GmbH, Salzburg AG für Energie, Verkehr und Telekommunikation, T-Mobile Austria GmbH, two UPC companies and Hutchison Drei Austria GmbH in relation to the legitimacy of blocking accessing to certain websites as a result of injunction claims asserted by copyright holders (see section 5.5 for further details).
8	Jan 2019 – Apr 2019	Six procedures initiated by the TKK pursuant to Art. 3/Art. 5 of the TSM Regulation against eight operators. The procedures concerned the legitimacy of blocking access to certain websites as a result of injunction claims asserted by copyright holders (see under 5.5 for further details).
9	Apr 2019	The TKK issues decisions versus A1 Telekom Austria AG, LIWEST Kabelmedien GmbH, kabelplus GmbH, Salzburg AG für Energie, Verkehr und Telekommunikation, T-Mobile Austria GmbH, two UPC companies and Hutchison Drei Austria GmbH in relation to the legitimacy of blocking accessing to certain websites as a result of injunction claims asserted by copyright holders (see section 5.5 for further details).
10	Since Feb 2019	Continuation by RTR of the request-for-information procedures initiated previously by the TKK (point 4 above) against nine operators (see section 5 for further details).
11	Since Feb 2019	Introduction of six assessment procedures pursuant to Art. 3 of the TSM Regulation and Art. 81 Par. 1a UrhG (see section 5.5 for further details).
12	Mar 2019	Initiation by RTR of an additional request-for-information procedure pursuant to Art. 5 Par. 2 of the TSM Regulation (see section 5 for further details).
13	Since Apr 2019	One ongoing procedure pursuant to Art. 3/Art. 5 of the TSM Regulation. The procedure concerns the legitimacy of blocking access to certain websites as a result of injunction claims asserted by copyright holders (see section 5.5 for further details).

05 Potential violations of net neutrality

and associated procedures

After the entry into force of the TSM Regulation on 30 April 2016 and ensuring that 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 previously recognised violations of net neutrality. As of 30 April 2019, a procedure from the first round of procedures in October 2016 is still pending before the Federal Administrative Court (BVwG), after being heard before the court of first instance in December 2017. This procedure, which had spent 18 months before the BVwG at the time this report was filed, is regrettable considering the legal certainty soon to be available for both end users and ISPs in what is still a new area of law.

Another procedure, initiated in October 2016, conducted by the TKK pursuant to Art. 5(1) of the TSM Regulation was ultimately dropped in December 2018 following the completion of pending technical conversion work by the operator concerned. Delays in this case had been caused in particular by the fact that the operator concerned had made the necessary changes as part of work involved in the takeover of another ISP and integration of the two networks.

As already stated in the 2018 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) of the 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 network address translation (NAT). This prevents these customers from using or providing their own services; this right follows, however, from Art. 3(1) of the TSM Regulation. A more detailed description is given in section 5.2.
3.	Zero-rating	The data volume used by a specific application or for a specific CAP does not count towards the data volume cap included in the customer's subscription.
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. A more detailed description is given in section 5.3.
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). A more detailed description is given in section 5.4.
7.	Blocking websites due to copyright claims	Even though jurisdiction for ruling on injunctions based on copyright claims 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 the third subparagraph of Art. 3(3) of the TSM Regulation (see section 5.5).

One key focus of activities in this reporting year was on procedures to determine potential violations of net neutrality by smaller (in terms of customer base) operators. To establish a level playing field, it was necessary to gradually start auditing smaller fixed network and mobile operators, after completing audits of the biggest national operators.

Already in early 2018, as part of continued monitoring of compliance with Art. 3 of the TSM Regulation and in a second round of request-for-information procedures, a total of 16 ISPs were sent requests as well as questionnaires about products and technical practices. By the end of the reporting period, the operators had appropriately responded in almost all of these procedures. One positive outcome is that six of these procedures had already been dropped between July and December 2018, as it had not been possible to identify any potential violations of net neutrality. In the remaining ten procedures (it should be noted here that four procedures involved a virtual network operator that had formed separate companies for its brands), RTR continued the previous practice of holding exploratory talks on behalf of the TKK in order to identify potential violations of the TSM Regulation. At the end of 2018, one operator announced discontinuation of business as of March 2019 because of the introduction of mandatory registration for prepaid card contracts, and this did in fact occur. To save costs, procedures relating to potential violations were dropped pending cessation of business activities.

At the beginning of 2018, the amendment to the TKG 2003 (FLG I No. 78/2018) duly entered into force, and with it the transfer of responsibilities for request-for-information procedures from the TKK to RTR. This resulted in the transfer of nine remaining procedures to RTR.

In these remaining procedures, the focus of TSM Regulation violations was primarily on the non-assignment of public IP addresses, port blocking and the forced disconnection of IP connections. Until the end of the reporting period in April 2019, seven ISPs were served with notices of deficiencies, requesting that they act to resolve the corresponding violations voluntarily before the imposition of supervisory measures. The informative and foundational work performed by the regulatory authority in 2016 and 2017 has also proven to be worthwhile, since all seven operators have already implemented or introduced technical measures to resolve the deficiencies identified. The two remaining procedures continue to be pursued and will be the subject of the next report.

In an unrelated case, several users submitted complaints to the regulatory authority about potential violations of the TSM Regulation by a small-scale operator. This resulted in the launch of another request-for-information procedure in February 2019, the operator being requested to issue a statement. At the end of the reporting period, it was not clear whether this procedure would lead to supervisory measures.

A key point of focus in the current reporting year was the approach to the handling of blocks placed on domains or IPs as a result of claims by copyright holders that the sites being operated under these domains/IPs were structurally in breach of copyright law. Much of the casework on net neutrality focused on these kinds of scenarios in the reporting year. In detail, the case concerns verification of compliance with or the applicability of point (a) under the third subparagraph of Art. 3(3) of the TSM Regulation, in relation to the blocking of content (websites) in response to copyright claims. Even though courts of law are authorised to issue 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) under the third subparagraph of Art. 3(3) of 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 section 5.5.

Alongside activities previously described as part of the stated procedures concerning existing products, there were continued reviews in accordance with national requirements to review contract terms (Art. 25 Par. 6 TKG 2003), so that general terms of business and fee provisions were verified for compliance with the TSM Regulation. In this context, it should be noted that a growing number of small-scale providers are including in their contract documents the minimum content pursuant to Art. 4(1) of the TSM Regulation. Attempts to enforce all providers to comply with this minimum content will be another important point of focus in the next reporting period. With respect to this minimum content requirement, no immediate steps in formal procedures, based on the TSM Regulation, needed to be taken in the reporting period: inclusion of this content is now mostly a routine matter.

5.1 Blocking of TCP/UDP ports or protocols

Request-for-information procedures conducted in 2018 revealed that some of the providers surveyed block various ports in the TCP and UDP protocols, typically citing as a reason the need to maintain network security and integrity (based on point (b) of Art. 3(3) third subparagraph).

This is problematic, since it restricts end-user rights pursuant to Art. 3(3) third subparagraph.

In terms of port blocking, varying sets of circumstances have arisen as a result of these new procedures. Once again, it became clear that port blocking does not follow any single, identifiable pattern. In most cases, the actual grounds for blocking specific ports were clarified in the course of procedures. Since the mobile operators who were involved in the procedures were all virtual network operators (MVNOs), most without their own core networks, these operators simply referred the matter to their host operators. Since these MNOs had already been audited in the first round of procedures, no further investigations were necessary. Results from the fixed network ISPs surveyed were again varied and port blocking strongly depended on factors necessitated by hardware. As an example, one ISP was using TCP port 22 (service: secure shell, SSH) for the maintenance of a part in its modem and had therefore placed an end-user block on the port. Some of these blocks were therefore of a ‘legacy’ nature.

At this juncture, it must once again 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 to conclude the legitimacy of port blocking as practised by other ISPs. To assess the appropriateness and necessity of blocking, the corresponding ENISA guidelines were also applied for the first time.

The following section provides a summary of selected findings.

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 operator states that the modem manufacturer offers no support in this matter. The operator has therefore agreed to remove this port block for all unaffected customers by August 2019 and to offer a replacement modem to affected customers on request.

TCP port 23 (Telnet)
One mobile operator confirms 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 PC 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 are considered to be legitimate – as they have been in previous procedures – since (pure) SMTP is a protocol frequently misused at retail level (for sending spam). One of the providers affected has since ceased network operations.

TCP/UDP port 53 incoming (DNS)

Three operators stated that this block was deployed to avoid the risks of DNA amplification attacks and DNS spoofing. Two operators stated that these blocks were limited to end users with dynamic IPs.

Final analyses are still pending for these cases.

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 port 80 and 8080 bidirectional (HTTP)

One MVNO blocked both these ports, which are necessary if end users wish to operate their own web servers. This action was justified by citing vulnerabilities in the hardware used by end users. The block was removed after replacing this hardware.

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 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 443 incoming (HTTPS)

One fixed network operator confirmed blocking incoming traffic on TCP port 443 for use by a wholesale partner. After further clarification, this block was removed. In terms of the fixed network internet connections provider by this operator directly, the operator stated that the block related to defective firmware in the modems used. These modems were replaced in the course of 2019 and the block was then also removed for these users.

TCP port 445 incoming (SMB)

One MVNO and a fixed network operator block(ed) incoming traffic on this port. The MVNO ceased operations in March 2019, however.

In the case of the remaining 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 stated that this TCP port was blocked for maintenance reasons. The block has since been removed.

TCP port 8089 incoming (TR-069)
This TCP port is not within the range of 'well-known' ports defined by IANA. This block was seen as justified because a certain brand of modem reserves this port for the TR-069 remote maintenance protocol and is therefore susceptible to corresponding manipulation.

An analysis was ongoing at the end of the reporting period.

5.2 Private IP addresses and services

Art. 3(1) grants end users also 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 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 that user's internet connection.

In mobile networks in particular, customers are occasionally assigned private IP addresses (via NAT). Apart from technical aspects, the main reason is the provider's wish to save on public IPv4 addresses, which are becoming scarce.[3] 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 such an address, for example because of wishing to offer services. The end user can then utilise that address with dynamic DNS services to allow routing to their own services. Assigning a public IP address on condition of payment of an additional fee (defined for instance in a specific subscription model or as an added option) or only to certain customer segments (such as business customers) is in any case to be considered a breach of Art. 3(1).

The last reporting period had shown that this problem is especially common with mobile network operators. In all but one case, which led to a request-for-information procedure involving a fixed network operator in February 2019, this circumstance exclusively affected MNOs/MVNOs in the current reporting period as well. On request, the above-mentioned fixed network operator then stated that end-users were currently being assigned only private addresses for IPv4 (carrier-grade NAT) – but public addresses in the case of IPv6. While the (additional) allocation of IPv6 addresses is to be welcomed, IPv6 penetration across the entire internet is currently only about 25%. If customers of this operator provide their own services, they would consequently be inaccessible for the entire IPv4 network, or accessible only via third parties. This procedure was still pending at the end of the reporting period.

In terms of the availability of public IP addresses at MVNOs, it is important that operators of the respective host networks are reminded of their obligations to allocate public IPv4 blocks to MVNOs since the latter repeatedly report problems here. While one MVNO planned no further measures, because of intending to cease operations at the end of the reporting period, six MVNOs took action that would enable them to allocate public IPv4

[3] While fewer than 232 (approx. 4 billion) addresses are available using IPv4 and are now becoming scarce, IPv6 allows a little under 264 (approx. 18 trillion) subnets.

addresses on demand in the future. One MVNO was acquired by an MNO in the period under review and its customers are being transferred to the MNO’s network. Once the switch has been completed, public IP addresses will also be available to those users. In three of the request-for-information procedures initiated, corresponding commitments were still outstanding as of the end of April 2019.

This problem area will also continue to occupy RTR’s attention in the future.

5.3 Technical discrimination and restriction / change of IAS

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

One request-for-information procedure conducted in 2018 revealed technical discrimination practices with one mobile network operator. The operator provided to users free of charge a proprietary application with access to a database of films and music as well as a sports station and radio station. No fee was charged for the volume of data consumed by using the application (zero-rating), with this initially viewed as being compatible with Art. 3(2) of the TSM Regulation. However, a breach of Art. 3(3) of the TSM Regulation was identified based on the fact that the aforementioned application continued to function entirely without restriction even after the data included in the subscription was used up – in contrast to other services and applications.

It proved possible to drop the respective procedure without a decision being issued: the operator modified its application to conform to the TSM Regulation.

5.4 Disconnection of IP connections

The right of end users to self-host services is also restricted when the internet connection (IP connection) is automatically disconnected, typically after a short period of time.

It was typical 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 by the providers here ranged from technical considerations regarding the assignment of IP addresses to the claim that this measure helped protect 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).

This practice also played a role in the current reporting period, although it occasionally gave rise to misunderstandings among MVNOs surveyed in the period under review. In the context of Art. 3(1), rights are considered restricted only when the IP connection is actually interrupted but not when the session is terminated for billing purposes. The latter typically does not lead to an interruption of the end user’s connection, nor does the IP address allocated to the user change.

After talks with affected operators (except for the MVNO that ceased operations in March 2019 and the other MVNO acquired by an MNO), it was discovered that these cases do not in fact involve an arbitrary disconnection of IP connections but merely the completion of 'session tickets' for the purposes of account settlement.

5.5 Blocking websites due to copyright claims

5.5.1 Website blocking in the reporting period

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 duly warned by a rights holder. A website in 'structural breach' of the law is a website that does not infringe exclusive rights as defined in the UrhG in an isolated case but instead breaches these rights regularly and deliberately. 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.[4]

Before awarding to a rights holder an injunction against the provider of internet access services, various basic rights first need to be considered.[5] In assessing claims according to Art. 81 Par. 1a UrhG, the entitlement to protection of intellectual property claimed by the copyright holder requesting the injunction, as well as that party's right to effective enforcement of the law, must be weighed against the basic rights to freedom of expression, freedom of information and freedom to conduct a business, to which internet users, website operators and the access provider involved in the procedure are entitled.[6] Since consideration of those basic rights is intrinsic to the assessment of claims based on Art. 81 Par. 1a UrhG, this provision is therefore an exception as referred to in Art. 3(3) third subparagraph point (a) of the TSM Regulation[7]. If a provider of internet access services adopts a proportionate traffic management strategy that accords with these claims, this does not violate the terms of the TSM Regulation.

