Body of European Regulators for Electronic Communications

BEREC

BoR (18) 170

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

4 October 2018

Contents

1 Summary and conclusions

Summary

This report gives an overview of the activities of the NRAs[1] in the course of implementing the net neutrality provisions of Regulation (EU) 2015/2120[2] and associated BEREC Net Neutrality Guidelines. This report reflects the second year of the application of the Regulation, covering the period from 1 May 2017 to 30 April 2018. BEREC has gathered information from 29 NRAs via an internal questionnaire. NRAs also published in national reports on the second year of application of the Regulation. To this information, descriptions of publicly known net neutrality cases or investigations have been added. These cases arose throughout the 12-month reporting period. However, this report does not constitute an exhaustive description of the current actions in the field of net neutrality.

The information in this report is organized according to the provisions of the Regulation. This report shows that NRAs have actively implemented the Regulation. It is evident that during the second year of the application of the Regulation, the adoption of monitoring methods has increased as compared to the first year. Moreover, quite a few NRAs have dealt with zero-rating cases and a handful of formal decisions was reached. More formal decisions are expected to follow during the remainder of 2018.

Concerning Article 3 of the Regulation regarding end-users' rights to open internet access, the analysis of complaints or end-user reports, information requests to ISPs and market surveys without requesting information from ISPs (e.g. checking ISPs' offers on their web pages) were the most mentioned activities among NRAs. All NRAs indicated they were monitoring the commercial and technical conditions related to the provision of internet access services, with the majority combining two or more sources of information among surveys, analyses of complaints, information requests to ISPs and technical network monitoring. Zero-rating offers were identified by almost all (27) NRAs, with music/video streaming and social networking the most frequently mentioned types of applications being zero-rated. Traffic management practices were assessed formally only by a small number of NRAs. According to the NRAs, monitoring activities are going on for investigating so-called "specialised services".

Concerning Article 4 on transparency and contractual terms, most of the NRAs usually applied multiple methods and most commonly more than two. The top three activities used by NRAs to assess the ISPs' compliance with Article 4 were 'formal and informal requests for information from the ISPs, 'market surveys without requesting information from ISPs, as well as the 'analysis of end-users' reports and complaints'. Half of the NRAs already set national specifications in relation to the different types of speed-related information required under Article 4 – maximum, normally available and minimum speed. Even though the Regulation has been in place for more than two years, in almost half of the countries ISPs have not yet included speed information in their contracts. A great majority of the NRAs monitor end-user complaints

[1] NRA is used in this report as reference to the National Regulatory Authority in the meaning of Article 5(1) of Regulation (EU) 2015/2120 as they have been designated by the national legislator. These do not fully correspond to the NRAs that are BEREC members and observers. See Question 1 below.

[2] This report refers as "the Regulation" to the net neutrality rules contained in 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.

about the performance of the internet access service. Two thirds of the NRAs (19 out of 29) offer an internet access service quality monitoring mechanism to consumers.

Concerning Article 5, the answers to the questionnaire indicated that a large majority of NRAs is monitoring the availability of high-speed internet access service, either by market surveillance without requesting ISPs, by requesting information from ISPs, by conducting internet access service speed measurements and/or by analysing complaints and end-user reporting.

Conclusions

This report shows a consistent treatment by NRAs of practices relating to the core principles of net neutrality, such as the ban on blocking of applications and discriminatory treatment of traffic.

The Regulation neither allows nor prohibits certain commercial practices *per se*. The zero-rating cases mentioned in this report illustrate that it is key to analyse the specifics details of the practice concerned and its circumstances. To this end, BEREC Net Neutrality Guidelines set out a number of criteria against which zero-rating needs to be assessed.

Striving for a coherent application of the Regulation, BEREC keeps facilitating the exchange of information and knowledge both at the level of Net Neutrality expert working group and in Plenary meetings during 2018. BEREC will continue this work in 2019.

Overall, BEREC concludes that the Regulation has been implemented by NRAs with adequate coherence. During the second year of the entry into force of the Regulation, a number of cases were decided upon by NRAs. At the time of writing of this report, also quite a number of cases are being analysed by NRAs. BEREC concludes that in analysing cases, NRAs coordinate and exchange information on ongoing cases. This is contributing to a coherent application of the Regulation.

BEREC notes that the evaluation of the Regulation (EU) 2015/2120 by the Commission will be conducted by 30 April 2019. Therefore, late 2018 BEREC will provide the Commission with an evaluation report on its experience with the application of the Regulation and the Guidelines. BEREC concludes so far that the Net Neutrality Guidelines are well suited to assist NRAs in performing their tasks of supervision and enforcement as set out in Article 5 of the Regulation. During the first and second year of implementing the Regulation, NRAs have gathered experience with net neutrality cases, which is used when preparing the evaluation report to the European Commission. At the same time, no cases have appeared in which the Net Neutrality Guidelines themselves were insufficient.

2 General questions

Question 1. Which types of activities has your NRA engaged in during 2017/18 in order to implement the Regulation (EU) 2015/2120? Please provide a brief account of:

- internal activities (e.g. preparing new internal procedures, dedicating teams / FTE, etc.)
- external activities (e.g. press-release, meetings with stakeholders or ISPs, drafting national guidelines on enforcement policy, stimulating self-assessment or internal compliance by ISPs, adopting administrative orders/decisions or imposing administrative fines etc.)
- any other actions of note:

24 NRAs reported/provided updated information on internal activities. Actions identified by member states included, amongst others:

- meetings with stakeholders (e.g. ISPs, vendors, consumer organizations);
- analysis of ISPs' implementation of the Regulation (e.g. reviewing the terms and conditions for internet access services and their online available information - at least with the biggest ISPs against the new obligations);
- (online) publication of information/recommendations/opinions for stakeholders and consumers;
- setting up/enlarging interdisciplinary teams whose members have technical, legal, policy and consumer affairs background;
- an update on the methodologies for measuring data parameters of networks by means of TCP protocol, on the methodology for measuring and evaluating data parameters of fixed electronic communication networks;
- update or development of measuring infrastructure for the purpose of checking and verifying selected parameters of data services of electronic communications provided to end-users in fixed and mobile networks (including certified measuring mechanism);
- enabling the comparison of data regarding availability and quality of high-speed internet from end-users in the mobile and fixed networks and consequently visualisation of the gained figures;
- technical and non-technical surveys and monitoring;
- identifying required changes regarding existing legislation and rules of procedure.

Concerning external activities, almost all (27) NRAs reported to have been involved in such activities. Examples of activities were: meetings with ISPs and/or stakeholders before and while implementing the Regulation, translation of the national NN report in English, supervision of specific cases from an Art 3(2) perspective, educational campaign to inform the public, publication of (draft) decisions, imposing of administrative fines due to non-compliance with the Regulation, initiating studies, providing press-releases, drafting a national regulation.

A majority of NRAs have performed assessments of ISPs general terms and of ISPs agreements on commercial and technical conditions to establish the presence or the absence of a possible violation of Article 3(2) of the Regulation. Many launched formal proceedings based upon the findings.

11 NRAs stated that they undertook other actions[3]:

- preparing an initiative to establish a framework related to the QoS of fixed and mobile broadband in order to set standards across the market on how QoS is measured and reported to the NRA for monitoring purposes (the framework will also ensure appropriate transparency measures for the benefit of the consumer and the market in general);
- preparing the annual NN report;
- launching an online end-user questionnaire regarding the satisfaction with the provisions of the internet access service;
- extending the diagnostic capacities (e.g. an online complaint handling mechanism)
- reflection on crowdsourced monitoring tools for end-users;
- development of studies in which the transparency of the internet traffic was investigated;
- preparation of a draft position on the implementation of Article 3 and Article 4 of the regulation, which was put for public consultation.

Approach	NRAs	Number
Internal activities (e.g. preparing new internal procedures, dedicating teams / FTE, etc.)	AT, BE, CY, CZ, DE, DK, EE, ES, FI, FR, HR, HU, IE, IT, LT, LU, MT, NL, NO, PL, PT, RO, SK, UK	**24**
External activities (e.g. press-release, meetings with stakeholders or ISPs, drafting national guidelines on enforcement policy, stimulating self-assessment or internal compliance by ISPs, adopting administrative orders/decisions or imposing administrative fines etc.)	AT, BE, BG, CZ, DE, DK, EE, EL, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, NO, PL, PT, RO, SE, SI, SK, UK	**27**
Any other actions of note	AT, BE, BG, FI, FR, IT, LT, MT, PT, SK, UK	**11**

Table 1. NRA activities during 2017/18 in order to implement the Regulation (EU) 2015/2120

3 Article 3(1) and 3(2)

Question 2. What approach have you taken to monitor the commercial and technical conditions related to the provision of internet access services:

- market survey without requesting information from ISPs (e.g. checking the relevant information on the ISP' s web pages, such as the general terms and conditions)
- information request from ISPs,
- analysis of complaints and end-user reporting
- technical network monitoring
- other, please specify: _____ .

Is there any change compared to the previous period? Y/N

[3] Note that these other actions partly overlap with *internal activities* and *external activities*.

Almost all NRAs used one or more of the above mentioned techniques to monitor the commercial and technical conditions related to the provision of internet access services. A majority of NRAs used a market survey (22), made information requests to ISPs (26) and performed an analysis of complaints and end-user reports (24). The market surveys and information requests typically involved examination of the terms and conditions and/or agreements under which ISPs provide internet access and the online available relevant information regarding the Regulation. A smaller number used technical network monitoring tools or said they were in the process of developing technical tools (8).

Examples for individual approaches by NRAs are: setting up a platform for end-users to report problematic situations with ISPs, maintaining a website focusing on information on the open internet, supervision concerning agreements between ISPs and end-users on technical conditions, ad-hoc checking of the relevant information on selected ISP's websites and informal contact with the ISP in case of possible violations, legal obligation of ISPs to notify their new or adapted terms and conditions, analysis of reports and complaints by vendors and ISPs, opening a formal assessment on the free choice of terminal equipment.

9 NRAs responded that there are changes compared to the previous reporting period (BG, IT, FR, LT, NL, NO, PT, SI, UK).

Approach	**NRAs**	**Number**
Market survey without requesting information from ISPs (e.g. checking ISP's offers on their web pages)	AT, BE, CY, CZ, DK, EE, ES, FI, FR, HR, HU, IE, IT, LT, LV, ML, NL, NO, PT, SE, SI, UK	**22**
Information request from ISPs	AT, BE, BG, CY, CZ, DE, DK, EE, EL, FI, FR, HR, IE, IT, LT, LU, LV, MT, NL, NO, PL, PT, RO, SK, SI, UK	**26**
Analysis of complaints and end-user reporting	AT, BE, BG, CY, CZ, DE, DK, EE, ES, FI, FR, HR, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SI, UK	**24**
Technical network monitoring	AT, BG, FR, HU, IE, LV, PT, SI	**8**

Table 2. Approach to monitor the commercial and technical conditions

Question 3. Pursuant to Article 3(1) have you completed any formal assessment of ISP restrictions on the use of technically compliant terminal equipment? Y/N

If yes, briefly describe the practice and the conclusions of the assessment (and enforcement action taken where applicable)?

The following NRAs stated that they have not completed any formal assessment of ISP restrictions on the use of technically compliant terminal equipment: AT, DE, EE, EL, ES, FI, HR, HU, IE, LT, LU, LV, MT, NL, NO, PL, PT, RO, SE, SI, UK (21).