In the period between early 2018 and April 2019, the TKK initiated a total of 14 supervisory procedures against internet access service providers who were suspected of having denied access to particular websites, and completed 13 procedures in this period. In the procedures, the providers claimed to have denied access to some of these websites in response to a court decision – such as a provisional injunction or a court ruling. They also referred to blocks that had been placed as a result of court settlements or solely on the basis of a warning issued by the rights holders.

[4] OGH 24 October 2017, 4 Ob 121/17y; TKK 26 November 2018, R 1–5, 8, 9/18; TKK 12 April 2019, R 1–6/19.
[5] ECJ 27 March 2014, C-314/12, UPC Telekabel Wien/Constantin Film Verleih et al.
[6] OGH 14 October 2017, 4 Ob 121/17y.
[7] TKK 26 November 2018, R 1–5, 8, 9/18; TKK 12 April 2019, R 1–6/19.

Even though jurisdiction for ruling on injunctions based on copyright claims normally lies with the ordinary courts, 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 but without a corresponding court ruling, the exception pursuant to Art. 3(3) third subparagraph (a) TSM Regulation must also be verified. In 13 of the supervisory procedures named, the procedure was concluded with a decision that provided a detailed assessment of the topic while considering the rulings of the Austrian Supreme Court (OGH) and the ECJ available when the particular decision was taken.

In summary, it can be said that blocks as a result of a legally enforceable court judgement concerning a claim pursuant to Art. 81 Par. 1a UrhG are binding on the national regulatory authority within the legal limits of the court's decision and that the decision in the supervisory procedure must be based on this court decision. If no decision binding on the TKK has been issued by the competent court against the affected provider of internet access services, then the actual existence of this claim under copyright law must be adjudged as preliminary in the context of the procedure pursuant to Art. 5 of the TSM Regulation.

In the 13 procedures completed, [8] 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 holder pursuant to Art. 81 Par. 1a UrhG. Additionally, the traffic management measures adopted, typically by setting up DNS blocks, were appropriate to the situation and observed the principle of proportionality. Only one provider of internet access services set an IP block for the kino.to and kinox.to websites, in addition to the DNS block. This was necessary as a result of a high court ruling[9] and was, by way of exception, in line with the principle of proportionality.[10] The technical implementation of network blocks is discussed in section 5.5.2.

As requested by a number of internet access service providers, the TKK initiated seven assessment procedures in the period from early 2018 to April 2019. Unlike the supervisory procedures pursuant to Art. 5 of the TSM Regulation as described above, the supervisory procedure here deals with websites that have not yet been blocked. While one procedure was terminated after all parties to the procedure withdraw their submissions in full, the remaining six assessment procedures are still at the fact-finding stage (see also section 4).

The assessment procedures are to determine whether an exception exists within the meaning of Art. 3(3) third subparagraph (a) of the TSM Regulation as well as whether it would be legitimate to subsequently block the website.

[8] TKK 26 November 2018, R 1–5, 8, 9/18; TKK 12 April 2019, R 1–6/19.

[9] OGH 24 January 2018, 3 Ob 1/18w.

[10] TKK 26 November 2018, R 5/19, citing OGH 24 January 2018, 3 Ob 1/18w.

5.5.2 Note: Technical options for implementing traffic management measures to block websites structurally in breach of copyright law

In the procedures addressing network blocks during the reporting period, the question also arose as to how to implement traffic management in detail and how the various implementation options might impact compliance with the TSM Regulation.

Various options for implementing a block are available to an ISP required to block a specific website. These differ in terms of technical implementation, options for bypassing the block, potential ‘overblocking’ effects and possible invasions of end users’ privacy.

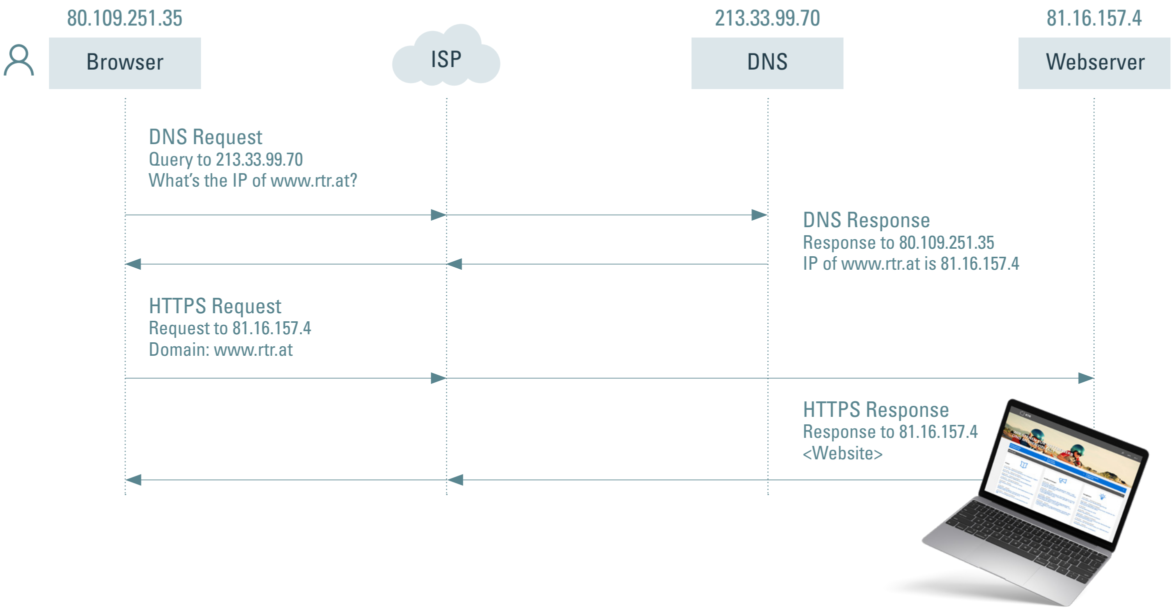
Accordingly, the following section discusses the blocking options using a DNS block or IP block. Not discussed here are types of blocks that would require an analysis of content data and therefore deep packet inspection (DPI) nor those that appear disproportionate (also from the perspective of data protection), such as DNS sniffing or the reading of TLS/SNI data or HTTP host names.

5.5.2.1 Technical principles

From a technical perspective, end users such as consumers and application providers are identified on the internet based on their IP addresses. Examples of IP addresses include 81.16.157.4 or 2a01:190:15fd:1c00::4, depending on the specific protocol used. Since such addresses are neither easy to handle nor simple to remember in day-to-day use, access is instead provided via domains, such as www.rtr.at. To translate the easily remembered name of the domain into the IP address that is actually technically necessary for communication, a domain name service (DNS) is then used. In simple terms, DNS is like an internet ‘telephone directory’ in which the matching IP address can be looked up for each domain. Structurally, the DNS is designed and implemented as a distributed system.

DNS queries take place without users’ knowledge. Accordingly, every internet access service includes an ISP-operated DNS server that is set up for the end user by the internet access provider and is (indirectly) queried by the user’s web browser when accessing a domain. This is shown (in simplified form) in figure 2: When accessing the www.rtr.at website, the end user’s browser automatically queries the DNS server to obtain the associated IP address. Only once this is provided can the browser then establish a connection to its ultimate destination.

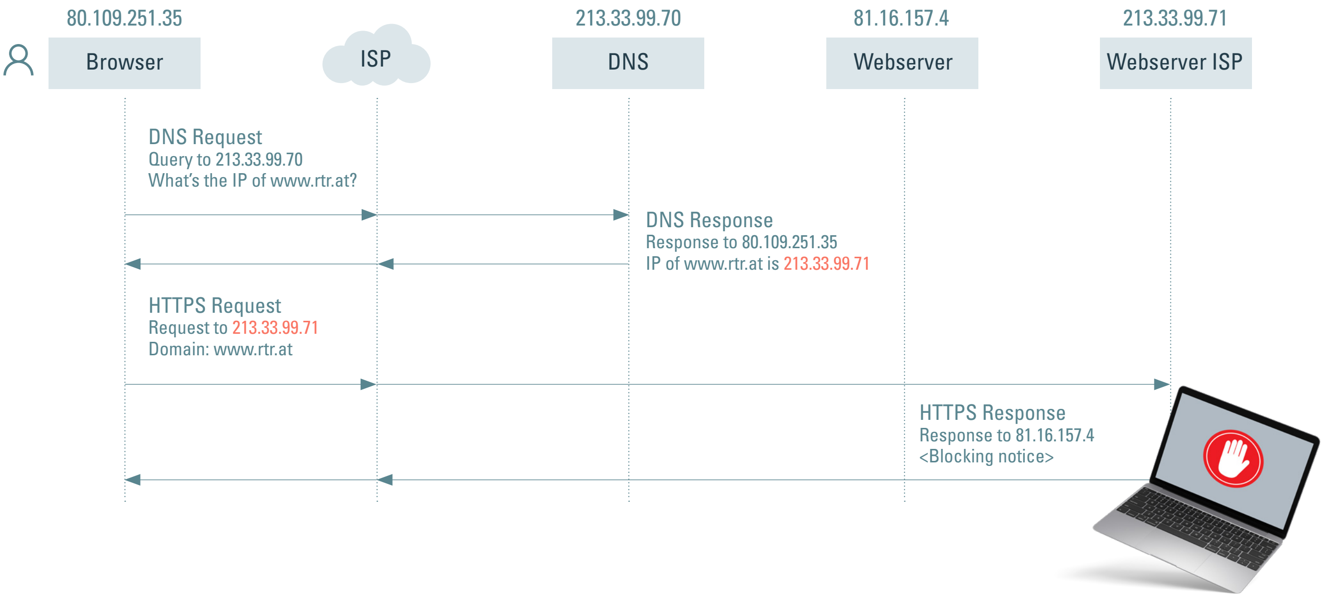
FIGURE 02: SCHEMATIC DIAGRAM OF WEBSITE ACCESS



5.5.2.1.1 DNS block

In the case of a DNS block, the ISP configures its DNS server to return for the domain to be blocked a different IP address than the original IP address. Queries to this domain are routed to an IP address under the ISP's control, which is typically a website explaining the reasons for blocking this particular content. This can be represented as a diagram as shown in figure 3: In the case of a DNS block, the DNS server responds to the query with an IP address that is assigned to the ISP and provides information about the block. The end user's browser is not provided with the IP address of the actual server.

FIGURE 03: SCHEMATIC DIAGRAM OF A DNS BLOCK



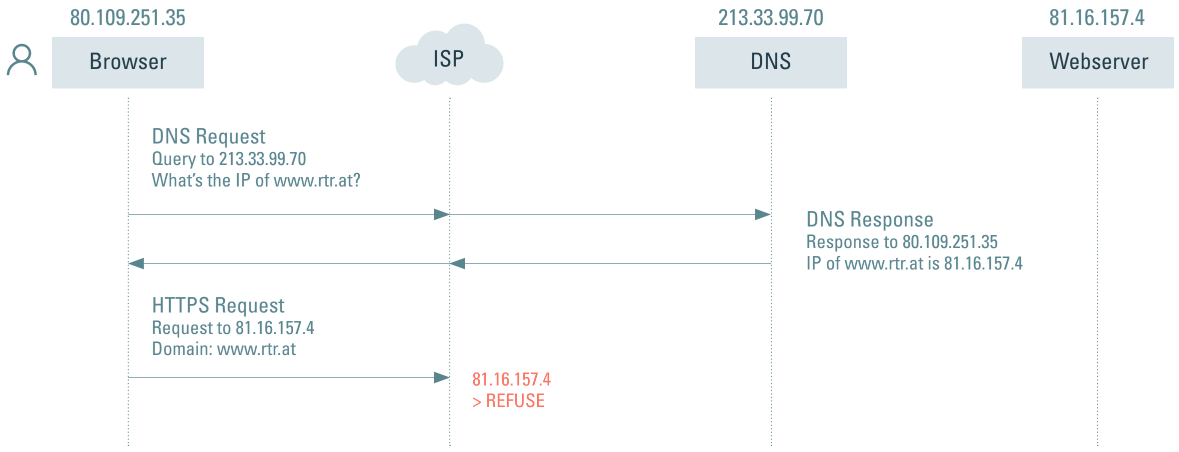
DNS blocks therefore offer a targeted way of preventing direct access to the affected domains. The end user is informed about the block while third-party domains are not affected technically by this kind of block. While a DNS block can in principle be bypassed, this does require the application of some basic technical knowledge. Examples of workarounds available to the end user include the use of a VPN service, the use of TOR[11] or changing the operating system's DNS server settings to point to an alternative DNS provider who is not under the control of the user's internet access provider.[12] On discovering the block, the website operator can move the site to an alternative/additional domain, thereby rendering the block useless.[13]

5.5.2.1.2 IP block

An IP block set up by the ISP prevents access to the blocked IP address by end users. This means that none of the traffic destined for the target IP is routed to the site, regardless of what triggered the traffic or the actual domain name accessed.

Since this kind of block does not use a technical redirection but directly blocks the IP address, end users cannot be informed about the block when attempting to access a domain that uses the blocked IP address. This can be represented as a diagram as shown in figure 4: While the DNS query is answered correctly in the event of an IP block, the ISP does not deliver any data packets to the blocked IP address regardless of the domain that is being queried.

FIGURE 04: SCHEMATIC DIAGRAM OF AN IP BLOCK



[11] The Onion Router, https://www.torproject.org/

[12] Popular providers of such DNS servers include Google (8.8.8.8), Quad9 (9.9.9.9) and CloudFlare (1.1.1.1).

[13] This was temporarily the case with the copyright-infringing website movie2k.to, which moved to movie4k.to after a block was set up. (https://t3n.de/news/movie2kto-neuer-name-movie4to-469942/)

While end users can bypass an IP block user, this again requires some basic technical skills and is possible by signing up to a VPN service or using TOR, for example. If the website operator discovers the domain is blocked, the operator can move the site to an alternative IP address, thereby rendering the original block useless. Since users typically use domains and not IP addresses to access websites, this change is invisible to the user and typically requires no further action – unlike the process of moving to a new domain, for example. Since hosting companies trade, re-use and change IP addresses frequently, continuous monitoring of the block's effectiveness is necessary.