BE, BG, CY, CZ, DK, IT, FR and SK (8 NRAs) conducted assessments, as shown below:

NRA	assessment
BE	BIPT is currently investigating whether an ISP is breaching the regulation by forcing its customers, subscribing to a fixed wireless 4G offer, to use a single 4G modem.
BG	Information was gathered with CRC`s Annual Questionnaire which was sent to all ISPs. CRC has not identified practices of restrictions on the use of technically compatible terminal equipment imposed by ISPs, which are not in line of Article 3(1) of the Regulation.
CZ	CTU reported 14 administrative proceedings related to linking the internet access service to the use of specific terminal equipment, which was not implied by a technical need. CTU identified 3 basic types of practices, which could lead to a limitation of the end-users´ right to use the terminal equipment of their own choice when using the internet access service. By certain ISPs operating nationwide, the conclusion of a contract on internet access service was automatically linked with getting terminal equipment offered by the respective ISP (usually by purchase) or such linkage could be (wrongly) deduced by a consumer due to unclear contract terms. Administrative proceedings were initiated in such cases and an obligation was imposed to change the (published draft) contracts on provision of internet access service, in order not to limit the free choice of terminal equipment. In case of ISPs operating at regional level, the use of terminal equipment, different from the one offered to a subscriber by the ISP, was subject to ISP´s prior approval. No conditions were stipulated for awarding such an approval and the awarding was left to the ISP´s subjective discretion completely. CTU therefore concluded that these situations could also lead to the limitation of the end-users´ right to use the terminal equipment of their own choice.
CY	According to the provisions of the Regulation (as interpreted in the Net Neutrality Guidelines BoR (16) 127), as adopted in national secondary legislation (Decree 72/2017) ISPs are required to report restrictions on the use of technically compliant terminal equipment. Following the collection of ISPs' reports, OCECPR's main finding was that ISPs impose an obligation to their subscribers to use the provided terminal equipment in order to be able to provide support and bundled services (telephony, internet, TV). Based on ISPs explanation, the provision of obligatory equipment by the ISPs is justified under the provisions of the Regulation and the Decree.
DK	As a result of last year's data collection, the DEA identified one ISP that offered unlimited data on the mobile phone but restricted tethering. The DEA issued an injunction ordering the ISP to remove this restriction. The ISP complied within the deadline set by the DEA.
IT	AGCOM organized several meetings with ISPs and Original Equipment Manufacturers (OEMs). AGCOM also launched a public consultation on the free choice of terminal equipment by end-users when using an internet access service. The public consultation aims at identifying possible measures which facilitate the free choice of terminal equipment (decision n. 35/18/CONS). After the

	consultation, AGCOM published a binding decision mandatory for all the operators (decision n. 348/18/CONS). The decision imposes that users must be free to use their own terminal equipment and confirm that the ubication of the NTP coincides with the physical termination point at the socket wall. Moreover, AGCOM issued a cease-and-desist order to end restrictions in the use of mobile terminals in tethering mode. Since users were required to pay an additional fee, AGCOM considered this practice in breach of Article 3(1) and 3(2) of the Regulation (decision n. 68/18/CONS).
FR	During the assessment of the terms and conditions on the mobile market, it was noticed that several ISPs imposed limitations on the free choice of terminal equipment when using an internet access service. These limitations include using tethering with a smartphone, using a SIM card in a modem/USB dongle/connection sharing device. All concerned ISPs have made sure to modify their offers by the end of Q3 2018. Until now, no formal decision was necessary after the assessment of the practices. On the fixed market, some ISPs prevent the possibility of using other equipment than their standard set-top box. This is still under investigation.
SK	According to the outcome of information requests of selected ISPs, none of the ISPs restricted the use of end-user own terminal equipment. However, in some cases, ISPs recommended the use of ISP's offered terminal equipment due to incompatibility avoidance within their networks.

Table 3. Assessments of ISP restrictions on the use of technically compliant terminal equipment

Question 4. What types of 0-rating services exist in your country?

- None
- Music streaming services
- Video streaming/IPTV services
- Social media services
- Voice and short messages
- Cloud services
- Email services
- Other_____

Is there any change compared to the previous period? Y/N

There were no zero-rating services identified by two NRAs (FI and SI), while one or more zero-rating services were reported by all other NRAs. Zero-rating of music streaming services, video streaming/IPTV services and social media services were the most often identified examples.

Among the diverse other zero-rating services were: GPS navigation services, audio books, e-book subscription service, radio channels, access to selected websites, Pokemon Go, the ISPs own apps and services, gaming, MyAccount-type of application, antiviruses, parental control

(via device), QoS measurement tools, news app, Whatsapp, TV app, access to e-papers, soccer contents, banking services etc.

Type of zero-rating service	NRAs	Number
Music streaming services	AT, CY, CZ, DE, DK, EE, EL, ES, HR, HU, IT, LT, LU, NL, NO, PL, PT, RO, SE, SK, UK	**21**
Video streaming/IPTV services	AT, BE, BG, CZ, DE, EE, EL, ES, FR, HR, HU, IE, IT, LT, LU, MT, PL, PT, RO, SK, UK	**21**
Social media services	BE, BG, CY, CZ, DE, DK, EL, ES, HR, HU, IE, IT, LT, LU, LV, PL, PT, RO, SE, UK	**20**
Voice and short messages	BE, BG, CZ, DE, DK, EL, ES, HU, IT, LT, LU, LV, PL, PT, RO, SE, UK	**17**
Cloud services	AT, EL, IT, PL, PT, RO	**6**
E-mail services	CZ, IT, PL, PT, RO	**5**
Other	AT, BE, CZ, FR, HU, IT, LT, LV, MT, PL, PT, RO, SE	**13**

Table 4. Type of zero-rating services

Question 5. Pursuant to Article 3(2) have you performed any formal assessments of agreements on commercial and technical conditions as well as commercial practices such as zero-rating or traffic price discrimination practices? Y/N

If yes, briefly describe the practice and the conclusions of the assessment (and enforcement action taken where applicable)

NRAs from 15 countries (BE, CY, CZ, DE, EE, FR, HR, HU, LU, MT, NL, NO, PT, RO, SE) said they had undertaken one or more assessments of zero-rating practices, while 13 NRAs (AT, BG, DK, EL, ES, FI, IE, IT, LV, PL, SI, SK, UK) responded that no formal assessment was performed. It should be noted that although most of the cases listed below are categorized as zero-rating cases, the real issue that arises from some of them is actually related to other commercial or technical conditions that may infringe the regulation.

Zero-rating cases and other commercial or technical practices

The following case descriptions serve as examples involving these practices as they were analysed and reported by NRAs.

AT: Charging consumers for the provision of a public IP addresses

A1 charges consumers to provide a public IP address: an additional package "A1 mobile dynamic IP" has to be purchased. The end-users' right to distribute information and content and to provide applications and services is limited by this practice because the ISP charges the customers in order to provide them a public IP address (Article 3(1) and Article 3(2) of the Regulation). The Austrian NRA has ordered the ISP to provide a public IP address free of charge to the end-user on request, to be implemented within 8 weeks after the decision.

Already paid fees (since 30 April 2016) had to be refunded. The decision was made in December 2017.

BE: BIPT assessment of Proximus zero-rating offer

On the 25th of April 2018, the BIPT issued an advice regarding the evaluation of the My Space Apps pilot project by Proximus. On 24 March 2017 Proximus launched a “pilot project” regarding sponsored mobile data. A number of selected Proximus customers whose smartphones function by means of an Android operating system received a text message by Proximus inviting them to install a Proximus app, the “My Apps Space”. That app allows the Proximus user to activate apps from participating companies that (initially) are not charged to their allowance for mobile data use, as the participating company pays the data use on its app “instead of the user”. The “My Apps Space” app was launched on 24 March 2017. The “pilot project” was stopped on 21 November 2017 by Proximus own initiative. Based on the figures and facts it was not possible to say that the sponsoring was of such a level that it could be stated that it had such an impact that it would result in a material reduction of choice for the end-users. No rights nor final conclusions can be drawn from this opinion, as the actual product was never fully launched and as such, this advice constitutes a hypothetical assessment. It was drawn up, in order to respond to an explicit request from a parliamentary Commission to finalize the evaluation of the pilot project even though it was stopped in the meantime.

Besides that, BIPT also discussed the intended zero-rating of a customer care app of an ISP, even after the data cap had been reached. It had no problem with this practice in relation to the reload function of the app (see para. 35 of the Net Neutrality Guidelines), but expressed serious concerns on this practice with regards to other functionalities of the app, such as using the customer loyalty points for retail purchases after the data cap has been reached.

CY: OCECPR assessment of zero-rating

According to the provisions of the Regulation (as interpreted in the Net Neutrality Guidelines) ISPs reported to OCECPR on their agreements on commercial and technical conditions and commercial practices. Following assessment of the reports, OCECPR’s main findings were that there are potentially two zero-rating practices offered by a single ISP. OCECPR proceeded with a further investigation of this matter and it was concluded that zero-rated applications are used from a minimal percentage of subscribers (0.01% and 0.1% respectively of the total number of single ISP’s subscribers). Based on this fact OCECPR considered that there is no immediate impact on user rights and decided to currently limit itself to monitoring the situation.

CZ: CTU two zero-rating cases

CTU launched administrative proceedings with two ISPs. The first case concerned zero-rating applied to one of the so-called social media services. In this case the commercial practice was adjusted immediately after the initiation of proceedings and therefore, the proceeding was closed. At present, this ISP offers special data bundles which can be used for (various) social media services and messaging services only. These are offered for free as a bonus to certain types of data bundles of general use. Data consumption from the special bundles is possible on condition that a subscriber has not used up the data volume from the bundle of general use.

Regarding the second case the data consumed for the use of a music streaming service did not count to the agreed data limit. The music service to which zero-rating was related could be used after using up the data limit, i.e. when all the other applications, services and content available through the internet were blocked. CTU assessed this practice as a breach of Article

3(3), first and third paragraph, of the Regulation (treating the data traffic unequally) and with regard to the fact that after using up the data limit the internet access of the users was limited to the only music service, this was assessed as a breach of 3(3), first and third subparagraph as well. In its decision, CTU imposed on the ISP the obligation to put the commercial practice into compliance with the Regulation.

DE: BNetzA decision on Telekom zero-rating service “StreamOn”

During the reporting period, BNetzA investigated Deutsche Telekom’s zero-rating offer “StreamOn”. In its Statement of Objections, pursuant to section 126 (1) of the German Telecommunications Act, BNetzA considered certain provisions of Deutsche Telekom’s general terms and conditions for content partner not in line with Article 3(2). These general terms and conditions did not allow for the participation of private content providers or for those providers of content that offer a download function in addition to streaming. In practice, however, Deutsche Telekom had already been handling the acceptance of such content providers other than stated in the wording). Upon this intervention by BNetzA, Deutsche Telekom submitted an amended version of the general terms and conditions for content partners in the proceeding and formally declared that these would enter into force on 1 March 2018. Accordingly, from now on, private persons and streaming suppliers that also provide a download function can participate in “StreamOn” as partners. Following these amendments, the requirements of the BNetzA for open and non-discriminatory participation in “StreamOn” have been met. With regard to the traffic management aspects of the case, reference is made to Q7 (under Article 3(3)).

Moreover, a content and application provider (CAP) of third party audio and video streaming content, that uses the bit torrent protocol for distributing the content, complained of not being allowed to participate in the Deutsche Telekom’s zero-rating offer “StreamOn”. After Deutsche Telekom declined the CAP’s request for participation, the CAP added a streaming client on his website to adapt to the Deutsche Telekom’s general terms and conditions for content partner. The assessment was not terminated during the reporting period.

DE: BNetzA investigation of “Vodafone Pass”

During the reporting period, BNetzA investigated Vodafone’s zero-rating offer “Vodafone Pass”. In its Statement of Objections of November 13, 2017, BNetzA determined, pursuant to section 126 (1) of the German Telecommunications Act, that the reservation to throttle video streaming traffic is a limitation of end-user rights according to Article 3(2) in conjunction with Article 3(1) and violates the net neutrality rules. BNetzA also sent questions to Vodafone as well as other stakeholders (including ISPs, TV stations, video and music streaming providers, cartel office, media authorities, consumer association, representatives of civil society). The proceedings were not formally terminated during the reporting period.

EE: ETRA assessment of Telia zero-rating

Telia introduced a zero-rating service in Estonia in the beginning of July 2017. The offer gives the users zero-rated access to their OTT service minu.tv and some other similar applications. ETRA found that the zero-rating proposition did not breach the Regulation because when the end-user has reached their data cap, all applications are blocked including zero-rated services and the offer only applies for bigger data caps.

FR: ARCEP assessment of zero-rating

An assessment of the zero-rating offers of two ISPs is underway. Some of the concerned ISPs have announced an evolution of their offers.

HR: HAKOM assessment of Vipnet and Hrvatski Telekom zero-rating

HAKOM investigated Vipnet's zero-rated VIP NOW streaming offer and found out that mentioned offer was not in line with the Regulation because the service can be freely accessed after the end-user has reached the data cap, while all other internet traffic is charged. After receiving a warning, VIP adjusted its offer to comply with the Regulation.

Furthermore, HAKOM also initiated a review on the tariff option "StreamOn" of Hrvatski Telekom which is a zero-rating offer. The bandwidth for video streams is throttled to a maximum of 2 Mbit/s (max. resolution of 480p) representing unequal treatment of data traffic and as such is currently assessed under Article 3(3) of the Regulation. Hrvatski Telekom upon HAKOM request will change it until end of September this year so the offer will be in line with the Regulation.

HU: NMHH assessment of zero-rating

In the reporting period, NMHH initiated an investigation whether the ISP's new types of zero-rated offers comply with net neutrality rules (Article 3(3) and Article 3(2) of the Regulation) and national rules on electronic communications. Investigations are still ongoing and no decisions has been made by NMHH.

In case of zero-rated offers launched before the reporting period, NMHH concluded that the ISPs in question market the option of using certain content and applications at no cost for the data transferred. The offers investigated included commercial practices as well as some traffic management measures. NMHH has found that these traffic management measures violated Article 3(3) of the Regulation. NMHH prohibited such unlawful behaviour and ordered the ISPs to discontinue the discrimination between various types of content. Two of the relevant NMHH's cases related to zero-rated access to social media websites and messaging applications and to music streaming are still in trial phase. In the third case (where online video streaming service was being zero-rated) the national court confirmed the NMHH's former decision.

IT: AGCOM assessment of zero-rating

During the reporting period, AGCOM has acquired information from the main ISPs of both landline and mobile networks (including the main virtual mobile operators) also by sending specific requests for information on the terms and conditions of the contract and technical and economic terms. In addition, hearings were held with stakeholders, also with a view to obtaining further clarifications on potentially critical aspects and issues. During the reporting period, all MNOs traded zero-rating offers that included the provision of music streaming services, streaming video / IPTV, social media, voice and SMS, e-books, e-reading, cloud storage solutions and other content (for example football games).

Following the delayed compliance by WindTre in relation to the correct application of the Regulation for one of the offers subject to the notice, AGCOM initiated a sanction procedure, closed with an immediate discharge fine of Euro 20,258 (the sanctioning procedure was launched before the introduction of the new sanctions system for violations of the rules on net neutrality).

In some cases, thanks to the discussion with operators and clarification of the existing legislation, the operators have modified otherwise potentially critical commercial practicesto the provisions of the Regulation thus avoiding further measures by AGCOM.

LU: ILR actions on zero-rating

The following assessments were undertaken: informal requests, internal quantitative and qualitative analysis.

MT: MT assessment of zero-rating

On studying a specific case, the MCA concluded that while the zero-rating offer is in place, its implementation does not infringe the regulation by means described in BEREC's Guideline 41. On further detailed analysis, the MCA noted that the number of mobile broadband subscribers to whom this offer is available is restricted since only IPTV customers of the same ISP are eligible. Given the subscriber base of both IPTV providers and broadband ISPs, the MCA concluded that the impact this offer may have on the market is limited. Therefore, while continuing to monitor the development of this offer the MCA concluded that its intervention at this stage would be premature.

NL: ACM assessment of T-Mobile zero-rating

T-Mobile was allowed to offer a zero-rating music streaming service, because the zero-rating was open for all music streaming apps and not just one. Therefore, the zero-rating offer is non-discriminatory and does not limit end-user’s rights. ACM expects an appeal to the decision by a digital rights organization, called “Bits of Freedom”. The administrative appeals court is expected to hear the case in autumn of 2018.

NO: Nkom assessment of Telenor and Telia zero-rating

Nkom has performed two regulatory assessments of commercial practices (zero-rating). Both of which regarding music streaming services, from two different ISPs. First, in the Telenor case, Nkom expressed an expectation that Telenor arranged that additional content providers could be included in the zero-rating offer (which Telenor did).

Second, in the Telia case, Nkom had critical comments to several factors considered in the regulator assessment based on para. 46 in the Net Neutrality Guidelines. However, the overall assessments concluded that the services were compliant with the regulation for the time being.

Critical comments in Nkom's assessments are in particular the following: Zero-rating schemes are offered by ISPs with considerable influence in the mobile internet access market. The CAPs included in the zero-rating schemes are, in practice, relatively limited, and cover only larger well-known providers. Zero-rating limits the end-users’ choice, in particular because of the relatively small data caps in proportion to the price, that are offered compared with other countries. The scale of zero-rating practices is increasing in the national market.

Finally, Nkom expressed that if zero-rating practices in the market don’t function satisfactorily, especially if the scale increases significantly, it is likely that Nkom would have to reassess its analysis.

PT: ANACOM draft decision on zero-rating and similar commercial practices

On 23 February 2018, ANACOM has approved a draft decision on zero-rating and similar commercial practices in Portugal. The draft decision was submitted to the prior hearing of

stakeholders, under the Administrative Procedure Code, as well as to the general consultation procedure provided in Article 8 of the Electronic Communications Law.

ANACOM has detected some incompatibilities with net neutrality rules for some zero-rating and similar commercial practices, as the traffic is not always treated equally when providing internet access service. This situation happens with some zero-rating offers where, in specific situations, all the applications are blocked (or slowed down) once the data cap is reached except for the zero-rating applications. It was also identified that the terms of use of some zero-rating and other similar offers are restricted to the national territory, in contradiction with the Roaming Regulation. Therefore, in the draft decision, ANACOM ordered the ISPs to amend the zero-rating and similar offers in accordance to the net neutrality and roaming rules. On that basis, it was requested information from ISPs about the following: the way they intend to correct their commercial offers; the adjustment on the information available about the commercial conditions of those offers (including agreements on commercial conditions); the specification of the conditions that must be verified to include other applications or content providers in zero-rating and similar offers.

Since, in general, data allowances are considerably smaller than those considered in zero-rating and similar offers, ANACOM also recommended the increase of the data cap for general internet access in order to be closer to the data caps applied for zero-rated applications.

ANACOM is currently analysing the responses to the public consultation and working on the consultation report, in order to communicate a final decision about the zero-rating and similar commercial practices in Portugal.

RO: ANCOM assessment of two zero-rating offers

One ISP offers zero-rated access to different categories of applications. Each zero-rating scheme is open for free entry for every content and application provider (CAP) providing a specific type of application (e.g. social, chat, video-streaming, audio-streaming, maps, email, cloud-storage-services) subject to a contractual agreement between a CAP and an ISP. The CAP is required to provide some information (e.g. IP) in order for the ISP to identify the specific traffic without analysing the content. The investigation has not yet come to a final conclusion but, from preliminary information received, no discrimination of traffic is involved. All traffic is treated equally and all traffic from the applications included in zero-rated categories is zero-rated both nationally and when roaming in EEA (subject to a regulated fair-usage policy) and both via mobile device and when tethering.

Subject to a new contract or a renewal (for a 12/24-month period), another ISP is offering its customers a bonus consisting of unlimited access to (all) internet, for speeds up to 1.5 Mbps for video streaming and up to 150 Mbps for any other type of content. According to information received, the throttling of video traffic is made permanently by the ISP in order to avoid possible network congestions. The bonus can easily be turned on and off (in which case a normal data-capped plan is used) by the consumer. ANCOM has found this practice to be a breach of the Regulation and has notified the ISP about it. Before taking any other legal action, the ISP has 15 working days to answer to the notification.

SE: PTS assessment of (i) two cases concerning agreements on technical conditions and (ii) one zero-rating case pursuant to Article 3(2)

PTS conducted supervisions concerning agreements between ISPs and end-users on technical conditions. The supervision of Tre concerned one clause of the end-user agreement

which stated that Tre charges an extra fee in order to enable its end-users to use e-mail and surf on internet on a BlackBerry-mobile. Tre explained to PTS that the clause in question concerned an additional service and that the end-users had access to internet irrespective of use of the additional service. PTS therefore closed that case.

PTS has also conducted a supervision concerning a clause in Telenor's agreements concerning pre-paid customers. Telenor explained that the condition wasn't relevant and removed the clause in question from the agreement. Therefore PTS closed the case.

PTS has initiated a supervision against Telia and the commercial practice zero-rating in Telia's offer "Sociala". The assessment is still ongoing.

UK: OFCOM initial review of three zero-rating offers

During the 2017-18 reporting period, OFCOM completed an initial review of three new zero-rating offers. In July 2017, Three launched a service called Go Binge, which zero-rates certain music and video streaming applications. In September 2017, Vodafone launched a new mobile offering, called Vodafone VOXI, aimed at people aged 25 and younger, which zero-rated selected social media and messaging applications. Later, Vodafone added optional selected video and music applications to the VOXI zero-rated offer. In November 2017, Vodafone launched Vodafone Passes, a series of five 'add-ons' which zero-rate data for selected applications in four different categories: Chat, Social, Music and Video. The fifth add-on is the Combo Pass which includes all four categories.

OFCOM concluded that the Three GoBinge zero-rated offer did not raise sufficient competition-related issues at the time it was reviewed to warrant opening a formal assessment. OFCOM opened a formal assessment of the Vodafone Passes and VOXI products, but this related to the traffic management practices employed alongside the zero-rating rather than the zero-rating of content *per se*. Vodafone only enables standard definition video to be available in conjunction with these zero-rated products, even where the original content is made available by the content provider in higher definition formats.

4 Article 3(3)

Question 6. If you started any monitoring of traffic management practices by ISPs what approach have you taken?

- market survey without requesting information from ISPs,
- information request from ISPs,
- analysis of complaints and end-user reporting,
- technical monitoring,
- other, please specify: _____

Is there any change compared to the previous period? Y/N

NRAs often used more than one of these techniques to monitor traffic management practices. 8 NRAs undertook a market survey without requesting information from ISPs. 25 NRAs reported that they had made information requests to ISPs while 18 had analysed complaints and end-user reports. Technical monitoring is up and running in 8 countries.

Other solutions included:

- the launch of a platform, where end-users can report problematic situations with ISPs,
- meetings with ISPs,
- reviewing publicly available information from ISP websites.

AT, CZ, FR, LU, MT, NL, PT, SE, SI (9 NRAs) stated that there is a change compared to the previous reporting period.