5.5.2.1.3 The domain name and IP address relationship

While in the past an IP address identified exactly one server and therefore one website, this kind of 1:1 relationship is no longer so prevalent in modern internet architectures. Technically, it is entirely possible for a domain to be accessible under various IP addresses and for a single IP address to be used to host multiple separate domains. This is no longer a 1:1 relationship but an n:m relationship.

While a domain can be allocated to one or more IP addresses by a DNS server, the reverse is not true. Instead, there are only a indicators that suggest one IP address is being used for multiple domains. No technical proof of the fact of such multiple assignment or exclusive assignment exists, however.

Indicators potentially suggesting the exclusive use of a certain IP address:

- The website is accessed by an IP address instead of the domain name, e.g. http://81.16.157.4
- A reverse DNS query[14] of the IP address results in the domain name being searched for
- Searching public repositories for the IP address in question[15] reveals only the domain being searched for
- Existing documentation from the hosting or caching provider indicating exclusive or multiple uses of IP addresses

While the points above provide a few possible options, even if all of these return a positive result, it is still not technically possible to prove beyond a doubt that an IP address is used exclusively by a single domain.

[14] Reverse DNS query: querying the DNS server for the associated 'in-addr' .arpa address. In the case of 81.16.157.4, for example, this would be 4.157.16.81.in-addr.arpa

[15] Such as searching for 'ip:213.208.150.180' with Microsoft Bing

5.5.2.2 Blocking of legal content: ‘overblocking’

Since the TSM Regulation stipulates that ISPs “shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services” [16], internet blocks must always be analysed in sufficient detail.

There is a possibility of blocks overstepping the mark, preventing access to content although there is no legal basis. This kind of blocking is termed ‘overblocking’.

5.5.2.2.1 Overblocking of content on a domain to be blocked

Since a block imposed across a domain will block all of the content on that domain, an analysis must first be conducted to assess the ratio of legal to illegal content and whether an indiscriminate content block appears justified. To help conduct such analyses, the legal concept of a website that is in ‘structural breach’ of copyright law has been developed and a website block may only be imposed on sites of this kind.

This kind of structural breach was deemed to apply to kino.to, for example, although it would be unlikely in the case of sites like YouTube or Wikipedia since here the vast majority of content is legal.[17] The following section does not further discuss this form of overblocking.

5.5.2.2.2 Overblocking of content on third-party domains and websites

In principle, it would be possible for website blocks not only to affect the domain to be blocked itself but also other, unrelated third-party websites.

For DNS blocks, this would be the case if the need to block a domain resulted in the blocking of an entire top-level domain on the DNS server. One example would be the blocking of Tonga’s entire top-level domain ‘.to’ in order to set up a block that was needed for ‘movie4k.to’.

In reality, a more important type of overblocking that is also harder to assess is the blocking of IPv4 addresses. Particularly with shared web hosting, many separate domains share the same IP address. This also results from the scarcity of available IPv4 addresses, the costs involved in procuring an exclusive IPv4 address and the support provided by technologies that enable multiple use by all of the popular browsers.[18]

[16] Citation from Art. 3(3) third subparagraph of the TSM Regulation
[17] OGH 24 June 2014, 4 Ob 71/14s.
[18] Server Name Indication (SNI), RFC 6066.

5.5.2.2.3 A special case: handling content delivery networks

Many websites utilise content delivery networks (CDNs) to improve website performance and scaling. CDNs enable queries from end users to be distributed over many data centres located around the world. This not only results in shorter load times for users (from the simple fact that data cannot travel faster than light) but also enables loads to be balanced across a larger overall volume of computing power during peak usage times while supplying data simultaneously to a large number of users. CDNs can be deployed only for certain types of page elements (such as images or videos) or can be used to build the entire online presence. CDN products are available for any size of site, thereby enabling cost-effective use for any business from start-ups to enterprise users.

Over 50% of the top 10,000 websites make use of CDNs.[19] Major providers include Amazon, Akamai, Microsoft, CloudFlare and Fastly. In the case of the procedures in the period under review, some of the websites to be blocked used the CloudFlare CDN: this network is therefore examined in greater detail by way of example below.

CloudFlare is an international company that manages several million domains and operates 165 data centres according to its own figures.[20] The company is headquartered in San Francisco and has a branch office in Munich, Germany.[21] CloudFlare operates the AS13335[22] and maintains public peerings with many internet exchanges, such as a 400 Gbps peering with DE-CIX in Frankfurt[23] and a 50 Gbps peering with the Austrian Vienna Internet Exchange (VIX).[24]

Alongside several paid subscription plans, CloudFlare also has a line of free products. This makes it possible for website operators to offer their own services with global availability while also protecting themselves against DDoS attacks. Under such an arrangement, CloudFlare operates like a caching server: the content from website operators is queried synchronously by CloudFlare the first time it is requested and is then cached for a defined period of time so that the original server no longer needs to serve content for subsequent site queries. CloudFlare is currently a very popular service – over 35% of the top million websites listed on Alexa use CloudFlare as a CDN.[25]

Technically, CloudFlare uses the Anycast routing methodology.[26] This means that DNS requests for a domain will always resolve to the same target IP address regardless of the location of the querying party, but this address can be served by multiple data centres and queries can be routed to a data centre that is geographically closer.

CloudFlare openly admits that domains share the available IP addresses.[27] This is also a simple question of maths, since CloudFlare only has around 1.7 million IP addresses at its disposal.[28]

The indicators described above also strongly suggest that CloudFlare uses an identical IP address to serve a range of websites: a website cannot be accessed directly via the IP

[19] https://trends.builtwith.com/CDN/Content-Delivery-Network; major CAPs such as Google or Netflix operate their own, proprietary CDNs.
[20] https://www.cloudflare.com/network/
[21] https://www.cloudflare.com/about-overview/
[22] https://whois.arin.net/rest/asn/AS13335
[23] https://www.peeringdb.com/ix/31
[24] https://www.peeringdb.com/net/4224
[25] https://www.datanyze.com/market-share/cdn/Alexa %20top %201M/cloudflare-cdn-market-share
[26] https://www.cloudflare.com/learning/cdn/glossary/anycast-network/
[27] https://support.cloudflare.com/hc/en-us/articles/205177068
[28] https://www.cloudflare.com/ips/

address,[29] reverse DNS queries produce no results and searches in public repositories for CloudFlare IPs reveal a multitude of unrelated websites.[30] In the procedures mentioned above, CloudFlare was also observed to change IP addresses for individual websites regularly, which is further evidence against the allocation of one static IP address to each website.

5.5.2.3 Technical issues to consider

In practice, website blocks in Austria make use of both DNS blocks and IP blocks, although most of the blocks are of the DNS type.[31]

If a block must be imposed for a specific domain but no specific technical method is stipulated, RTR believes that a nuanced approach must then be taken. This is especially the case if the site to be blocked uses a CDN.[32]

While the effectiveness of both the block and the potential for overblocking by DNS blocks is not technically affected by CDN use, this is not the case for IP blocks, for the reasons outlined above: not only is technical proof of the use of an exclusive IP address hard to come by, but it is also current practice particularly within the CDN industry to use one IP address to serve multiple domains. Nor was any evidence to the contrary obtained about the domains actually investigated in the procedures conducted in the reporting period. In fact, the sharing of one IP address between multiple domains investigated during the procedures meant that a 1:1 allocation of IP address to domain could actually be ruled out.[33]

Although setting an IP block might seem more effective at first – because it cannot be bypassed by using a different DNS server, for example – not only the website operator but also users with sufficient basic technical expertise can work around the block, while the risk of overblocking increases substantially. This must be considered when assessing whether a block is proportionate, thereby evaluating compliance with traffic management pursuant to Art. 3(3) third subparagraph of the TSM Regulation.

[29] See for example http://104.27.180.161

[30] Such as a Bing search for 'ip:104.27.180.161'.

[31] TKK 12 April 2019, R 1–5/19.

[32] See 5.5.2.2.3.

[33] TKK 12 April 2019, R 1–5/19.

5.6 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 and the status and duration of procedures. More detailed descriptions of the cases can be found under the individual subsections of section 5. It should be noted that facts are collected separately for 'Number of cases', which may have been used collectively in what equates to a smaller number of cases.

TABLE 03: OVERVIEW OF CATEGORIES OF SUSPECTED NN BREACHES

KEY: 👍 Voluntarily discontinued 📁 Procedure pending ⚖ Pending before a court
⚑ Procedure terminated 📝 Discontinued by official decision

CATEGORY [34]	NUMBER OF CASES IN THE REPORTING PERIOD	PROCEDURE STATUS *	PERIOD
Port blocking	13	📁 2 ⚑ 3	Q 2/18 – Q 2/19
Private IP addresses	10	⚑ 3 📁 7 ⚖ 1	Prior to Q 3/17
Zero-rating	0		
Specialised services	0	⚖ 1	Q 2/18 – Q 2/19
Technical discrimination and restriction of internet access	1	👍 1 ⚖ 1	Q 2/18 – Q 2/19
Traffic redirection (proxy)	1	👍 1	Q 4/18
No server operation possible	1	👍 1	Q 2/18 – Q 2/19
Disconnection of IP connections	8	👍 4 ⚑ 1 📁 3 ⚖ 1	Q 2/18 – Q 2/19
Blocking websites due to copyright claims	14 **	⚑ 13 📁 1	Q 2/18 – Q 2/19

* The status of procedures pending or dropped/concluded with a decision in the reporting period, including procedures from previous periods awaiting a court decision.
** Fourteen procedures were initiated, although the number of affected websites is higher.

[34] 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 products available on the market are monitored continuously by the regulatory authority.

5.7 Measures in accordance with Art. 5(1)

In the third reporting period (ending in April 2019), no measures as defined in Art. 5(1) TSM Regulation were considered necessary to ensure compliance with the provisions of that article. This was because dialogue was initiated with the companies early on and discussions usually resulted in constructive solutions compliant with the TSM Regulation. Numerous procedures pursuant to Art. 5(1) were initiated but then dropped without a decision and order (e.g. because of the voluntary resolution of the issue by the operator); such cases are not listed here. The regulatory authority nonetheless, as a matter of course, monitored compliance with the provisions of Art. 3 and Art. 4 TSM Regulation on an ongoing basis.

The decisions on measures issued against A1 Telekom Austria AG in December 2017 pursuant to Art. 5(1) of the TSM Regulation remain valid. A less positive outcome, however, is the length of the procedure before the Federal Administrative Court, since these two decisions were the first issued on the basis of the TSM Regulation, while a rapid legal assessment would have been desirable so as to offer concrete guidance for future procedures.

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

KEY: 🔨 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's request • Increase in period for disconnecting IP connections from 24 hours to 30 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 1-5, 8, 9/18
R 1-6/19
	LIWEST Kabelmedien GmbH;
	kabelplus GnbH;
	Salzburg AG für Energie, Verkehr und Telekommunikation;
	T-Mobile Austria GmbH;
	UPC Telekabel Wien GmbH;
	UPC Telekabel-Fernsehnetz Region Baden Betriebsgesellschaft m.b.H.;
	Hutchison Drei Austria GmbH;
	A1 Telekom Austria AG
		The procedure was initiated to assess the legitimacy of blocking access to certain websites as a result of copyright claims.
		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 holder pursuant to Art. 81 Par. 1a UrhG.
		In addition, the traffic management measures actually adopted, typically by setting up DNS blocks, were appropriate to the situation and observed the principle of proportionality.
		Only one provider of internet access services set an IP block for the kino.to and kinox.to websites, in addition to the DNS block. This was necessary as a result of a high court ruling[35] and was, by way of exception, in line with the principle of proportionality.
		A decision was therefore issued to drop the procedure pursuant to Art. 5(1) of the TSM Regulation, in the absence of a violation of Art. 3 of the Regulation.
			R 1 – 5, 8, 9/18: 26 Nov 2018
			R 1 – 6/19: 12 April 2018
				✓

[35] OGH 24 January 2018, 3 Ob 1/18w.

06 Other indicators and activities

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, a total of 1,676 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 meet the minimum content requirements specified in Art. 4 of the TSM Regulation (such as minimum speed, maximum speed, normally available speed and advertised speed), since these items 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 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 94 requests in the reporting period (last reporting period: 112).

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

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 continuous availability of non-discriminatory internet access services

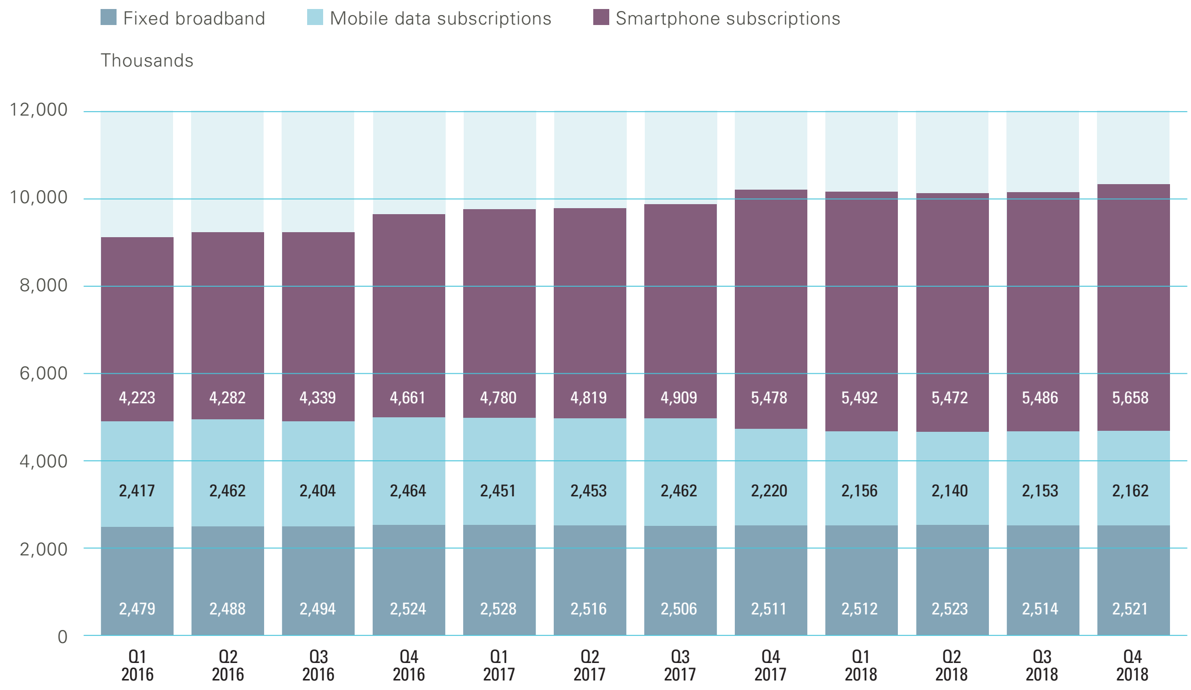
Art. 5(1) of the TSM Regulation requires national regulatory authorities to ensure compliance with Art. 3 and Art. 4 TSM Regulation and to promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology.