Approach	Countries	Number
Market survey without requesting information from ISPs	AT, BE, CZ, FR, HU, IT, MT, NL	**8**
Information request from ISPs	AT, BE, BG, CY, CZ, DK, EE, EL, ES, FI, FR, HR, IE, IT, LT, LU, LV, MT, NL, NO, PL, PT, SE, SK, UK	**25**
Analysis of complaints and end-user reporting	AT, BE, BG, CY, CZ, DE, DK, EE, FI, FR, IE, LT, LV, MT, PL, RO, SI, UK	**18**
Technical network monitoring	AT, FR, HR, HU, IE, LV, PT, SI	**8**
Other	IT, FR, UK	**3**

Table 5. Approaches of NRAs regarding monitoring of traffic management practices by ISPs

Question 7.

Pursuant to Article 3(3) 1 to 3(3) 3; have you completed any formal assessments of an ISP's traffic management practices? Y/N

If yes, briefly describe the practice and main conclusions of the assessment (and enforcement action taken where applicable).

Eleven NRAs (AT, BG, CY, CZ, DE, FR, HR, LT, MT, RO, SV) pointed out that they had completed formal assessments of traffic management practices.

CZ: CTU assessment of traffic management

CTU ran 4 administrative proceedings regarding the breach of Article 3 (3), first and third paragraph of the Regulation. In most cases (namely in 3 cases) the data rate was automatically lowered only for some types of applications, services and content when the agreed data limit was exceeded. For other types of data transmission (e.g. browsing websites run at http protocol or using e-mail) the data download and upload speeds remained unchanged.

The Czech Telecommunications Office assessed these practices as unequal data traffic management which is forbidden and therefore imposed the obligation for the ISPs to change the contract terms. The last of the administrative proceedings was related to a zero-rating practice. This practice enabled the use of one music streaming service even after the user´s data limit was exhausted and the internet access service was interrupted (which means all the other applications, services and content available through the internet access different from the only one to which zero-rating was applied, were blocked). Also, in this case ISP was imposed the obligation to bring the contract terms into compliance with the Regulation. CTU

also dealt with measures regarding the data traffic management in other two zero-rating offers of music and video streaming services in the Czech market.

In both situations the ISP reserved in the contract terms the right to implement data traffic management measures (or to introduce them in the future) consisting of lowering the quality of video covered by zero-rating or the data transmission rate. These measures were not supposed to be implemented for the data transmissions which were counted to the user´s data limit. In view of the fact that no measure was put into practice according to CTU´s findings, no administrative proceedings were launched. After meetings with CTU the ISPs made changes into the contract terms upon which the provisions regarding the data traffic management were removed.

MT: MCA assessment of traffic management practices

MCA has requested detailed information on various elements related to the Net Neutrality regulation from the ISPs using a self-assessment questionnaire, which was based on the BEREC questionnaire. MCA notes that there were no instances reported where ISPs were applying traffic management in violation of the Regulation. There was one instance where an ISP reported the use of DPI to identify specific traffic for charging purposes in conjunction with zero-rated applications. However, upon request for further clarifications the ISP stated that information was extracted from IP headers. Final assessments of these statements are still in progress at the time of writing.

SK: Teleoff information requests for traffic management practices

ISPs in Slovakia used the traffic management practices such as differentiation of traffic management based on different access types, modification of content or traffic, blocking or throttling of specific user categories, specific content or application types, specific content providers, websites, or some port or protocol. According to the outcome of information request of selected ISPs:

- practices dictated by European or national legislation (exception a) were used by 78% of ISPs,
- practices linked to the integrity and security of the network (exception b) were used by 56% of ISPs and
- practices linked to the prevention of exceptional or temporary network congestion (exception c) were used by 33% of ISPs.

FR: ARCEP investigation of traffic management practices

ARCEP’s services have detected several traffic management practices that are in the scope of the Regulation, both through the assessment of the terms and conditions of ISPs’ offers, as well as through the circulation of a specific questionnaire. Last year ARCEP had addressed practices that were blocking specific services (peer-to-peer, newsgroups, tethering – see question 3) and that might not be deemed compliant with the Regulation (not fitting the criteria for exceptional traffic management). The targeted practices have ceased. During the past year, ARCEP specifically assessed the traffic management practices of one ISP because its customers reported (in large numbers) a deterioration of QoS regarding particular online services. The investigation concluded that there was no apparent discriminative traffic management policy. However, the problem was more likely located at the interconnection level: the interconnection between the concerned ISP and its international carrier was thoroughly assessed. Before a formal decision from ARCEP’s board could be reached,

negotiations between the concerned ISP and online services were reported, which could lead to a resolution of the QoS problems encountered by the customers. ARCEP is currently still monitoring the case.

HR: HAKOM assessment of traffic management practices

To monitor ISPs' traffic management practices and ensure compliance with the Regulation, HAKOM conducted a traffic management (TM) survey requesting information from Croatian ISPs about existing TM practices (e.g. QoS mechanism used in the network, number of traffic classes and implemented rules of prioritization, aggregation factors used, rules for upgrading their network elements). At present HAKOM is still analysing the gathered information, but high-level analysis of received responses showed that TM measures are only applied by the ISPs as a preservation of integrity and security and as a congestion management measures. ISPs specify in terms and conditions, which are published on their website and constitute the part of an end-user contract, in a clear and comprehensive way the impact of traffic management measures, description on how the measures might affect the end-user experience in general and with regard to specific applications and any measures applied when managing traffic which uses personal data.

Formal assessment regarding possible violations of Article 3(3) has also been conducted (technical discrimination of traffic in the context of zero-rated video service). Proceedings are closed as ISPs ensured compliance with the Regulation after discussions with the NRA without the need to take any formal decision. In order to verify that ISPs' TM policies are effectively implemented as described in their Terms and Conditions, HAKOM is also using HAKOMetar Plus (mobile crowd-sourcing application) measurement results. HAKOMetar Plus besides measuring speeds also provides some network service tests ("TCP-ports" and "UDP-ports" test for detection of blocking of specific ports, traceroute test and VoIP test for possible delaying or throttling of traffic, etc.). HAKOM has not yet received complaints with regard to TM practices.

Formal assessments have been conducted in Austria. The practice included a specific form of "traffic shaping" of zero-rated services. The ISP (A1) offered zero-rated audio & video streaming as an add-product only in connection with shaping of the available bandwidth for these zero-rated services. So zero-rated content could only be consumed at a speed of 1.7 (SD content) or 3 (HD content) Mbit/s, irrespective of the factual connection speed available. This resulted in a reduction of content-related traffic for the ISP and in quality cutbacks for the end-user. The practice has been assessed as constituting a violation of Article 3(1) and 3(3) and the ISP has been ordered to stop the practice.

BNetzA formally concluded one investigation concerning traffic management practices during the reporting period. In addition, they have few ongoing cases in which BNetzA assesses traffic management measures in Germany. In a few other cases, they did not find any infringement of Article 3(3) of the Regulation.

DE: BNetzA decision on Telekom "StreamOn" video throttling

During the reporting period, BNetzA investigated Deutsche Telekom's "StreamOn" zero-rating offer and in particular took action with regard to the throttling of video. On December 15 2017 BNetzA has prohibited the "throttling of video" in the MagentaMobil tariffs "L", "L Plus", "L Premium" and "L Plus Premium", as this breaches the obligation of equal treatment of all data traffic. Under "StreamOn" the data transmission rate for video streaming in the MagentaMobil "L" tariff is slowed down to such an extent that videos can only be received in SD quality.

According to the BNetzA's findings, there is no objective technical reason for such slowing down of the data transmission rate, as video services do not need restricting. Conversely, according to the applicable regulations, the performance of an individual network does not provide grounds for restricting the data transmission rate for data-intensive communications.
On January 12 2018, Telekom filed an objection against BNetzA's decision of December 15 2017. On January 30 2018, Telekom filed an application for interim relief (i.e. requesting suspension of the immediate enforcement of the decision). The interim proceedings are still pending. Prior to its decision, BNetzA had determined in a Statement of Objections in the beginning of October 2017 that, pursuant to section 126(1) of the German Telecommunications Act, Telekom Deutschland GmbH had infringed the roaming and net neutrality requirements, and probed Telekom for comments and remedial action.

DE: BNetzA assessment of blocking inbound traffic

In another case a mobile ISP blocked by default all unknown incoming connection requests in its network. However, such inbound traffic is possible when the mobile end-user has first initiated a connection to the IP address of the foreign network. The ISP proposed a remedy for end-users, which want to avoid the blocking of incoming connections, to use a VPN solution. Customers with an IPv4 address could also replace the standard configured APN in their mobile device by an alternative APN that provides an "open" IPv4-connection. Connections using the IPv6 protocol are not supported by the proposed remedy. The affected ISP justified this blocking in particular with the aim of avoiding network outages since the location management system cannot handle an abnormal high number of requests (e.g. pinging of IP ranges), i.e. to preserve the integrity and security of the network. The ISP also argued that blocking incoming connections is protecting its mobile customers from attacks and "bill shocks". The case is not yet formally terminated.

DE: BNetzA assessment of other traffic management measures

In several other cases, BNetzA found no infringement of Article 3(3), either because the traffic management measure was justified or because no traffic management measure was detected. These cases included port blocking (cf. also Q8) or the blocking of a website by an ISP upon a court order. Moreover, several complaints concerned the alleged throttling of YouTube services but BNetzA did not find evidence of such throttling.

AT: NRAs decisions

In Austria two traffic management practices have been assessed. The Austrian NRA has reached a formal decision in these cases, which have been published. The Austrian NRA found that the traffic management practices violated Article 3(3) of the Regulation.

Throttling of video content

A1 Telekom Austria AG (A1) has launched a zero-rating service, called "Free Stream". This service includes zero-rating access to certain music and video platforms, which can be added to certain mobile plans. The option could be added free of charge. The program is open for all interested content providers which use adaptive bitrate technology. A1 may continue to offer Free Stream. The product does not directly breach Regulation. However, A1 also throttled zero-rated music and video content to 1.7 Mbit/s for SD content and 3.0 Mbit/s for HD content. After investigation by the Austrian NRA, the music and video throttling was found to be in breach of Article 3(3), third paragraph of the Regulation. The Austrian NRA ordered A1 to stop the practice within 8 weeks. The decision was made in December 2017.

Disconnecting users

A1 disconnects users every 24 hours. The end-users' right to distribute information and content and to provide applications and services is limited by this practice and A1 also discriminates traffic provided by the end user (Article 3(1), Article 3(2) and Article 3(3) of the Regulation). The Austrian NRA has ordered A1 to stop the disconnection every 24 hours and extend the timespan between disconnections to at least 31 days, to be implemented within the following 6 months after the decision. The decision was made in December 2017.

BG: CRC assessment of traffic management practices

In Bulgaria traffic management practices applied from the ISPs include:

- prioritization for the traffic for network management and control over the rest of the traffic;
- optimization for specific content, applications or services, or a combination thereof, where the optimization is necessary in order to meet the requirements of services for a specific level of quality;
- blocking specific ports and/or websites.

CRC's analysis of the collected information showed that the described traffic management practices seem in line with the Regulation.

FI: FICORA traffic management survey

While FICORA did not undertake any formal assessments, they conducted a traffic management survey, requesting information from Finnish ISPs. One of the main conclusions was that many ISPs were blocking communication ports and justifying their activities with the security exception.

CY: OCECPR assessment of traffic management practices

ISPs in Cyprus were asked to report to OCECPR on traffic management practices. Following assessment of the reports, their main findings were that some ISPs used traffic management practices (mainly cases where ISPs limited the access rate of heavy users based on their traffic volume in order to prevent congestion of the network), which may constitute infringement of the provisions of the Regulation. OCECPR informed the concerned ISPs that their practices may constitute an infringement and requested further action in order to ensure compliance with the provisions of the Regulation and Decree 72/2017.