To provide a degree of perspective and a more accurate estimate of progress, the following charts also show the long-term trend. The charts are interpreted only for the reporting period, however. In the explanations that follow, reference is therefore made to the most recent set of available figures: nonetheless, figures for some indicators were not yet available for Q1 2019 when the report was compiled.

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
- Price baskets fixed vs. mobile broadband
- Quality dimensions

FIGURE 05: FIXED AND MOBILE BROADBAND CONNECTIONS [36]



Source: RTR

Figure 5 shows a continuous increase in the number of broadband connections since 2016. The number of smartphone subscriptions in particular has risen. For the reporting period, this means that the number of smartphone subscriptions rose from 5.47 million to 5.66 million between Q2 2018 and Q4 2018. The number of mobile data subscriptions fell from 2.14 million in Q2 2018 to 2.16 million in Q4 2018. The number of fixed broadband subscriptions remained almost unchanged (approx. 2. 52 million).

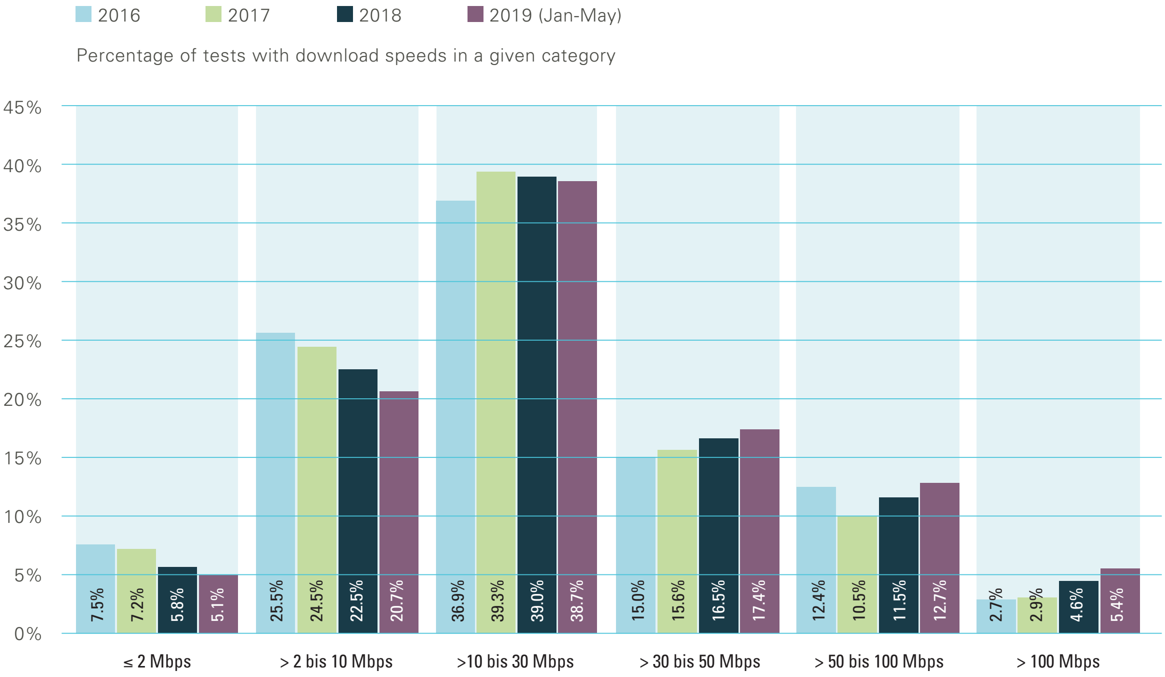
Data (Open Data)[37] generated with the help of the RTR-NetTest[38] is used to assess the quality of internet access. The RTR-NetTest allows users to check the speed and quality of their internet connection, reliably and independently of their provider. From Q2 2018 up to and including the first quarter of 2019, the RTR-NetTest was used for unrepeated measurements over 855,000 times in Austria (with a location accuracy of less than 2 km). More than 219,000 of the tests were mobile service measurements. Year-on-year, an increase was seen both in overall measurements and the number of mobile service measurements.

[36] Data on broadband connections is collected quarterly in accordance with the Communications Survey Ordinance (KEV) but was not yet available for Q1 2019 when this report was prepared. 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 including both data as well as minutes and text messages are considered smartphone subscriptions, regardless of whether post-paid or pre-paid. For details, see the most recent RTR Internet Monitor (in German): https://www.rtr.at/de/inf/InternetMonitor_2018

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

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

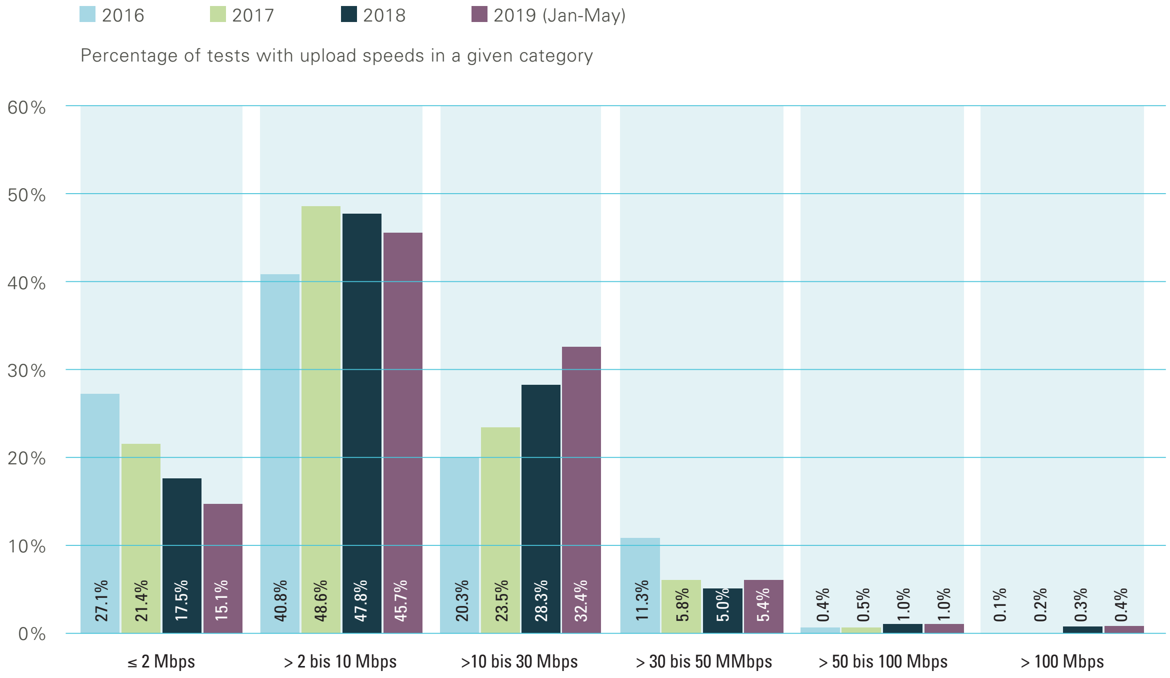
FIGURE 06: DISTRIBUTION OF DOWNLOAD SPEEDS OVER REPORTING PERIOD



Source: RTR-NetTest

Figure 6 reveals the percentages of tests with download speeds in a given category. It can be seen that as early as 2016 most of the measurements display download speeds of 10 to 30 Mbps. While this proportion grew in 2017, it shrank slightly in 2018. The percentage of measurements under 2 Mbps dropped between 2016 and 2019, while the proportion of measurements in excess of 100 Mbps rose over the same period.

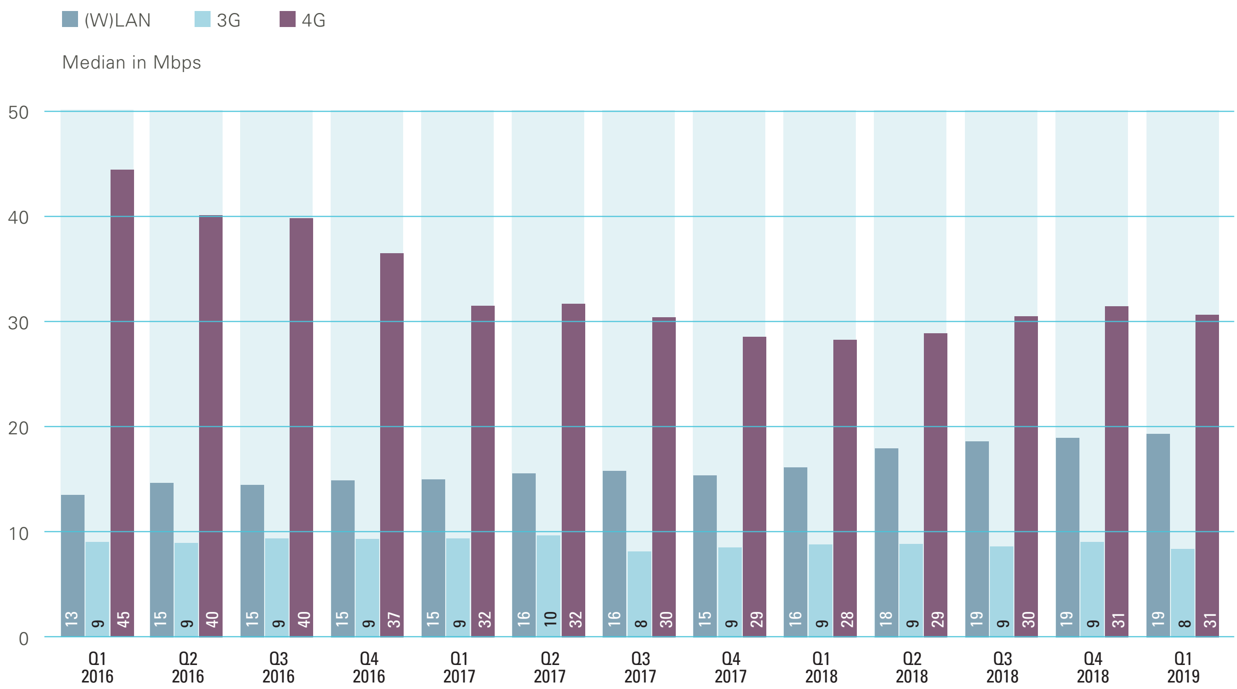
FIGURE 07: DISTRIBUTION OF UPLOAD SPEEDS OVER REPORTING PERIOD



Source: RTR-NetTest

Figure 7 depicts the ratios of tests with upload speeds in a given category. Back in 2016, most of the tests showed an upload speed of 2 to 10 Mbps, while the share grew strongly in 2017 only to shrink again slightly in 2018. The percentage of tests with an upload speed of less than 2 Mbps can also be seen to have fallen sharply. Interestingly, the share of tests with an upload speed of between 30 and 50 Mbps has dropped since 2016.

FIGURE 08: DOWNLOAD SPEED BY TECHNOLOGY

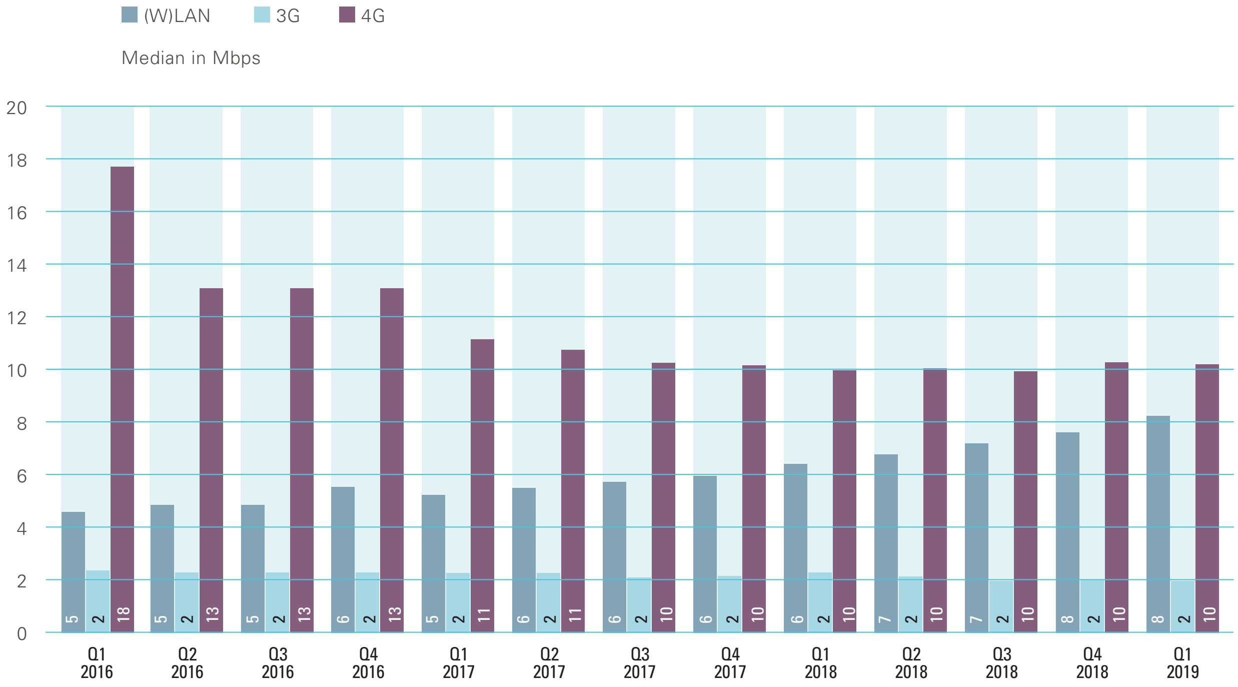


Source: RTR-NetTest

Figure 8 depicts the median[39] download speed measured with the RTR-NetTest over time, broken down by type of technology. It can be clearly recognised that, based on median, far higher download speeds can be reached with 4G mobile telecommunications technology than with (W)LAN or 3G. However, the download speed for 4G has fallen since the start of 2016. This trend was reversed in the period between Q2 and Q4 2018, with download speeds rising from 28.9 Mbps to 31.4 Mbps. In Q1 2019 the download speed for 4G mobile services fell once again, however, to 30.7 Mbps. 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' as a result of market competition and demand, until the next technology (often associated with new spectrum) creates in turn new capacities. Consequently, the figure does not suggest a deteriorating quality of connections or in fact reveal anything about net neutrality. Of all the technologies assessed, the lowest download speeds were achieved with 3G. Considering the low data transmission rates supported, 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.

[39] 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.

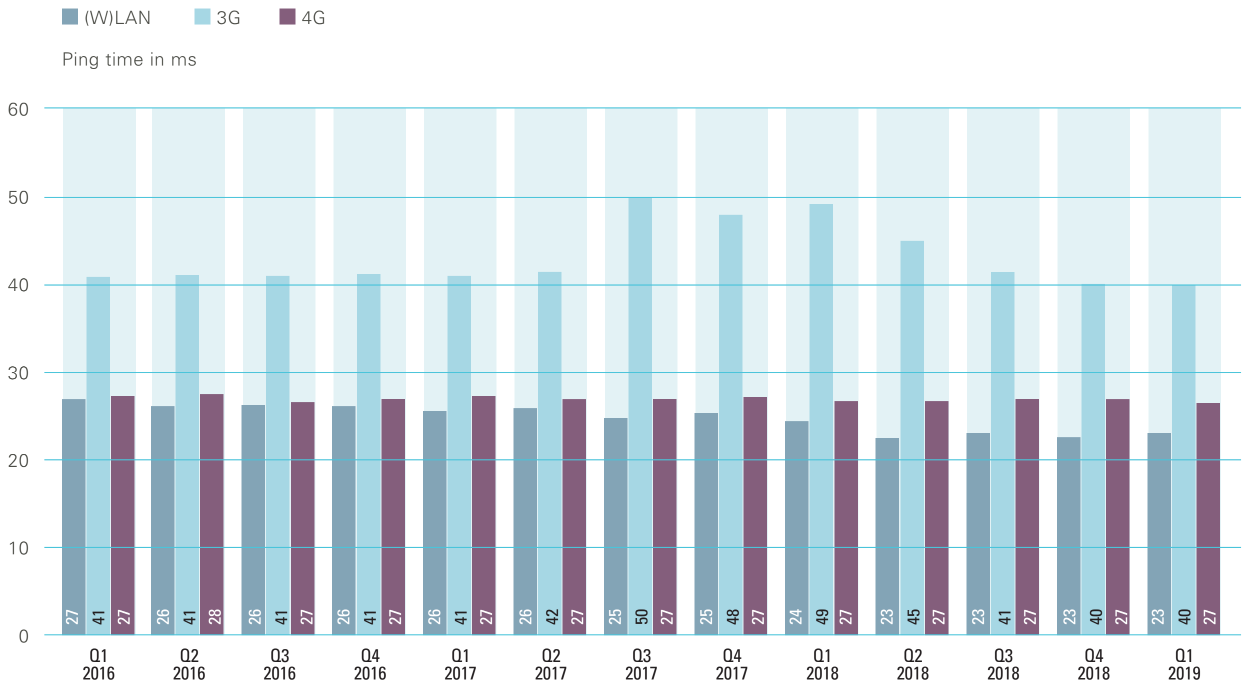
FIGURE 09: UPLOAD SPEED BY TECHNOLOGY



Source: RTR-NetTest

Figure 9 depicts the median upload speed. While this chart once again underlines the fact that 4G mobile technology enables the fastest upload speeds, a decline can also be ascertained. This decline did not persist in the reporting period, however, with the upload speed staying relatively constant at 10 Mbps. The upload speed measured for (W)LANs has risen constantly and was around 8 Mbps at the end of the reporting period. The upload speed for 3G mobile connections remains relatively constant at around 2 Mbps.

FIGURE 10: LATENCY (PING) BY TECHNOLOGY [40]

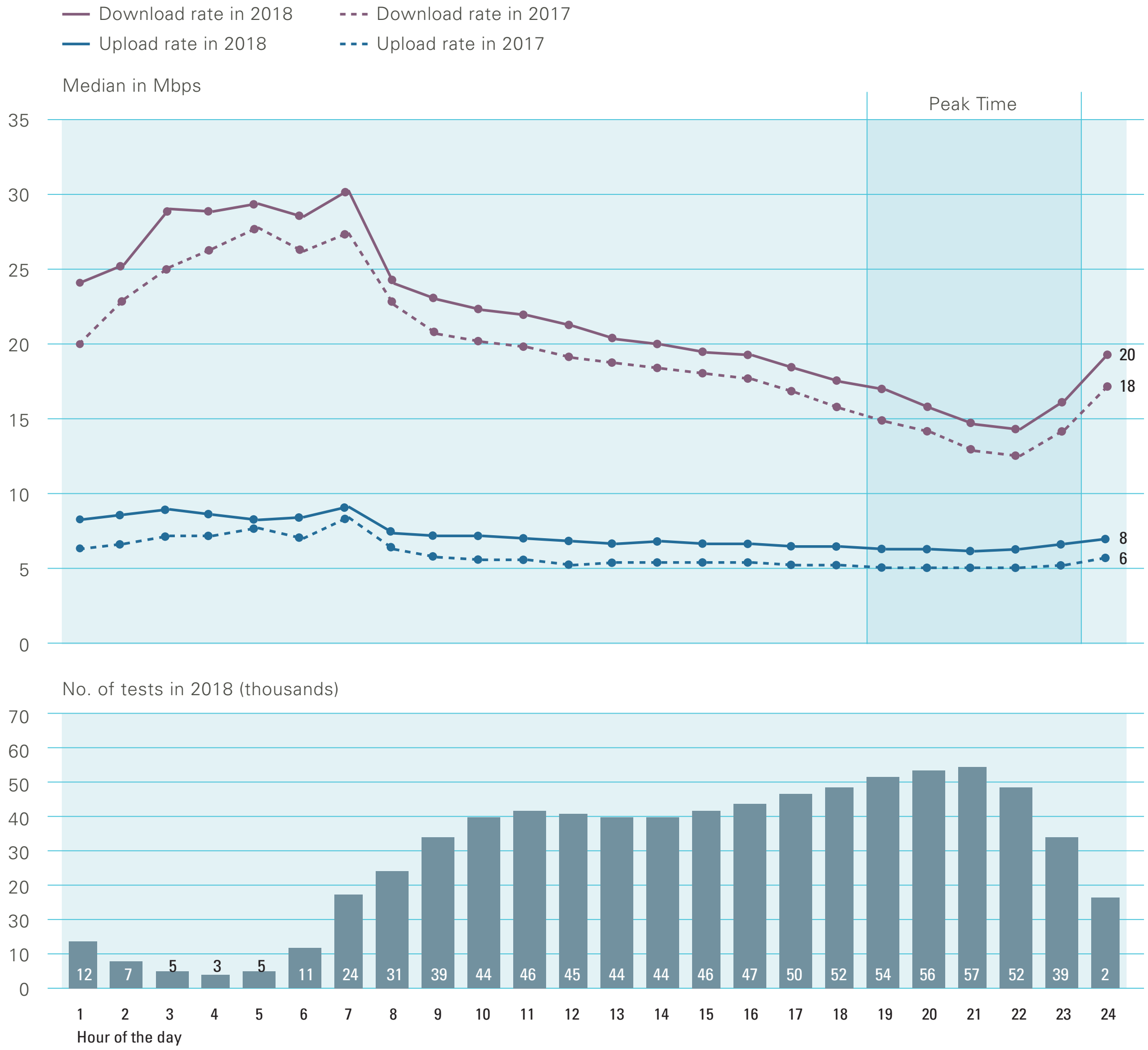


Source: RTR-NetTest

Figure 10 depicts median latency. Roughly the same figures for latency (between 22.5 ms and 27 ms) can be achieved using 4G mobile technology and (W)LANs. The figures are relatively constant for (W)LANs and 4G in the reporting period. With 3G, however, latency is much higher, although this has again decreased from 45 ms to 40 ms since Q2 2018.

[40] 'Ping' (or 'latency', the technically correct term) 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. The ping time is measured in milliseconds (ms). While latency is a key indicator with online games, ping time can also have a significant impact on the 'sluggishness' of access when normally surfing in the internet. Both the technology used to access the internet and the extent to which access is utilised significantly affect latency.

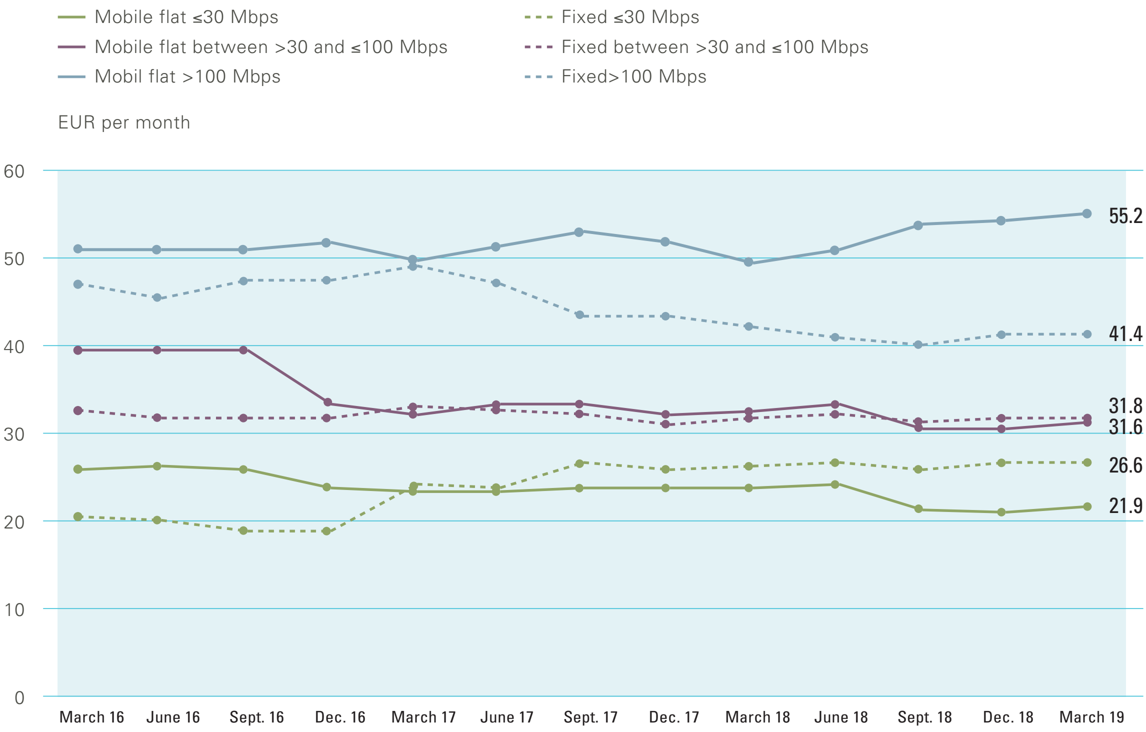
FIGURE 11: DOWNLOAD AND UPLOAD SPEEDS BY TIME OF DAY IN 2017 AND 2018



Source: RTR-NetTest

Figure 11 shows the median download and upload speeds by time of day over the last two years. The median download speed in 2018 was slightly higher than in 2017, by an average of approx. 2 Mbps. The median upload speed in 2018 was around 1.3 Mbps higher than the figure for the previous year. The figure also shows that the median download speed falls sharply between 18:00 and 22:00, although no similar pattern is discernible for the median upload speed. Most of the measurements were also made during this period in 2018 (over 50,000 every hour). During early morning hours between 4:00 and 7:00, the download speed is the highest, at roughly 30 Mbps in 2018. In the course of the day the median download speed drops continuously to only about 15 Mbps between 21:00 and 22:00. The median upload speed during the day is relatively steady at about 7 Mbps.

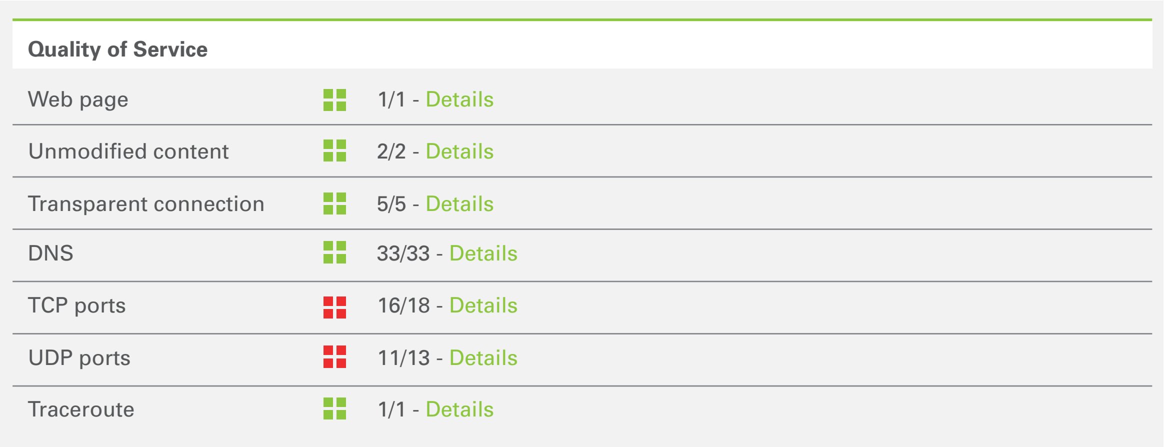
FIGURE 12: PRICE BASKETS FIXED VS. MOBILE BROADBAND



Source: RTR

Figure 12 contrasts the three price baskets for fixed network broadband (each without TV) with the three price baskets for mobile broadband (with unlimited data volume). 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. It is clear that, for higher bandwidths (>100 Mbps), mobile broadband is more expensive than fixed broadband (prices between EUR 40.20 and EUR 55.20), with the reverse being true for lower bandwidths (≤30 Mbps; prices between EUR 21.10 and EUR 26.60). From May 2018 to March 2019, prices for mobile broadband at high transmission speeds (>100 Mbps) rose slightly, while prices fell slightly for mobile broadband at low transmission speeds (≤30 Mbps). In the category >30 to ≤100 Mbps, prices remained virtually the same during the reporting period and have also been relatively constant historically (prices between EUR 30.70 and EUR 33.40).