Question 8. Did you conduct any research or survey on port blocking practices by ISPs? Y/N

If yes, please briefly describe significant findings.

Fifteen NRAs (AT, BE, BG, DE, FI, FR, HR, LT, LV, MT, NL, PL, RO, SI, SK) surveyed port blocking practices by ISPs.

NRAs have reported that ISPs claim to perform port blocking for security reasons and to prevent spam. Therefore, ports such as 23, 25, 53, 135 and 445 are sometimes blocked by some ISPs.

LT: RRT investigation on port blocking

RRT has investigated an end-user complaint that an ISP is blocking port 25. Therefore, the Lithuanian end-user could not use the SMTP server on his device to send e-mails. The device of end-user's choice could only send e-mails via port 25, and this setting was not customizable. The ISP claimed that blocking port 25 is necessary to preserve the integrity and security of the

network. RRT concluded that blocking port 25 permanently infringes on end-user's right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice as stated in Article 3(1) of the Regulation. The ISP did not provide sufficient evidence that unblocking port 25 would compromise security of its network, thus granting the exception for port blocking traffic management practice as stated in Article 3(3), third paragraph, sub b, of the Regulation. RRT ordered the ISP to unblock port 25.

SI: AKOS information requests for traffic management practices

AKOS conducted a survey on port blocking practices by ISPs in Slovenia based on ENISA'S questionnaire. The purpose of the questionnaire was to determine how ISPs' security measures influence the Net Neutrality regulation (whether ISPs block certain ports in order to preserve the integrity and security of the network to mitigate security risk). Based on the responses, ISPs have implemented different security measures, which also includes (permanent) blocking of certain most commonly exploited TCP/UDP ports (e.g. 19, 53, 135-139, 445, 593). The majority of the measures target specific customers/users. Some target larger groups of customers. Unsolicited inbound traffic is blocked by default for mobile users. The security measures differ from one ISP to another according to risk assessment.

LV: claims from ISPs about port blocking

Some ISPs in Latvia have claimed they block specific ports for the end-user safety. They have also stated that ports can be unblocked on end-user demand.

MT: ISPs engage in port blocking

Based on the response received to the aforementioned questionnaire, it was evident that some ISPs in Malta apply port blocking to specific ports, either to prevent the distribution of spam or to protect against security threats. These practices are both in line with the Regulation.

BE: BIPT questions to ISPs about port blocking

BIPT transmitted an ENISA-based questionnaire containing some questions on port blocking to Belgian ISPs, serving a large portion of Belgian internet consumers. The treatment, analysis and transmission of the responses will be done in the period covered by the next implementation and supervision report.

IE: COMREG technical monitoring of port blocking

Technical monitoring has suggested that port blocking is practiced on certain networks in Ireland. If COMREG ever get any enforcement powers, they will investigate these formally.

RO: ANCOM questionnaire on port blocking

ANCOM has participated in a research conducted by ENISA. In this regard, in 2018 they sent a questionnaire to IPSs about the security related exceptions included in the Regulation. The objective of this questionnaire is to collect information about the security measures taken under the exception b) set out in Article 3(3), third paragraph of the Regulation. The information collected through this questionnaire will be used by ENISA for the development of a document that gives a general aggregated overview of how these exceptions are being used, what are the good practices in this area, challenges, etc. When centralizing the answers provided by ISPs, ANCOM found, among others, that typically, ISPs try to prevent security issues related to: malware/viruses propagation, denial of service, phishing, spam; the most commonly security measures applied by ISPs are: port filtering, IP filtering, URL filtering, DNS filtering,

port blocking, service blocking IP blocking and DNS blocking; ISPs blocked the following ports: 25, 110, 123, 135:139, 143, 445.

SK: Teleoff survey on port blocking

Teleoff conducted survey among the 10 biggest ISPs in Slovakia, which included also port blocking. Responses did not prove practices breaching the Regulation. Some of the ISPs used blocking of ports (in most cases 25 (SMTP), 80 (HTTP), 445 (SMB), 7547 (CWMP)), but only for the sake of integrity and security of their networks.

FR: ARCEP survey on port blocking

The only port blockings reported by French ISPs were targeting port 25, which is understandable from an operational point of view: the limited resource in IPv4 addresses inhibits the possibility to give out fixed IP addresses for residential customers and therefore makes the use of port 25 for emailing irrelevant. ARCEP expects that this issue will be solved by the transition to IPv6. Apart from the general survey on traffic management practices, no other specific research was undertaken on port blocking. In the absence of a technical investigation, it is possible that the list is not exhaustive. Some end-users reported an instance of blocking port 53, a matter that is still under investigation.

NL: ACM conversation with ISP about port blocking

One Dutch ISP seemed to block port 5060. After a conversation with the ISP, they said that they don't block any port and that with a little bit of technical skill you can open every port. Port 5060 is just the standard one, because it works the best with automatic updates etc. ACM concluded that there was no need for formal enforcement actions.

HR: HAKOM survey on port blocking

HAKOM have made survey among ISPs on port blocking practices conclusions was that ISPs do not use permanent port-blocking measure, just temporarily justifying it with the security exception. Main reasons indicated by ISPs in Croatia for blocking ports (23, 25, 53, 135 and 445 etc.): spam, prevention of DDoS attacks and safeguard users from malware, spoofing. As previously mentioned, HAKOM offers HAKOMetar Plus measurement tool to end-users, which allows measuring different QoS-parameters, including blocking of UDP and TCP ports.

AT: NRAstudy on "transparency of networks" and port blocking

The Austrian NRA commissioned a study on "transparency of networks" as a benchmark in 2016, which was continued in two rounds in 2017. The study gives insight into the practices in telecommunication networks of different ISPs. The basic idea of the study was to transfer data packets from end-users to a server. Modifications (such as blocking) were identified and recorded. In total, 15 test metrics were implemented during the study. In addition, the Austrian NRA offers the RTR-NetTest (https://www.netztest.at), a crowd-sourced measurement tool which allows measuring different QoS-parameters, including blocking of UDP and TCP ports.

AT: NRA information procedures and port blocking

So called "information procedures" conducted with five major Austrian ISPs showed that some ISPs block different ports of the UDP and TCP protocols. It was indicated that blocking is required for network security and integrity (Article 3(3), third paragraph, sub b). There were differences between fixed and mobile networks with no homogeneous picture, different ISPs block different ports. The actual background for blocking was only partially mentioned. To a large extent, port blocking has historical reasons or is a consequence of network configuration

of the specific ISP. In some cases, issues with modem firmware were “fixed” with port blocks. In addition to the blocking of specific ports, it was identified that the use of private addresses or the implementation of so-called firewalls also leads to factual blocking of incoming traffic (thus blocking of all incoming TCP and UDP ports) in some networks. The Austrian NRA held bilateral meetings with the affected operators and the actual grounds for blocking specific ports were clarified. Some port blockings were classified as justified under Article 3(3), third paragraph, sub b, while other port blockings could be lifted.

DE: BNetzA investigation on port blocking practices

BNetzA investigated port blocking practices implemented by two ISPs in Germany. One ISP blocked ports UDP/TCP 0, TCP 445 (mobile network). Another provider blocked UDP 67/DHCP, UDP69/TFTP, UDP/TCP 135-139 and TCP 445 (cable network). Overall, BNetzA considered the blocking of these ports permissible according to Art. 3(3), third subparagraph, sub b. However, Article 3 (3), third subparagraph, sub b does not imply an obligation to block these ports. One ISP amended its general terms and conditions according Article 4, first paragraph, sub b, providing information about these port blocking practices. Another ISP also assured to do this.

BG: Some ISPs block ports for preservation of network integrity and security

Some ISPs in Bulgaria block certain ports in order to preserve the integrity and security of the network and to protect terminal equipment and end-users from DDOS attacks and spam.

FI: FICORA statement on port blocking

The main finding from the conducted traffic management survey was that many Finnish ISPs were still blocking multiple communication ports and justifying their activities with the security exception. The approach taken by each ISP was better aligned than last year, but still ISPs were blocking different communication ports and the same ports were mainly blocked by just a few ISPs. FICORA issued a statement that sufficient grounds for most of the port blocking practices had not been provided and that other measures than those included in FICORA's recommendation should be withdrawn by the ISPs. FICORA contacted all ISPs that did not provide sufficient justifications and monitored that ISPs removed all port blocking practices that violates the Regulation.

PL: port blocking by ISPs

Out of 24 questioned ISPs in Poland, most do not apply any port blocking practices.
One ISP indicates that it blocks ports for incoming internet traffic.
Five ISPs block the following ports:
1) 25,
2) 25, 123 53 and other ports considered as dangerous, the list of which is updated,
3) 25, 587, 135-139, 445, 1900, 69,
4) 23, 80,
5) 25, 80, 8080, 22, 23, 16, 162, 53.
ISPs justified that blocking ports is necessary to prevent the distribution of spam or to ensure the network security and also to protect end-users’ equipment from attacks.

5 Article 3(5)

Question 9.
What approach have you taken to monitoring services other than internet access services (called specialised services below)?
- market survey without requesting information from ISPs (e.g. checking ISP's offers on their web pages)
- information request from ISPs
- analysis of complaints and end-user reporting
- technical network monitoring
- other, please specify:

Is there any change compared to the previous period? Y/N

More than half of the NRAs used the first two methods of monitoring specialised services (SpS), namely through market surveys without requesting information from ISPs and through formal information request from ISPs. Remarkably, most of them used both methods, as shown in the table below, while 11 NRAs said there were changes compared to the previous period regarding their monitoring approach of SpS.

Approach	NRAs	Number
Market survey without requesting information from ISPs (e.g. checking ISP's offers on their web pages)	BE, CY, CZ, EE, ES, FR, HR, HU, IE, IT, LT, LV, MT, NL, PT, SI, SV	**17**
Information request from ISPs	AT, BE, BG, CH, CY, CZ, EE, EL, FI, FR, HR, IE, IT, LT, LV, MT, NL, PL, PT, SI, SV	**21**
Analysis of complaints and end-user reporting	AT, BG, CY, CZ, DE, ES, FI, FR, IT, PT, RO	**11**
Technical network monitoring	AT, BE, HR, HU, IT, LT, MT	**7**

Table 6. Approaches of NRAs regarding monitoring of services other than internet access services

Question 10.

Is there an NRA or national interpretation of or guidance on "services other than internet access services", which has not yet been mentioned in the BEREC NN Questionnaire of 2017? Y/N

No NRA has or disposes of a national interpretation of or guidance on "services other than internet access services", which has not yet been mentioned in the BEREC NN Questionnaire of 2017.

PL: UKE Questionnaire on specialised services

The ISPs in Poland responded to the UKE Questionnaire and they mainly named the IPTV and VoLTE as specialised services. Furthermore, the following specialised services have been indicated: IP telephony (with IPTV, as part of the Triple Play bundle in the cable television networks), VoIP services, data transmission services for businesses (including VPN), second layer data services (ethernet and ATM), video services, music streaming, telemetric services. In their replies to the UKE Questionnaire, ISPs indicated that they handled different kinds of traffic with enhanced quality and higher priority than for the internet access service (e.g. priorities for all kinds of on-net signalling, including for the SIP protocol).

Question 11.

Have you completed any formal assessments of the provision of specialised services by ISP? Y/N

If yes, briefly describe the practice and the conclusions of the assessment (and enforcement action where applicable)

In total, 8 NRAs completed formal assessments of the provision of specialised services by ISPs.