FIGURE 13: 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 testing

Figure 13 shows an example of a result from the RTR-NetTest quality of service test. A green light depicts a positive test result. 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, while download speeds improved somewhat and no significant decline in upload speeds could be recognised.

07 Focus topic
zero-rating

7.1 What is zero-rating?

Zero-rating offers are offers in which the amount of data consumed by particular applications (apps) or services/content is not counted towards the volume of data included in the mobile services subscription;[41] this data usage is therefore charged at a rate of 'zero' (i.e., it is 'zero-rated'). The discussion about zero-rating is part of a larger European debate on the subject of net neutrality, which within the EU is governed by the TSM Regulation. This Regulation came into force in mid-2016 and additional information is provided in the BEREC guidelines for interpreting the provisions of the Regulation. Since over the last few years zero-rating has developed into a major subject of interest in the net neutrality debate, BEREC is also planning to lay out further specifics regarding relevant regulatory approaches to scrutinising zero-rating in a revised version of the guidelines. Given the growing significance of this subject, RTR has also decided to spotlight zero-rating in this year's Net Neutrality Report. RTR also intends to highlight specific aspects of net neutrality, each with their own areas of focus, in the years to follow.

First we will look at the regulatory framework. It has already been mentioned on more than one occasion that the goal of the provisions of the TSM Regulation is to preserve open access to the internet for end users (retail consumers as well as content and application providers – 'CAP's), and to ensure that the internet continues to remain innovation-friendly. The 'theory of harm' underlying zero-rating offers is not so much one of (in) efficiency as it is one of competitive distortions in downstream CAP markets, while there are fundamental concerns regarding the potential negative impact on innovations over the longer term. Innovations are central to economic and social development and comprise the engine that drives substantial change in many areas of life. In other words, the net neutrality discussion is also largely about ensuring (future) innovative power.

The TSM Regulation does not use the term 'zero-rating' at all – even though there was an intense discussion before the Regulation was adopted. Zero-rating is addressed in connection with paragraph 2[42] of Art. 3 (Safeguarding of open internet access) of the TSM Regulation in conjunction with Art. 1. According to the general understanding of the regulatory authorities, zero-rating is not prohibited in principle but rather the benefits and disadvantages should be weighed on a case-by-case basis, with all of the ramifications taken into consideration.

[41] Zero-rating is generally not relevant to fixed network tariffs since most products already offer flat rates, which means that data usage does not play a significant role in the design of the tariff.

[42] There is stated: (2) Agreements between providers of internet access services and end users on commercial and technical conditions and the characteristics of internet access services such as price, data volumes or speed, and any commercial practices conducted by providers of internet access services, shall not limit the exercise of the rights of end users [RTR note: this means retail consumers and CAPs] laid down in paragraph 1.

In the European Union (EU), zero-rating is practised by a number of mobile network operators (see in this regard section 7.4 below) and can be found in several different forms, such as:

- an exclusive or nonexclusive offer of a service provided as zero-rated;
- an offer that encompasses one service (a specific application) or a category of services;
- an offer that is updated at specific intervals and references a 'Most Popular' list (for example, top downloads in app stores);
- an integrated offer by an ISP;
- an offer involving payment by a CAP for having its app zero-rated (sponsored data);
- a component of a tariff or a tariff add-on that can be added by the customer for a specific charge;
- an offer that is possibly also associated with technical differentiations (throttling of the service, discriminatory treatment based on data volume used);
- an offer that may have varying levels of intrusiveness with regard to the underlying traffic management or the measures for identifying and charging for traffic. Consequently, it may also in some cases – to varying degrees – conflict with the provisions of Art. 3(3) second and third subparagraphs;
- and similar offers.

In addition, combinations of the features listed above as examples are also possible (for instance, as an exclusive, proprietary offer by the operator). Normally, the various options are to be evaluated differently with a view to their effects. A number of potential benefits are generally associated with zero-rating, including, for instance, the following:

- end users are able to purchase a service without that particular service being counted towards the data included in their subscription (in other words, the users are able to consume more of that service);
- it potentially enables providers to win over new end users;
- Zero-rating can boost competition among ISPs (it is also generally utilised as a competitive dimension);
- Zero-rating can also potentially advance CAPs' efforts to enter the market since it increases the likelihood that they will be chosen by customers.

There are also a number of potential disadvantages offsetting the possible benefits:

- With zero-rating, an ISP may select the applications to be included in the offer; the ISP defines the categories, draws distinctions between them, specifies the technical standards and other wholesale conditions or criteria. If there is no open zero-rating offer, the provider chooses de facto winners and losers in the downstream markets and in doing so becomes the gatekeeper.
- Zero-rating offers harbour the risk of market fragmentation and higher transaction costs, since in the worst-case scenario, a CAP would have to negotiate with every single mobile network provider over wholesale contracts (each of which may be different). This and other factors (how categories are defined, wholesale contract language and terms and conditions, etc.) contribute to the erection of barriers to market entry and may result over the longer term in a reduction of end users' choice of CAPs.
- Zero-rating can influence competition between MNOs, and also between MNOs and MVNOs and/or resellers. MNOs combine zero-rating with strategies such as product upselling and competitive differentiation. MVNOs, on the other hand, generally pay for their wholesale sourcing per unit, so that marginal costs equal to the wholesale price are always incurred; MVNO process are at a disadvantage with zero-rating because, as a rule, they are exposed to a higher risk than MNOs, which have nearly zero marginal costs.

Given the potential benefits and disadvantages of zero-rating, it is easy to understand why, although zero-rating has not been banned as a rule by the TSM Regulation, its impact still needs to be scrutinised on a case-by-case basis. For this reason, RTR has taken the initiative at this early stage to look at the question of the particular aspects that should be examined on a case-by-case basis, and has come to these preliminary conclusions:[43]

- The question that needs to be answered is, what kind of pull might the zero-rating product be exercising, i.e. how appealing is it? In essence this means assessing whether the offer limits the consumer's freedom of choice (over the short or long term) and whether consumers retain their ability to additionally choose other offers, thus maintaining access to innovations in future. Key indicators for this are the ratio of the volume of zero-rated data consumed to the volume of data included in the tariff, and the price/GB.
- In addition, the ISP's market position, the range of the zero-rating offer, and the market position of the CAP whose services are zero-rated should be assessed. The impact on the retail mobile network markets and on the downstream markets (in which the CAPs are active) should also be taken into consideration in this process.
- The contract between CAP and ISP is also relevant. The question is whether such a contract exists and what any underlying terms and conditions might be. Related to this are issues such as barriers to market entry and barriers to expansion for CAPs, market segmentation by the ISP and exclusive agreements.
- Ultimately, any zero-rating offer also needs to be assessed in the context of offers already available in the market. If key applications with high market penetration are already offered with zero-rating by two MNOs, for instance, and if the volume included for those applications is high in comparison to the remaining included data, a third such offer would be assessed differently than a new offer. Cumulative effects extending across providers should thus also be examined as required (which, taken the other way around, nonetheless does not mean that a single zero-rating offer would not result in intervention by the regulatory authority).

The extent to which a product is (un)problematic in view of the TSM Regulation's 'theory of harm' can be determined based on the answers to these questions. The more appealing the product and the stronger the market position of the CAP(s) and ISP(s), the more likely it is that end users' freedom of choice will be limited. The more complex or more restrictive any wholesale contracts are, the more likely it is that CAPs will face barriers to their market entry or expansion due to zero-rating. Based on European decision-making practice to date and the regulatory authorities' common understanding, it is clear that any technical differentiation that treats zero-rated traffic differently (for example, by slowing it down) than other internet traffic is equally prohibited as a product where, after the included data has been consumed, no other services are available or are only available with some kind of limitation but where zero-rated traffic, by contrast, can continue to be used without limitation. While it is true that zero-rating does not require ex-ante approval from the authorities, these types of technical discrimination nonetheless constitute a breach. As a rule, sponsored data and exclusive agreements with a mobile operator also tend to draw more attention from regulatory authorities.

To review the effects of zero-rating, RTR gathers data on the use of zero-rating offers at irregular intervals.[44] The dimensions surveyed include the number of users of zero-rating offers, the number of users whose use exceeds the data included in the tariff, the data included in the tariff, the data actually consumed, and the total zero-rating volume consumed. These data are collected monthly for each tariff. If there are multiple categories of applications in a zero-rating offer (for instance, audio, video, social network, and chat services), the zero-rating volumes consumed per category are also queried. In the case of offers with a special dynamic or range, the wholesale contracts are also analysed. The impact of the zero-rating offer on downstream markets will then be examined in detail if (for instance) the offer's range is broad, usage is intensive, there is potentially an identical offer from another MNO and where the CAP has any special market position. For zero-rating offers that are comprised of whole categories of services, no data regarding use of individual applications is collected (for instance, regarding Facebook in the category 'social networks'), as this would raise data privacy issues. At most there would be a question regarding the entire category on offer. The information provided below outlines several of the findings from ongoing monitoring (while still safeguarding business and trade secrets).

[43] Zero-rating has become a key topic in the European debate regarding the openness of the internet and there are a number of relevant offers; given the aim of European harmonisation, RTR consequently believes it will be necessary in any case to adjust the assessment criteria in the event that new guidelines regarding a (potentially) revised net neutrality regulation specify other criteria.

[44] The surveys are taken two to three times a year depending on the variability of the product, its range and the underlying marketing expense. These surveys are based on the provisions of Art. 5 (Supervision and enforcement) of the TSM Regulation.

7.2 A look at the consumer side

As of April 2019, 18 different tariffs including zero-rating offers were being marketed by three mobile service providers (A1, Kurier mobil and Krone mobile). In addition, there are nine add-ons – in other words, packages that can be added to specific tariffs or to all tariffs – from two providers (A1 and H3A), which means that at present, offers from a total of four companies are available on the market. However, in the case of two of these companies – Kurier mobil and Krone mobile – the only service offered that does not count towards the included data is the electronic download of their newspaper product as ePaper. As these offers are of little significance in the mobile telecommunications market and only encompass a single zero-rated product, they will not be addressed further.

This leaves two key zero-rating players in the Austrian mobile telecommunications market with relevant end user offers. No new offers have been launched by H3A since December 2016, making A1 the most recent mover and shaker, switching its core brand's entire product range to zero-rating and also introducing zero-rating categories for B.free in April 2019.[45] Within the A1 Go! (for private and business customers) and A1 Xcite (for private customers) product lines, every tariff first marketed as of April 2019 now includes a zero-rating component (under the Free Stream brand). Specifically, A1 has structured its offer to encompass four zero-rating categories: audio/music streaming services, video streaming services, chat services and social media services. Generally speaking, any of a CAP's applications that can be allocated to one of the four categories can be included in A1's zero-rating component, making it accessible for the end user without the data used in connection with the service counting towards the included data. A1's wholesale offers are thus basically open (see also section 7.3 below in this regard).

Additionally, for contracts entered into before 1 May 2017, A1 also offers add-ons (with prices of between EUR 3.90 and 9.90). Nevertheless, the vast majority of A1 customers are enjoying zero-rating via new contracts, since any growth in the core brand's tariffs always means zero-rating growth as well.

As for H3A, the second large provider of zero-rating services, the company's zero-rating products offered in March 2019 are designed as add-ons that the customer can add to the tariffs. The first zero-rating offers from H3A date back to 2004; the bulk of the offers were launched prior to the date the TSM Regulation came into force (and in certain cases also adapted to the provisions of the TSM Regulation). H3A's offers include services such as Spotify (which can no longer be ordered), 3 Film and 3TV, Kiosk (newspapers and magazines), and its own cloud services. H3A does not have an open offer accessible to various CAPs like the A1 offers; the offers are either arranged individually or there is a selected partner, as with Spotify. Overall, however, the number of actual users of H3A's zero-rating offers is considerably lower than those of A1, which is why it is the A1 product range that we will be primarily addressing below.

The share of users who either have tariffs with zero-rating included or who take advantage of an add-on is about 5–15% of all customers who have a mobile data or smartphone subscription.[46] The upper limit here is based on the assumption that all customers who have a relevant tariff component as an add-on are taken into account. The lower limit is based on the number of active users.

[45] The B.free component covers the category 'chat' and is available in the two tariffs B.free L and B.free M. See: https://www.a1.net/handys/mehr/b-free/s/wertkarte (in German). At present there is no zero-rating in the A1 yesss! product line.

[46] The upper limit is defined in particular via H3A's Mobile TV product, which was frequently added to tariffs prior to the TSM Regulation coming into force. Actual use, on the other hand, lags far behind.

One of the concerns that accompanies the introduction of zero-rating offers is the possible increase in price per GB; in other words, that either the price of the tariff will increase and/or the included data will be reduced as a result. This could be based on the reasoning that appealing services that the customer would use regardless are already included in the zero-rating offer, and therefore the customer would need a smaller volume of freely available data, which is why this could also be limited. From a net neutrality perspective, this kind of development is worrying, since it would mean that an increasingly smaller volume of data (or an increasingly higher-priced data volume) would be available to the end user to be used for other or new services.

The table below provides an overview of the A1 product portfolio for private customers, which make up the majority of zero-rating subscribers.