AT: NRA decision on specialised service for linear live-TV and Video on Demand

The Austrian NRA has published a decision on the prioritization of linear live-TV and Video on Demand traffic. In Austria, an ISP provides a TV-product which consists of 2 parts: linear live-TV and Video on Demand (replay functions and VoD movies). Both are prioritized/optimized. The ISP argues that the whole product is a specialised service (SpS) (Art 3(5) of the Regulation). The Austrian NRA sees it as problematic that in case of a justified SpS (linear live-TV according to para. 113 of the Net Neutrality Guidelines) the ISP can “add” an additional service, arguing that it is part of the SpS. There are many stand-alone VoD products in the market, so the NRA believes that this product needs to be considered separately. The Austrian NRA conducted a survey regarding technical and economic characteristics of the offer.

End-users’ rights, as defined in Article 3(1) of the Regulation, are limited because the ISP prioritizes the VoD traffic of the A1 TV product over all other traffic provided over the internet access service. With this, all other services, content and applications are slowed down, restricted, degraded and discriminated.

The requirements for a specialised service are not fulfilled by the VoD component of the product. The Austrian NRA has ordered the ISP to stop the practice and replace the affected set-top-boxes within 3 years.

SI: AKOS measurements on IPTV streams

AKOS is running measurements on multicast IPTV streams provided by the ISPs. They measure the technical IPTV parameters and also some other Key Performance Indicators (KPIs) that determine the picture quality. With these measurements, they can compare the quality and bandwidth consumption of this SpS between different ISPs.

FR : ARCEP monitoring specialised services

Last year ARCEP assessed voice over broadband, managed IPTV and entreprise VPN and their delivery as specialised services. The items presented in ISPs' responses showed indeed that those services had special QoS requirements and were delivered without detriment to the availability or quality of internet access services. Further studies on specialised services are still under investigation.

NL: ACM informal conversation about specialised service

ACM had an informal conversation with a Dutch ISP about the regulatory conditions for a specialised service for public transport company staff.

UK: OFCOM monitoring of specialised services

During the 2017/18 reporting period, OFCOM monitored compliance with Article 3(5) by:

- reviewing publicly available information from the largest ISP websites, including most especially the Key Fact Indicators (KFIs) they publish about their traffic management practices;
- issuing information requests to the largest ISPs, as part of and enforcement programme, when their KFIs indicated they offered specialised services, and reviewing the responses to those requests.

HU: NMHH monitoring IPTV

As in last year, NMHH continuously monitored ISPs' conditions for the provision of IPTV and examined related contractual terms. Examinations did not reveal major problems in Hungary but NMHH are continuing their monitoring process.

CY: ISP report to OCECPR about specialised services

According to the provisions of the Regulation (as interpreted in the Net Neutrality Guidelines), as adopted in national secondary legislation (Decree 72/2017), ISPs in Cyprus reported to OCECPR on specialised services. Following assessment of ISPs reports, OCECPR found out that provision of the type of specialised services offered by ISPs does not constitute an infringement of the Regulation.

CZ: CTU analysis of contract terms

CTU found a problem with the definition of influence of the use of specialised services on the internet access services (Article 4, paragraph 4, letter c of the Regulation). According to CTU findings over the reference period, a definition of these facts was often missing in the contract terms or was incomprehensible to the end-users (particularly the consumers). For the time being the situation has remedied as regards the internet access providers operating nationwide, as they were imposed the obligation to state these facts in the contracts covering the internet access service by the decision issued in the administrative proceedings. CTU has addressed the biggest local internet access providers with a request to remedy the situation as well.

6 Article 4

6.1 Article 4(1) – approach to monitoring and enforcing compliance

Question 12. What approach have you taken to monitoring and enforcing ISPs' compliance with their transparency obligations set out in Article 4?

- market survey without requesting information from ISPs (e.g. checking the applicable "terms and conditions"),
- (formal or informal) information request from ISPs,
- analysis of complaints and end-user reporting,
- other_____

Is there any change compared to the previous period?

It looks like the three approaches as shown in the table below have more or less equal preference among the NRAs.

Approach	NRAs	Number
Market survey ~~without requesting information from ISPs~~ (e.g. checking ISP's offers on their web pages)	BE, BG, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LU, LV, MT, NL, NO, PL, PT, SI	**21**
Information request from ISPs	BG, CY, CZ, DE, DK, EE, EL, ES, FR, IE, IT, LV, MT, NL, NO, PL, PT, RO, SK, UK	**20**
Analysis of complaints and end-user reporting	AT, BG, CY, CZ, DE, ES, FI, FR, IE, IT, HR, LV, MT, PL, PT, RO, SI, UK	**18**
Other	DE, FR, IT, LT, LU, PT, RO, UK	**8**

Table 7. Approaches of NRAs regarding monitoring and enforcing ISPs' compliance with their transparency obligations set out in Article 4

Furthermore, the following approaches were applied by NRAs:

IT, LT, PT, SI, UK analysed the contractual terms (e.g. by monitoring websites) used by ISPs. IT published statistical comparative values of ISPs QoS results reached in past periods. PT, UK monitored ISPs' websites. Similarly, in DE regular spot checks of the terms and conditions were carried out. Bilateral meetings and discussions with ISPs were held in LU and RO. In AT, the ISPs are obliged under the Austrian Telecommunications Act 2003 (TKG 2003) to notify their T&Cs to the Austrian NRA before they start a new communication service or change existing services.

IT, by virtue of a competence attributed by the Decree Law of 16 October 2017, n. 148 art. 19 quinquiesdecies, launched a public consultation (decision no. 33/18/CONS) regarding the definition of technical characteristics and the definitions of the various types of physical infrastructure used for the provision of telephone services, television networks and electronic communications. Following the consultation, AGCOM published a binding decision (no. 292/18/CONS) which defines the technical characteristics and corresponding names of the different types of infrastructure by which fixed broadband and ultra-broadband access services

are provided to end-users and imposes, on ISPs, certain obligations of transparency in advertising as well as in the contract.

In FR the body responsible for protection of end-user rights and compliance with consumer law (DGCCRF) has undertaken a market survey in order to review the transparency engagements of ISPs' contracts. The conclusion of this survey was that French ISPs do not fulfil the requirements of Article 4 of the Regulation for the time being. DGCCRF will work together with ARCEP to lay out more precise requirements.

Two out of three NRAs (21) explicitly pointed out that there is **no change** compared to the previous period (AT, BE, BG, CH, CY, CZ, DE, DK, EE, FI, FR, HR, HU, IE, LT, LV, MT, PL, SE, SK, UK).

Question 13. Have you completed any formal assessments of the ISPs' contract conditions and their compliance with requirements set out in Article 4(1) sub a-e?

If yes, please describe the main findings. [Note: detail of compliance in relation to speeds information requested below under Q16, 17]

A formal assessment of the ISPs' contract conditions and their compliance with Article 4(1) sub a-e was completed by 14 NRAs (AT, CY, CZ, BG, HR, HU, IT, LU, MT, NL, NO, PL, SI, SK). More specifically, in IT the NRA publishes links to the ISPs' terms of service on its website.

It should be noted that the question asked whether formal assessments were completed. Not having done so should not be confused with monitoring and enforcing ISPs' compliance with their transparency obligations, see Q12 above.

General Findings

Overall, the degree of ISPs' compliance with the requirements set out in Article 4(1) sub a-e seems to differ among countries, ranging from complete or high compliance (DE, CY, MT, SK), to sporadic incidents (e.g. where information is either missing or not easily accessible, e.g. PT, LU), to situations leading the NRA to start administrative proceedings (e.g. CZ). However, it also seems that where NRAs did not start formal investigations, their activities led to improvements (see below DE, NL, UK). The ease of accessing or finding relevant information can also be a problem in practice (see below LU, PT). In AT, CY and HR the ISPs are obliged to notify their terms and conditions to the NRA before launching a communication services or when modifying them.

More specific findings

CZ pointed out that most of shortcomings were found in relation to the obligation stipulated in Article 4, first paragraph, sub b-d. The NRA launched 24 administrative proceedings, approx. half of them being closed already and obliging ISPs to alter their contractual terms.

According to PT, the degree of completeness and detail of the information made available varies depending on the subject and differs among ISPs. Also, some information is provided by reference to ISP's websites and is not always easy to access. Similarly, LU stated that relevant information was missing and difficult to find, e.g. there was no clear explanation of traffic management measures, speeds or on how other QoS parameters may in practice impact internet access services.

AT and HR referred to ISPs' problems, specifying realistically achievable speeds for mobile. NL pointed out that most ISPs did not define speeds at all, however, following policy rules

published by the NRA most ISPs now define speeds in their contracts. ES pointed out that some ISPs have to include information on traffic management measures and their effects in their contracts.

No infringements with regard to Article 4(1) sub a-e were found in CY and MT. A high level of conformity with the Article 4(1) exists in SK where 90% of ISPs complied with contract conditions set out in Article 4(1) sub a (resp. 80%/100%/100%/90% for articles 4(1) sub b-e).

DE pointed out that there were consumer complaints concerning the contractual restriction of VoIP. Upon intervention of the NRA the ISP changed its terms and conditions. In another case in DE, it could be achieved after discussions with the market that two ISPs adapted their terms and conditions, now also informing about the possibility to apply admissible port blocking and related effects on applications or services respectively assuring to do so. In the UK, through the NRAs engagement with ISPs, key changes were secured to ISP consumer contracts to enhance transparency around traffic management and how ISP practices may impact on privacy and protection of personal data, as well as changes to improve transparency of the remedies available to consumers if they experience performance issues with their internet access service. No formal investigations were initiated.

Lastly, in HU ISPs with over one thousand subscribers are required to verify compliance with their guaranteed service level indicators by submitting an annual declaration of compliance to NMHH or a certificate issued by a designated body.

Question 14. Have national specifications been set in relation to the different types of speeds laid out in Article 4(1) sub d?
Question 15. Are these requirements or the NRA's opinion/recommendation legally binding?

Specifications

National **specifications in relation to the different types of speed** have been set by 15 NRAs (BE, CY, DK, FI, HR, IT, LU, LV, MT, NL, PT, RO, SI, SK, UK). Table 8 displays that several countries used **percentage values** by defining minimum and normally available speeds as percentage of the maximum speeds (HR, FI, IT, LV, SI, SK). In IT a **statistical** approach is used for minimum and maximum speeds referring to certain speed measurements in a given time interval. In MT **typical speed ranges** were set by the NRA. In LU the guidance concerning the speeds also contained best practices.

However, the table also shows that in each of these cases speed specifications did **not cover all types of speeds** mentioned in Article 4(1) sub d. Other countries did not specify the speed values, but require ISPs to provide information about the speeds. E.g., in BE the information to be provided has to be based on the category of the connection (e.g. for ADSL/VDLS2 technologies based on the line's attenuation and the distance of the connection from the active network equipment). In HU, while there is no specification of speeds, ISPs with over one thousand subscribers are required to verify compliance with their guaranteed service level indicators by submitting an annual declaration of compliance to NMHH or a certificate issued by a designated body. In the UK the Advertising Standards Authority has made major changes to the way broadband speed claims can be advertised. Under the new rules, speed claims in broadband ads should be based on the download speed available to at least 50% of customers

at peak time and described in ads as “average”. This marks a change from the current position that advertised “up to” speeds should be available to at least 10% of customers.

Legally binding or informal

In 9 countries these requirements or NRAs’ opinion/recommendation are **legally binding** (BE, CY, FI, HR, HU, IT, LV, MT, RO). IT specified that the minimum contractually agreed speeds are binding.

In most cases where speeds are specified by the use of percentages, the specification is binding (FI, HR, IT, LV – not in SI, SK).

In 11 countries specifications or requirements are **not legally binding** (AT, CZ, DK, LT, LU, NL, PL, PT, SI, SK, UK).