TABLE 05: A1 GO! AND XCITE PRODUCT PORTFOLIO – RANKING OF TARIFFS

Tariff plan	Ranking by price/ GB (low to high) as of 04/2019	Ranking by absolute price (low to high) as of 04/2019	EUR/GB as of 03/18	EUR/GB as of 04/19	Delta price 03/18 to 04/ 19 in %
A1 Go! Premium	1	7	-	0.90	-
A1 Go! XL	2	6	1.30	1.33	+2.57
A1 Xcite L	3	2	1.99	1.99	0.00
A1 Xcite S	4	1	2.74	2.19	-20.00
A1 Go! L	5	5	2.41	2.50	+3.45
A1 Go! M	6	4	2.99	3.12	+4.18
A1 Go! S	7	3	4.74	4.99	+5.28

Table 5 shows that there was a slight price increase in most of the A1 tariffs. Nevertheless, this does not allow any generalisations, since the period of observation was only about one year. Moreover, the trend in the RTR Internet Monitor's broadband basket (01/2019)[47] shows few if any changes. Currently, there does not appear to be any sign of any easing in competitive pressure, which in the broadband segment for private customers is reinforced by the fixed network. It is also apparent that, while the two tariffs in the Xcite line intended for young people have the lowest prices, they only range around average as far as prices per GB go. The situation is different for the Go! line: the increase in prices is accompanied by an improvement in the price/GB ratio such that, in terms of included data volume, high-end products offer the most advantageous ratio.[48] Also with regard to the zero-rating categories included in the respective tariff (see table 6), we see that the most expensive tariffs each include zero-rating categories while the less expensive tariffs mostly include only audio streaming and chat services. This trend is broken only by the A1 Xcite L tariff for young people, which also includes social media services.

A closer look at A1's zero-rating offers also reveals the following trends: as expected, the volume of zero-rated data per subscriber increases in each tariff. This is attributable firstly to the fact that every new customer simultaneously becomes a zero-rating customer, and secondly to increasing intensity in usage, which in turn is related to the fact that additional zero-rating categories were introduced over the course of 2019. For private customer tariffs, chat services were included in September 2018 and social media offers were included in October 2018. For business customer tariffs, both of these categories were included in October 2018.

TABLE 06: TARIFF PLANS WITH ZERO-RATING AVAILABLE TO A1 PRIVATE CUSTOMERS – APRIL 2019

	Price1 = least expensive tariff	Audio streaming	Video streaming	Chat services	Social media services
A1 Xcite S	1	x		x	
A1 Xcite L	2	x		x	x
A1 Go! S	3	x		x	
A1 Go! M	4	x		x	x
A1 Go! L	5	x	x	x	x
A1 Go! XL	6	x	x	x	x
A1 Go! Premium	7	x	x	x	x

[47] https://www.rtr.at/de/inf/internet-monitor-12019-ePaper (in German).

[48] situation that can also be found internationally. Also see the RTR study on zero-rating discussed in section 7.4, which is available for download at https://www.rtr.at/de/inf/ZeroRatingEU2019.

Measured as the ratio of zero-rated data used and data included in the tariff to all zero-rating tariffs in Q1 of 2018 (i.e. at the end of the last reporting period), use was still nearly zero or well below 10%. By April 2019, in contrast, the figure had risen to between 5% and 10% – irrespective of the tariff. There was a tenfold increase in the ratio when calculated as a weighted (by zero-rating subscribers) average across all private customer tariffs. The increase was smaller for business customers. A major increase is also identified at the end of Q1 2019, which was partly attributable to zero-rated video offers (in the higher-end tariffs). Explanations by A1 point to possible effects from extraordinary events such as the Champions League or even the finale of the series 'Game of Thrones' (not only the finale but all of the seasons could be viewed again). This does not seem implausible, since starting in April 2019 the use of zero-rated video offers drops off again significantly and is only slightly higher than the level existing in January of the same year. Nevertheless, demand for the use of the zero-rating offer definitely appears to fluctuate.

The 'consumption' of data by consumers usually falls far below their included data – in other words, they generally wish to remain on the safe side when choosing a tariff. In view of this fact, the ratio of data consumed for zero-rated services to the total volume of data actually consumed (including zero-rating) can provide further insights. Depending on the tariff, for private and business customers this proportion ranges from below 10% to up to 30%, whereby we should also point out here that there was a significant, short-term increase in the first quarter of 2019.

With regard to the concerns expressed above, these proportions mean that the average data included in each tariff was still significantly higher than the average volume of zero-rated data consumed, despite a considerable rise in zero-rating overall as well as in all of A1's individual categories. This means that the zero-rated volume utilised within the tariff on average by all customers could also be easily covered through the included data. Because the number of A1 subscribers with zero-rating tariffs (included zero-rating and zero-rating as an add-on) still comes out to considerably less than 10% and A1's market share in the private customer segment is less than 50%, there has thus far been no reason to assume any limitation of end users' choice to an extent that would raise concerns Therefore, from the perspective of the authority, the commercial agreements to date (Art. 3(2) of the TSM Regulation) do not currently endanger the rights of end users (consumers or CAP) as set out in Art. 3(1) of the TSM Regulation.[49] Given the current data situation, the conclusion might be different if there were no similar tariffs (without zero-rating) available in the market – if customers were in effect forced into a zero-rating offer and the pull were commensurately stronger. However, given current competitive pressure in the mobile retail markets and the existence of similarly structured offers with and without zero-rating, the conclusion is not warranted at present.

The information on A1's Free Stream offers provided thus far has dealt with zero-rating as a whole or individual tariffs and customer categories, as well as the question of how powerful the pull exercised by these products is and whether innovations might be hampered (via the effects on the end user side). Admittedly, this view is inadequate for the assessment of the effects on downstream markets. Other levels need to be examined here. As a first step, we will now shift our focus to individual categories of zero-rating products.

[49] See recital 7 of the TSM Regulation. (7) [...] Such agreements, as well as any commercial practices of providers of internet access services, should not limit the exercise of those rights [Note: under Art. 1 TSM Regulation) and thus circumvent provisions of this Regulation safeguarding open internet access. [...] National regulatory and other competent authorities should be required, as part of their monitoring and enforcement function, to intervene when agreements or commercial practices would result in the undermining of the essence of the end users' rights.

It has already been mentioned that new zero-rating categories were added to A1's offers during the current year under review (in September and October of 2018), meaning that, at most, a comparison extending beyond the period of the last year is possible only for the two categories of audio and video streaming. One such comparison shows that the percentage of zero-rated audio services relative to the total (now much larger) zero-rated volume has fallen significantly, whereas, by contrast, the decline has turned out to be more moderate for video services.

Percentages weighted by subscribers demonstrate that, across the entire private customer tariff portfolio of the A1 core brand, the chat services offered in all A1 tariffs accounted for by far the largest share of zero-rated traffic. By contrast, video streaming placed far behind this, which in all likelihood is related to the limitation to three (of seven) comparably expensive tariffs, since, in every tariff in which the two options were offered, the zero-rating consumption of video services closely approached that of chat services. For the same reason (lower number of tariffs with fewer users), video services as a whole also remain behind audio services. For business customer tariffs, in contrast, the picture is more balanced. In this segment, audio streaming and chat services were at basically the same level at the end of the reporting period. Video services lagged considerably behind and social media services were left in the dust. This ranking as well is also almost certainly due to the fact that the latter two categories are provided within only a few tariffs.

More specific conclusions regarding the traffic volume within individual categories, in other words per service, are unable to be drawn from this information, since such data are not collected by A1 and other companies, nor is this permitted under data privacy legislation. The CAPs also do not collect traffic volume data, which is why the impact of the zero-rating offer on the position of an individual CAP in the respective market cannot be determined. The latter is explained by the fact that the respective category definitions do not necessarily comprise only one downstream market[50] but instead may very well relate to different markets. From the viewpoint of the regulatory authority, any interventions are to be justified on the basis of the overall context as unpacked here and on the evaluation of the categories. In doing so, it might need to be assumed that all of the zero-rating traffic under one category is attributable to a specific application. A more thorough examination of the various downstream markets after a specific service in a zero-rating category is added is not feasible after the fact, since the markets are dynamic, and a separate review needs to be performed in each case for market delineation (national and international) and product market definition. The fact that many zero-rating products are platforms, i.e. multifaceted markets, increases the complexity. A more thorough examination would always take place to investigate any claims of competition challenges, if customer complaints became more frequent[51] or if the overall picture clearly pointed towards a higher utilisation of zero-rating services, with a stronger pull exercised by a single category and beyond merely a single operator.

[50] So, for instance, Amazon Prime Music does not belong to the same market as Radio 88.6, and yet both services are in A1's 'Music/Audio' category.

[51] To date, there have not yet been any cases involving zero-rating in the RTR monitoring system for customer issues.

7.3 Wholesale level: the CAP–ISP relationship

To complete the picture, in addition to a more detailed view of the situation from the consumer side as set out in the section above, we also need to examine the wholesale level. Here as well it is primarily the products offered by A1 that are of interest, since other providers do not have corresponding categories in which CAPs can be included openly, or do not or no longer push zero-rating offers. As stated at the start, at the wholesale level the primary concern is the openness of the offer and its terms and conditions, which can become barriers to market entry or expansion.

In principle, any service provider offering services in one of the specified categories can become an A1 zero-rating partner. To date, RTR has not received any complaints to the contrary and A1 has not reported any such in connection with monitoring. There was only one company that had showed interest in becoming a partner, but it ultimately decided on its own accord to shelve the idea. According to information provided by A1, the average length of time required to include a new CAP in the offer is about two to three months.

A1 makes the decisions regarding category definitions and allocating a specific service; this makes A1 the gatekeeper, determining the number of tariffs and/or the number of customers who can be reached. There is nothing in place to allow individual (as the case may be, particularly strong) CAP partners to have a say regarding the inclusion of new zero-rating partners in the offer. If there is a legitimate suspicion that a streaming service breaches statutory provisions (e.g. copyright law) or contains inappropriate content, A1 can refuse to allow participation in the programme or, if the service is already being offered, suspend the service if necessary after demanding that conformity with the law be established. A1 can adapt the scope and structure of the zero-rating offer as well as the allocation to tariffs at its own discretion; any decision regarding discontinuing the offer also lies exclusively within A1's purview.

As far as the scope of the zero-rating offer is concerned, A1 distinguishes and defines each of the four categories mentioned above. This is an attempt to precisely delineate which component of traffic is now actually subject to zero-rating.[52]

As for the technical terms and conditions for inclusion in the offer, A1 stipulates that zero-rating can only be implemented if the streaming partner keeps A1 continually informed of the precise and complete technical specifications allowing A1 to separate the zero-rating content from other content. In A1's view, the appropriate technical specifications are comprised of:

- IP addresses
- URL (uniform resource locator)
- SNI (server name identification)
- Protocols

In RTR's view, while the use of the IP address for traffic identification seems unproblematic, there are nevertheless doubts concerning the other options as to whether these are compatible with the provisions of Art. 3(3) second subparagraph of the TSM Regulation and applicable data privacy law. A broader discussion of this issue has flared up recently in data privacy circles as well,[53] but we will have to wait for the revised BEREC guidelines to learn of the outcome and any ramifications. Nevertheless, it is a fact

[52] For example, chat services are defined as "solely text, image, video and voice messages via the respective app, provided such are received and/or sent as a completed message"; any other services that might be able to be used in the app, for instance live voice or video telephony, or externally linked content, are excluded from the zero-rating offer. Quoted from the General Terms of Service "under which streaming partners can participate in the A1 Free Stream offer by A1 Telekom Austria AG".

[53] Vgl. etwa das Schreiben der EDRi an verschiedene Institutionen: https://edri.org/wp-content/uploads/2019/05/20190515_EDRiOpenLetterDeepPacketInspection.pdf

that in the majority of cases, traffic for the participating services is not identified using the service's IP address as the distinguishing feature.

Additionally, A1 also reserves the right to reduce the bandwidth for zero-rated video content made accessible based on adaptive bitrate technologies. From the perspective of the regulatory authority, this kind of interference is not permitted pursuant to Art. 3(3) of the TSM Regulation, which is why the TKK reached a corresponding decision in December 2017 – just before the launch of the first Free Stream tariffs. As of the time this report was prepared, the proceedings had not yet been concluded; at present no reductions in bandwidth are taking place due to the provisional application of the decision by the TKK.

During the talks concerning the launch of Free Stream, RTR also pointed out to A1 that – even if the court decision permitted a reduction in bandwidth – each customer would nonetheless have to be given as soon as possible the option of temporarily (for instance, to be able to view a film in the best possible quality) or even permanently opting out of and back into the zero-rating offer.

In other respects, liability is assumed under the wholesale offer only for wilful misconduct or gross negligence, whereby the amount of liability is limited to EUR 50,000; the preparatory period required to amend the wholesale terms and conditions of business is at least four weeks, the legal venue is Vienna.

The fundamental problem is that, in particular cases, such wholesale offers put the ISP in a special position through the definition of categories and allocation policy, and as a whole they contribute to strong market defragmentation (many providers with different category definitions, allocation policies and other rules) with high transaction costs. Apart from this, the main concerns involving wholesale provisions continue to be the problematic issues of data privacy and traffic identification, as well as technical limitation and discrimination. A glance at the offers available in April 2019 in table 7 also shows that it is not just large international companies that are taking part here: many national CAPs are also interested in being included,[54] expecting customers to use their services more often if they are zero-rated. For end users as well, zero-rating offers provide a benefit for the short term (since they result in an additional product option), at least as long as the disadvantages for innovation and market entry addressed above are not severe.

[54] In its study "The Net Neutrality Situation in the EU. Evaluation of the First Two Years of Enforcement" (2019), under the heading "New entry barriers for the provision of online services", epicenter.works et. al. also expresses the apprehension that zero-rating offers are resulting in an attenuation of European services on offer and that national services or worldwide offerings will win out. Since the regulatory authority has no figures on the use of services without zero-rating, nothing can be stated at this time to allay this apprehension.