For example, in AT, market players agreed to use or at least consider an information sheet drafted by the NRA to inform customers of the details laid down in Article 4(1), sub b of the Regulation. The main intention was to achieve comparability among the terms and conditions of different ISPs. The ISPs accepted the NRA’s opinion/recommendations, but if necessary the NRA could set legal binding measures. However, even though in BG speed requirements set in national guidelines - preceded by a public consultation - are not legally binding, yet the NRA indicated that it will follow them when examining ISPs’ compliance.

Imposed by

Such specifications in relation to the different types of speed were imposed by 14 NRAs (BE, CY, FI, HR, HU, IT, LU, LV, MT, NL, PT, RO, SI, SK).

In 6 cases they were **agreed upon by market players** (AT, DK, HU, IT, SI, UK). Agreement by market players often coincides with non-binding specifications (AT, DK, SI, UK), but there are also cases where a legally binding specification comes along with agreement by market players (HU, IT).

More specific findings

In IT a co-regulatory framework applies. Specifications were set in a technical working group involving stakeholders and then included in an NRA decision. In DK, the Danish Consumer Ombudsman has issued a set of guidelines on the marketing of broadband connections.

A revised voluntary Broadband Speeds Codes of Practice for fixed services was published by the NRA in the UK (1 March 2018). The main changes to the Code were to (*inter alia*): improve relevancy of speed estimates at the point of sale by reflecting peak time speeds; provide a minimum guaranteed download speed at the point of sale.

In NL the NRA published (after a public consultation) the policy rule on the provision of information concerning internet speeds, setting out the NRA’s interpretation of the different internet speeds. This policy rule entered into force on January 1, 2018 for new contracts, and on March 1, 2018 for existing contracts of both consumers and business end-users.

The answers provided to Q14 and Q15 show that there is a variety of institutional settings on how specifications are set. In almost all cases, this involved activities by the NRA, taking the form of recommendations or decisions etc.

Country	Specification of speeds by the use of percentages	Achievability of speeds
CY		Fixed network ISPs are required to set time periods when maximum and normally available speeds are achieved resp. when speed may be limited to the minimum.
DE		Max: speed: 90% of the contractually agreed maximum speed should be achieved at least once at each of at least two measurement days (download speed of fixed broadband lines). Normally available: ≥ 90% of the measurements Min.: Not below contractually agreed speed at each of the 2 measurement days Requirements (*inter alia*): at least 20 measurements on at least two separate days)
HR	Min speed ≥ 70% of max speed Normally available speed: not specified because of the high threshold for minimum speed	
FI	Min. speed ≥ 70% of max speed Normally available speed: 90% of max speed (both apply only for fixed connections with max speed ≤100 Mbps) Max. speed: may not be lower than the advertised speed of the connection	Max. speed of (fixed): connection must be such that the user can expect to receive it at least some of the time. Estimated max. speed (mobile): must be possible to be realistically achieved in actual usage conditions.
IT	Min. speed/ max. speed: 95- and 5-quantile (respectively) of the speeds measured in a time interval (6 months for statistical comparative values / 24 hours for single users' lines)	Max. speed is defined based on actual measurements, therefore it is achievable.
LV	Min speed: ≥ 20% of max. speed	
SI	Normally available speed: at least 80% of max. speed	Normally available speed: at least 90% of the time of the day outside peak hours

Country	Specification of speeds by the use of percentages	Achievability of speeds
	Max. speed: theoretically the highest data transfer rate from the server or to the server	Max. speed: achievable at least once per day Min. speed lowest actual data transfer speed from the server or to the server (except for network failures)
SK	Min. speed: ≥ 40% of max speed Normally available speed: ≥ 90% of max. speed Advertised speed: recommended to be applied such that it allows to evaluate advertised speed against real performance of internet access service	Normally available speed: 90% of any continuous 4-hour measurement period Max. speed: at least once between 00:00 to 24:00

Table 8. Specification of speeds by the use of percentages and achievability of speeds

Question 16. To the extent your NRA has reviewed the terms and conditions in ISP contracts, did ISPs define in their contracts minimum, maximum, advertised and normally available upload and download speeds of the internet access service in the fixed network?[4]

Definitions provided (completely/widely)

Fixed network ISPs contractually defined these speeds in 19 countries (AT, BE, BG, CY, CZ, EE, ES, HR, IT, LT, LU, LV, MT, NL, NO, PL, PT, SI, SK).

DE pointed out that ISPs increasingly defined these speeds in their contracts. While in NL speeds were not defined by most of the ISP, this changed significantly after the NRA had published its policy rule. FI referred to one case where the normally available speed was missing and some of the other speeds defined did not seem to be in line with the NRA's opinion. The case was settled. HR mentioned a partial compliance, since all ISPs have not yet defined the normally available speeds (upload/download). IT pointed out that minimum speeds are specified in contracts. AGCOM is considering whether to modify regulation in order to introduce other parameters as well.

Lacking provision of definitions

6 countries (CH, EL, FR, HU, IE, RO) pointed out that these speeds are not contractually defined. IE specified that absent enforcement powers, there appears to be no incentive to comply. FR points out that ISPs only define the theoretical maximum speeds for their fixed

[4] Note: remarks provided in this section only relate to countries where the NRA has reviewed the terms and conditions in contracts of fixed network ISPs.

access offers. IT stated that minimum speeds only are specified. In NO, speeds are defined in contracts only to a limited extent.

Examples[5]

CZ identified an unclear or incomprehensible definition of the transmission speeds as a frequent issue. With regard to the minimum speed, there were instances where the minimum speed exceeded the normally available speed or where contractual terms contained various minimum speeds. In PT most of the speed information is provided by reference to IPSs' websites. In particular, where information is provided on different webpages not always easily accessible, it is doubtful whether ISPs are compliant with the requirements of the Regulation.

In PL, ISPs assume different reference periods for which the normally available speed is determined. Most ISPs assumed 24 hours as reference period, others the monthly billing period, while others merely quote the recital of the Regulation.

BG identified two cases where ISPs did not include in their contracts information about the usually available speeds for download/upload.

Other aspects

In 5 cases the advertised speed was not defined separately but equalled the maximum speed (DE, CZ, HR, LT, PL).

DE and PL point out that speed information is provided either as percentage or as concrete figures, while in MT ISPs advertise the headline speed of their connection and include a reference to the typical speed range (TSR) in their terms and conditions.

GR mentioned that the NRA had issued a recommendation in early 2018 advising the ISPs to grant an imbursement to customers in case advertised speeds are not achieved and to eventually mention the different speeds in their contracts. Similar, in LV the end-user can claim compensation if the guaranteed minimum speed – at least 20% of maximum – is not reached.

Question 17. To the extent your NRA has reviewed contracts of mobile ISPs, did they define in their contracts advertised and estimated maximum upload and download speeds of the IAS in the mobile network?[6]

Definitions provided (completely/widely)

Generally, the situation is quite similar for mobile internet access services. In 14 countries – where NRAs have reviewed the mobile ISPs' contracts – these speeds are defined in contracts (AT, BE, BG, CZ, EE, ES, HR, IT, LT, LU, LV, MT, PL, PT, SK).

DE pointed out that ISPs increasingly defined these speeds in their contracts, typically mentioning concrete figures for the respective speeds. FI clarified that this issue was not studied last year, however, these parameters have already been defined.

[5] Note: Examples may also be provided here for a country where the requirement to provide contractual information is largely met across all ISPs.
[6] Note: remarks provided in this section only relate to countries where the NRA has reviewed the terms and conditions in contracts of fixed network ISPs.

HR explained that ISPs provided estimated maximum speeds in a geographical manner using mobile internet access service coverage maps with estimated speed values of network coverage in all locations for different network technologies.

In IT ISPs specify in their contracts the advertised speeds. AGCOM is considering whether to modify regulation in order to introduce other parameters as well.

In NL, after intervention by the NRA, contracts now inform about the speeds. Prior to this intervention none of the ISPs did so. The general terms and conditions only referred to the website of the ISP in question where the coverage card could be found.

LV specified that ISPs included in contracts references to their webpage.

It should be noted that according to para. 142 of the Net Neutrality Guidelines the requirement to include in the contract and publish information about advertised speed does not entail a requirement to advertise speeds. This requirement only applies in case where speeds are advertised. Thus, where no speed is advertised and where information on estimated maximum speed is provided the country is classified as “speeds are defined in contracts”. This holds e.g. for MT where ISPs include estimated maximum upload and download speed figures based on their network capabilities.

Lacking provision of definitions

8 countries (CY, EL, FR, HU, IE, NO, RO, SI) pointed out that these speeds are not contractually defined.

IE specified that absent enforcement powers there appears to be no incentive to comply. FR explained that ISPs only define the theoretical maximum speeds for their mobile access offers, i.e. the maximal reachable speed for a given access technology. In EL ISPs do not define advertised and estimated maximum speeds in their contracts, but only guide their customers to the use of relevant measurement tools and platforms. In CY, this happens because ISPs do not advertise any speeds, therefore they do not define any advertised and estimated maximum upload and download mobile speeds in their contracts.

Examples[7]

CZ specified that regional mobile ISPs often did not define the speeds, while the largest ISPs defined them but in an unclear or incomprehensible way. In many cases, the advertised speed was set out as an interval or was defined for some end-users only (certain percentage of the total number of end-users). Nevertheless, following the NRAs inspection activities and its decisions, the situation gradually improved.

BG mentioned a non-compliance issue referring to a lack of information about the maximum speed when the volume limitation is reached in the contract terms of one mobile ISP.

AT pointed out that as far as mobile services are concerned the (often significant) deviation between the estimated maximum speed for 3G and 4G connections set out in their terms and conditions and the realistically achievable speeds in their mobile networks is still a problem. Similarly, LT referred to cases where mobile ISPs indicated on their maps that users can expect 300 Mbps while only 80 Mbps are achievable at maximum. The NRA advised to specify the parameters on the map with realistically available speeds. Also HR referred to mobile ISPs

[7] Note: Examples may also be provided here for a country where the requirement to provide contractual information is largely met across all ISPs.

difficulties to specify realistically achievable speeds (setting up of unique realistic usage conditions).

However, PL stated that the majority of ISPs indicate the estimated maximum speed in such a way that the end-user is aware of the achievable maximum speed of the internet access service in different locations, in real conditions of use. ISPs also stipulate in the contracts that it is possible to achieve the estimated maximum speed under favourable circumstances, also explaining the factors impacting upon this (see also below “Realistic usage conditions”).

Realistic usage conditions

In some countries (AT, BG, CZ, LU, MT, PL) ISPs mention in their terms and conditions factors impacting on the available speed. Reference is made to factors such as the device, network coverage, radio signal quality, network load and number of users in any given location, time of day, geographical factors, density of the building, distance between receiving terminal and transmitting antenna).

In 3 countries (CZ, HR, UK) discussions were held with mobile ISPs with the aim of defining realistic usage conditions under which the estimated speed can be achieved.

More specifically, the NRA in CZ recommended to indicate the data transmission speeds for individual locations or areas with the mobile network coverage in the form of geographical maps. However, this recommendation was not fully accepted by the internet access ISPs. At present, only the maps showing the coverage by the individual technologies can be found on the ISPs´ websites. For each technology the estimated maximum speed is also stated. These figures do not represent the values actually measured by the ISPs in the respective location or area nor values calculated with regard to a usual network load. The advertised data download and upload speeds are not stated either.

In the UK an industry working group has been established by the NRA to provide consistent cross-industry messages and information on mobile coverage. This will involve agreeing to a common means of measuring coverage, which will involve further testing, using both test equipment and crowdsourcing. The working group will consider how best coverage information should be presented to consumers to make it easy to understand. Ofcom has advised ISPs that they will communicate with them on mobile speeds separately, once the work of the industry group is closer to completion.