TABLE 07: GEOGRAPHIC DISTRIBUTION OF STREAMING SERVICES BY REGION AND CATEGORY

Co. headquarters / Category	Video	Music/audio	Chat	Social
Number in Austria	5	12	0	0
Number in the rest of Europe	12	3	1	0
Number in the rest of the world	2	3	3	2

As of April 2019

For an overall picture of the Austrian market, the issue of the future of zero-rating offers also needs to be raised. The more data is included in tariffs and the stronger the competitive pressure is towards flat-rate offers, the less appealing zero-rating offers start to look. It remains to be seen whether zero-rating offers should be viewed as upselling strategies intended to make it more appealing for companies to enter the field of flat-rate products. The fact that Magenta has not offered any such tariffs to date and is now offering flat rates for its top-of-the-line smartphone products (5G Ready, Mobile Gold, Mobile Platine) could imply that zero-rating products are possibly just a short-term, interim step towards a broader distribution of mobile flat-rate products. It has also been noted that H3A has not launched any new zero-rating offers in quite some time and that existing offers (like Spotify) are expiring. In any event, support to ensure a competitive environment remains essential for development of the mobile telecommunications markets.

The following portion of this special section on zero-rating expands on the issues and deals with the international significance of zero-rating offers and their effects on prices and included data volumes. At its heart is a comprehensive econometric analysis that examines the previous impact of zero-rating offers.

7.4 Empirical econometric analysis of zero-rating in the EU

Regarding the impact of zero-rating, many theoretical papers have been published to date but hardly any empirical studies.[55] For this reason, in late 2018 RTR decided to prepare an international comparative study focusing on two questions central to the debate on net neutrality: first, what effects do zero-rating offers have on the volumes of data included in the tariffs; and second, to what extent does the introduction of zero-rating lead to an increase in prices per GB of transferred data? Both concerns are significant because they reduce the incentive to utilise offers without zero-rating and may also limit innovation (for instance by decreasing incentives, exercising a pull or erecting barriers to entry).

As part of the study, an analysis was conducted on tariff data (including information on zero-rating) from over 11,000 tariff plans offered by more than 50 different mobile network operators in 15 EU Member States during the period 2015–2018, with the objective of determining the effect of zero-rating on the volume of included data, prices and prices per included data unit.

According to the data, specifically in the period from the first half of 2015 to the first half of 2018, the significance of zero-rating increased in the 15 countries examined: the number of mobile network operators offering tariffs that included zero-rating for specific applications rose from only 5 to 20, while the percentage of tariffs within the sample that included zero-rating rose from about 5% to some 25%. This percentage varied considerably from country to country, and in most countries over the course of time as well. In the second half of 2018, there was some decline in the percentage of zero-rating offers, and several operators discontinued theirs altogether.

While the percentage of offers that included zero-rating increased, data caps (volume of included data) also increased significantly at the same time, and in several countries the percentage of flat-rate tariffs increased as well. A comparison between tariffs with zero-rating and tariffs without zero-rating shows that zero-rating plans are more expensive on average, include a higher data cap and feature a lower price per GB. This is a result that is also in line with national observations (in this regard, see table 5 and table 6 in section 7.2).

In order to more precisely analyse the differences between tariffs with and without zero-rating, regression analyses were used to allow to control for factors such as other tariff features and systematic differences between operators and over time (constant operator and time effects). Additionally, an operator-level basket approach was used, allowing developments at the operator level to be followed. This was done to determine how changes in the percentage of offers from a particular operator that include zero-rating affect other tariff features.

The study found no consistent evidence across all countries and the entire period that would suggest that zero-rating reduces included data, or increases the prices per GB or monthly prices. Some of the findings actually indicate that, all other things being equal, zero-rating is associated with higher data limits and lower prices per GB. Nevertheless, these findings are not statistically significant for all specifications.

When looking at the effect of zero-rating at the country and period level, it becomes clear that the direction and magnitude of the effect (and its statistical significance) vary considerably from country to country as well as within several countries over the course of time. It was not possible, however, to identify a particular pattern that might help explain or predict the effect (such as a tendency over time or at the country level, or the

[55] One of the few germane publications comes from epicenter.works (2019): "The Net Neutrality Situation in the EU. Evaluation of the First Two Years of Enforcement", available at: https://epicenter.works/sites/default/files/2019_netneutrality_in_eu-epicenter.works-r1.pdf

number of mobile network providers or countries with higher data limits in comparison with countries having lower data limits).

Finally, we now look at the effect of zero-rating across different categories of apps. Viewed thus, we find that tariffs including only social media and chat apps are associated with a higher volume of included data and a lower price per GB than the control group (tariffs without zero-rating). For tariffs including only zero-rated video or audio apps, the reverse tends to be observed.

Overall the study comes to the conclusion that zero-rating appears to have no systematic effect on other tariff features such as included data, price and price per GB. 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. Where zero-rating is to be assessed on a case-by-case basis (and the effects on the market as a whole), the assessment of the specific effect in individual countries should be undertaken in a way that takes into account the situation in that particular country.

RTR's study, in English, can be downloaded from
https://www.rtr.at/de/inf/ZeroRatingEU2019.

08 Outlook
on further activities

The NRA in Austria 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 in 2016. 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, the guiding principle also in the third reporting period, is to be maintained in the future. Specifically, the activities described below are planned for 2019/2020 or until the next report is prepared in June 2020.

Monitoring activities

1. **Transparency investigation.** Another investigation is planned in the coming reporting year to evaluate the transparency status in relation to transmissions (whether traffic is modified). If any corresponding evidence is identified, as in the past, requests for information and additional steps will be initiated where required.

Section 5 referred to the additional official instruments described below, which allow verification of conformity with the provisions of the TSM Regulation:

2. **Additional requests for information.** As presented in the timelines in section 4, the request-for-information procedures initiated for 16 other operators in February/March 2018 were completed by the TKK in the reporting period. Nine of these procedures were transferred to RTR due to a change in responsibility resulting from the amendment of the TKG. However, some eight to ten request-for-information procedures, which include mobile and fixed network providers, are planned for the upcoming reporting period.

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 are held and procedures launched in the event of any peculiarities, repeated complaints or similar developments.

4. **Ongoing review of general terms of business.** The fourth instrument relates to the powers under Art. 25 TKG 2003, according to which all general terms of business must be submitted to the regulatory authority and can also be contested by the TKK – where any provisions of Art. 4(1) of the 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 permitted in principle by the TSM Regulation; such issues include zero-rating within the data cap, development of the internet in general and proliferation of specialised services. This is the procedure already followed for existing zero-rating products.

5. **Information from ongoing market observation.** Under the KEV,[56] the regulatory authority periodically collects information on changes in internet access markets, implemented technologies and other items, and makes this available along with

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

analyses derived from that information (such as hedonic prices, the mobile price index and price baskets). 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, published in RTR's quarterly Internet Monitor and Telekom Monitor, can be downloaded as Open Data[57] by interested parties.

6. **Certified monitoring mechanism.** The regulatory authority has been offering the RTR-NetTest for several years now (www.netztest.at). This is used for evaluation purposes in conciliation procedures (as well as court proceedings) in order to ascertain whether the operator is or has been providing a deficient service. Since the TKG amendment in November 2018, the regulatory authority has been offering a performance monitoring mechanism for end users (Art. 17b TKG 2003), which is considered a certified monitoring mechanism within the meaning of Art. 4(4) of Regulation (EU) 2015/2120. A review is currently underway to determine whether any, and if so which, other steps will need to be taken under that provision.

International cooperation

The special significance of international cooperation in the context of net neutrality was highlighted in section 3. Collaboration at this level will continue in the coming reporting year (05/2019 to 04/2020) with the priority areas described below.[58]

1. The international exchange among regulatory authorities, aimed at a harmonious implementation of net neutrality provisions (within the framework of BEREC but also bilaterally), will continue in 2019/2020, for example through ongoing procedures 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 2019. The report will be based on the national reports on net neutrality to be released by 30 June 2019 and on the BEREC data survey to be carried out in June 2019.[59]

3. BEREC began to work on an update to the existing net neutrality guidelines at the beginning of 2019. The basis for this work is the BEREC Opinion on the evaluation of the net neutrality regulation, which was sent to the European Commission at the end of 2018 and used as input for the evaluation of the TSM Regulation by the European Commission. A stakeholder workshop regarding the update of the net neutrality

[57] See RTR's Open Data Portal, https://data.rtr.at

[58] The information provided in the following is primarily based on the BEREC Work Programme 2019: https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/8337-berec-work-programme-2019 and on the draft for the BEREC Work Programme 2020: https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/8365-outline-for-berec-work-programme-2020. The last version of the 2020 work programme, currently under preparation, should be finally adopted in late 2019. The 2019 Work Programme is currently being drafted and should be finally adopted in late 2019.

[59] BEREC Report on the implementation of Regulation (EU) 2015/2120 and BEREC Net Neutrality Guidelines.

guidelines was held at the end of May 2019. Additionally, the updated guidelines will be the subject of consultations in late 2019. The final, updated guidelines are set to be published in the spring of 2020.

4. Another focal area within BEREC's (and RTR's) international activities for 2019 concerns the development of a tool to check the quality of internet access services (in accordance with the objectives set forth in Art. 4 and Art. 5 TSM Regulation). The work on this tool was started in late 2018 and should be completed in late 2019. The tool will then be available to interested regulatory authorities so that they can implement it at national level and adapt it for their existing tools. 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 for various test metrics, which was published as a document.[60] 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,[61] which presents how these metrics can be implemented in the future tool while applying the Open Source and Open Data principles. RTR is contributing substantially to the work in this regard.

5. And finally, the work of other NRAs is being looked at and reviewed for its relevance for Austria, with action being taken where applicable. For instance, various NRAs have already published studies raising the issue of other factors that may have a negative effect on the openness of the internet. This is also relevant because such negative effects can ultimately jeopardise the objectives of the TSM Regulation (of maintaining the internet as an engine of innovation, for example). Examples in this context include, for instance, the study by the French NRA, ARCEP, on the influence of user devices on open access to the internet, or the study by the Dutch NRA (ACM, which is also the competition authority) published in April 2019, which looked at the influence of app stores on open access to the internet. These studies are along the same lines as the RTR study on the significance of app stores, user devices and operating systems for open access to the internet, which was just published a few weeks ago. It also focuses, among other things, on competition issues that are relevant to the demand side as well as those relevant to the supply side (CAP or application developers). Further questions regarding the effects of platforms on the open internet will be examined in the upcoming reporting year.

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

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

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 dominated by procedures and discussions on how to resolve certain practices deemed problematic from a net neutrality perspective. There were detailed discussions (beyond procedures) in particular on zero-rating issues and regarding individual aspects associated with network slicing. RTR expects that these two topics will also be at the top of the list of issues to be discussed in the upcoming reporting year, whereby the focus of the talks was last aimed at the application of the provisions of the TSM Regulation in concrete terms to new net and service developments.

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 open dialogue about any issues that might arise as well as new developments and concerns relating to net neutrality.

Information for the public and further considerations

To the extent such information can be made accessible to the public, the activities mentioned will be made available on the RTR website, or RTR plans – as has been done in the past – to refer via its website to other relevant proceedings, studies, and activities by institutions in the general field of net neutrality.[62]

[62] For details, follow these links: https://www.rtr.at/en/tk/Netzneutralitaet und https://www.rtr.at/en/tk/Internationales.

09 Appendix

9.1 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 08: 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 5
"main results and values retrieved from technical measurements and evaluations conducted in relation to supervising and enforcing the Regulation"	section 6.3
"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 5.7

9.2 Index of figures and tables

Figures

Figure 01:	Timeline of events in the reporting period	14
Figure 02:	Schematic diagram of website access	26
Figure 03:	Schematic diagram of a DNS block	26
Figure 04:	Schematic diagram of an IP block	27
Figure 05:	Fixed and mobile broadband connections	38
Figure 06:	Distribution of download speeds over reporting period	39
Figure 08:	Distribution of upload speeds over reporting period	41
Figure 09:	Upload speed by technology	42
Figure 10:	Latency (ping) by technology	43
Figure 11:	Download and upload speeds by time of day in 2017 and 2018	44
Figure 12:	Price baskets fixed vs. mobile broadband	45
Figure 13:	Quality of service test (RTR-NetTest)	46

Tables

Table 01:	Timeline of events in the reporting period	15
Table 02:	Summary of problematic practices in light of the TSM Regulation	17
Table 03:	Overview of categories of suspected NN breaches	32
Table 04:	Procedures in accordance with Art. 5(1) TSM Regulation pending in reporting period	34
Table 05:	A1 Go! and Xcite product portfolio – ranking of tariffs	53
Table 06:	Tariff plans with zero-rating available to A1 private customers – April 2019	54
Table 07:	Geographic distribution of streaming services by region and category	59
Table 08:	Sections of this report as mapped to the BEREC guidelines	66

9.3 Abbreviations

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
CAP	content and application provider
CDN	content delivery network
CERT	computer emergency response team
CPE	customer premises equipment
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
DPI	deep packet inspection
GDPR	General Data Protection Regulation
EC	European Commission
HTTP	Hypertext Transfer Protocol; protocol for transferring data to the application layer via a computer network (e.g. internet)
HTTPS	Hypertext Transfer Protocol Secure; communications protocol on the World Wide Web that allows data to be transferred securely
IANA	Internet Assigned Numbers Authority; a department of ICANN, responsible for assigning numbers and names on the internet
IAS	internet access service
ICANN	Internet Corporation for Assigned Names and Numbers; coordinates the allocation of unique names and addresses on the internet
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
M(V)NO	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
SNI	see TLS-SNI

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol; very simple (and early) file transfer protocol
TKG	Telecommunications Act
TKK	Telekom-Control-Kommission
TLS-SNI	Transport Layer Security – Server Name Indication; an extension of the transport layer security protocol that allows multiple encrypted, retrievable websites with different domains to share one server on TLS port 443, even if it has only one IP address
TSM Regulation	Telecoms Single Market Regulation; REGULATION (EU) 2015/2120 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)
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; web: www.rtr.at

Responsible for content

Mag. Johannes Gungl (Telecommunications and Postal Services Division)
Austrian Regulatory Authority for Broadcasting and Telecommunications

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 2019 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

Rundfunk und Telekom Regulierungs-GmbH

Mariahilfer Straße 77–79 | 1060 Wien | Österreich
T: +43 1 58058-0 | F: +43 1 58058-9191 | M: rtr@rtr.at
www.rtr.at