Overall assessment of answers provided to Q16 and Q17

More generally, the answers to Q16 and Q17 typically show that for a given country, speeds were contractually defined - respectively not defined - by both fixed and mobile ISPs. Out of those countries where mobile speeds are not contractually defined, in 4 countries (CY, NL, NO, SI) fixed speeds were contractually defined however.

6.2 Article 4(2) – procedures for end-user complaints

Question 18. Have ISPs established "*transparent, simple and efficient procedures to address end-user complaints…*" according to Article 4(2)? Y/N

If yes: What kind of procedures has been established by ISPs (e.g. hotlines, complaint templates)?

Is there an industry wide approach in relation to these procedures? Y/N

If yes, was this approach:

- imposed or facilitated by the NRA,
- prescribed by national legislation,
- voluntarily agreed upon by the market players,
- other _____

Is there any change compared to the previous period? Y/N

In most countries (26: BE, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, MT, NL, NO, PL, PT, RO, SE, SI, SK and UK), ISPs have established procedures for addressing end-user complaints in case of non-conformance of the provided services with the contractual terms.

In general, such procedures were already in place before the Regulation entered into force, as providers of internet access services are required to do so as part of existing telecoms legislation based on the Universal Service Directive[8]. In the UK, the complaints-handling rules have recently been overhauled.

16 NRAs (CY, DE, DK, EL, FR, HR, HU, LV, MT, NL, PL, RO, SE, SI, SK and UK) reported that there is an industry-wide approach, whereas 12 NRAs (AT, BE, BG, CZ, EE, ES, FI, IE, IT, LT, LU and PT) mentioned that this is not the case. Further details related to the industry-wide approach are outlined in Table 9.

Industry-wide approach	Respondent	Number
Imposed or facilitated by the NRA	CY, DE, IT, RO, SI, UK	**6**
Prescribed by national legislation	CY, EL, HR, HU, LV, SE, SI, SK	**8**
Voluntarily agreed upon by the market players	FR, MT, NL, PL, SE	**5**
Establishment of an independent private complaints board by the telecom industry in cooperation with the Danish Consumer Council	DK	**1**

Table 9. Industry wide approach regarding procedures for end-user complaints

[8] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services.

Generally, different channels are made available by ISPs facilitating the filing of complaints by end-users. The most common channels are telephone lines, web forms, letters and customer service points.

25 NRAs (AT, BE, BG, CY, CZ, DE, DK, EE, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI and UK) reported that there is no change compared to the previous reporting period, whereas changes in the respective procedures have been performed in SK.

6.3 Article 4(3) – additional transparency requirements

Question 19. Did you nationally (e.g. NRA, Ministry) provide guidance or impose **additional** transparency or information requirements on ISPs following the coming into force of the Regulation? Y/N

If yes, please provide details of the requirements.

According to Article 4(3), Member States could introduce additional monitoring, information and transparency requirements. 18 NRAs (BE, BG, CZ, DK, EE, EL, ES, FI, FR, IE, LT, LV, MT, NO, PL, SE, SK and UK) neither provided guidance nor introduced such requirements during the reporting period. However, in BG, the NRA initiated two administrative proceedings, but the corresponding final decisions which include transparency requirements are pending.

Four NRAs (CY, HR, HU and IT) reported that national and/or secondary legislation already prescribe transparency and information requirements.

Seven NRAs (AT, DE, LU, NL, PT, RO and SI) mentioned that in their Member State additional transparency requirements have been implemented or guidance has been provided during the reporting period. Further details are outlined hereafter.

In AT and LU, the respective NRAs provided guidance to ISPs, as well as organized several meetings and bilateral discussions for this purpose.

In DE, the ordinance for framework provisions on the promotion of transparency, publication of information and additional facilities for cost monitoring on the telecommunications market of 1st of June 2017 obliges fixed and mobile ISPs to provide more transparency when offering internet access services. ISPs are obliged to provide product information sheets where the consumer can quickly and easily see the essential contractual provisions before concluding the contract (data transmission rates available, contract duration, monthly costs). Also, consumers obtained the right to information on reliable measurement results for their internet connection and specifically on the actual data transmission rate.

In NL, the NRA determined, in their policy guidelines, that the speeds should be expressed in Mbit/s or Gbit/s.

In PT, the preparation of the final decision, which will support the provision by ISPs of simplified information sheets in pre-contractual and contractual situations is ongoing.[9]

[9] ANACOM has launched in April 2018 the process for introducing at COM.escolha (tariff comparison tool available via its website and which is loaded by the ISP on a voluntary basis) specific fields for the loading by the ISP of information relative to the data transmission speeds foreseen in the Regulation. This development of the comparison tool was concluded at the beginning of October 2019 and it is now expected that the ISP will soon be loading the mentioned information on data transmission speeds.

In RO, the electronic communications providers have to publish relevant information on their website, according to the provisions (which entered into force on 1st of May 2018) of an NRA's decision. For instance, such information is referring to speeds and the remedies available to consumers in case of non-conformity.

In SI, ISPs are required to explain to the end-users the relevant information according to Article 4(1) of the Regulation, especially regarding the impact of restrictions on data volumes, media sharing and other QoS parameters of the user experience by using internet access services. Furthermore, ISPs have to publish information on how specialised services and potential traffic management measures may affect the quality of the internet access service.

6.4 Article 4(4) – monitoring mechanism

Question 20. Is there an NRA or national interpretation of "*significant discrepancy, continuous or regularly recurring*"? Y/N

If yes,

- How are these terms interpreted?
- Was the definition:
  - imposed by the NRA (e.g. using Article 5(1)),
  - voluntarily agreed upon by the market players
  - other_____

With regard to Article 4(4) of the Regulation, the competent authorities of 6 Member States (CY, CZ, DE, HR, IT, MT) provided a national interpretation of "significant discrepancy, continuous or regularly recurring" regarding the actual performance. The different approaches used are outlined in Table 10. Some of these NRAs also gave a material interpretation of the terms, which can be found in Table 11.

Approach	**Respondent**
Definition imposed by the NRA	CY, CZ, HR, MT
Definition voluntarily agreed upon by the market players	-
Non-binding administrative notice issued by the NRA	DE
Interpretation approved by the NRA after discussions within a technical committee with operators, consumers' associations and the Ministry's technical staff	IT

Table 10. Different approaches of interpretation used by the NRAs

Respondent	Interpretation
HR	Non-compliance regarding fixed download speed if the results of at least 3 tests conducted in a period of 5 consecutive days (at least one test must be carried out every 24 hours) shows that speeds are below 70% of maximum/advertised speed. Tests are carried out by means of a certified tool for broadband speed tests prepared by the NRA.
CY	Non-compliance if results of measurements over 3 consecutive days show that the speed received by the end-user is less than or equal to 80% of the minimum or normally available speed specified by the ISP.
DE	Non-conformity regarding fixed download speeds if one of these cases occurs: • 90% of the contractually agreed maximum speed is not achieved at least once at each of at least 2 measurement days; • the normally available speed is not achieved in 90% of the measurements; • the speed falls below the contractually agreed minimum speed at each of the 2 measurement days. By measuring with the broadband monitoring mechanism, the following requirements need to be considered: • At least 20 measurements must be performed; • The measurements must be taken on at least 2 separate days; • The number of measurements is to be spread equally over the 2 days, so that at least 10 measurements are taken on a specific day; • The measurements must be taken using a LAN connection; • The measurements are to be carried out using the installable version of the NRA's broadband monitoring mechanism.
IT	End-users could terminate their contract without additional costs if minimum contractual speed is not achieved twice in 45 days. Measurements are run every 15 minutes on a certified tool during 24 hours. Minimum speed is calculated as the 95-quantile of measurement in the interval.
MT	• "significant discrepancy": this definition is implicit as any connection performing below the stated ISP's information regarding speed is considered as discrepant • "regularly recurring": no interpretation published

Table 11: Interpretation of the terms

In BG, the NRA issued for consultation a draft position on the definition of the terms "significant and continuous" and "regularly recurring". Based on the outcome, the NRA considers to determine a corresponding definition. In SK, the NRA also intends to issue a national interpretation of Article 4(4) of the Regulation.

22 NRAs (AT, BE, BG, DK, EE, EL, ES, FI, FR, HU, IE, LT, LU, LV, NL, NO, PL, PT, RO, SE, SI, and SK) mentioned that they do not provide any additional guidance or national interpretation.

Question 21. Do you collect or monitor the number of end-user complaints? Y/N

If yes, what was the level of end-users' complaints about the performance of the internet access service, relative to contracted parameters (speeds or other QoS parameters)?

22 NRAs (AT, BG, CY, CZ, DE, DK, EL, ES, HR, IE, IT, LT LU, LV, MT, NL, PL, PT, RO, SE, SI and UK) have reported that they are monitoring the number of end-user complaints, whereas six NRAs (BE, EE, FI, HU, NO, SK) indicated not to do so. One NRA (FR) has reported that it is not yet monitoring formal end-user complaints concerning discrepancies of performances, but that end-users can now report such problems on the new signalling platform "j'alerte l'Arcep".

Based on the data collected, end-user complaints are usually related to discrepancies between actual and contractual speed, as well as other quality of service (QoS) parameters, as set out in Table 12. Complaints referring to net neutrality issues generally correspond to less than 10% of the total number of ECS complaints.

Respondent	**Information related to NN complaints**
AT	112 requests related to the quality of mobile networks, 21 requests regarding the quality of fixed networks, 1 request referring to port blocking Total number of requests submitted for conciliation: 1783 Large number of general inquiries including net neutrality issues
BE	Complaints handled by the Ombudsman: 128 regarding internet interruptions, 72 regarding internet speed, 5 related to irregularities with respect to the zero-rating of mobile data, 2 about the principle of zero-rating
BG	Complaints due to insignificant divergence from contracted parameters for fixed internet access services (mostly related to the service quality of mobile internet access services and especially related to poor network coverage)
HR	2017: 23 complaints regarding internet QoS in fixed networks, 8 complaints regarding internet QoS in mobile networks (mainly related to the poor network coverage) 102 complaints regarding achieved minimum speed (12 months)
CY	12 complaints concerning QoS parameters (mainly fixed broadband connections – 12 months) No breaches of the regulation have been determined
CZ	Approx. 56% of the complaints were related to the non-compliance with the agreed quality parameters. Others concerned traffic management measures and commercial practices (incl. zero-rating) 0 complaints referring to any limitation of the choice of terminal equipment
DK	0 complaints

Respondent	Information related to NN complaints
DE	Between 1000 and 1200 requests per year concerning the speed of the internet access service (in total 81000 complaints in 2017)[10] Approx. 30 substantiated complaints based on the measurements done with the NRA's measurement tool and by considering the respective instructions
GR	176 end-user complaints (12 months)
IT	Complaints mostly related to minimum speed
LV	6 complaints of 92 about the performance of the internet access service (corresponding to 6.5% of total ECS complaints)
LT	Low number of complaints concerning speeds and other QoS parameters
LU	0 complaints
PL	Approx. 1% of the complaints were about the non-provision of the contractually agreed internet access service speed and usage of traffic management measures by ISPs
PT	01.05.2017-31.12.2017: 639 complaints regarding speed parameters
RO	Approximately 40 complaints regarding the performance of the IAS (fixed and mobile)
SI	12 complaints (approx. 4% of total number of complaints)
ES	0.5% of total claims (2017)
SE	Few
NL	Few complaints about the performance of the internet access service

Table 12. Level of end-user complaints about the performance of internet access services

Question 22. Have specific additional remedies been introduced for consumer redress in relation to non-conformance of the internet access service with the contract terms (e.g. legal action before courts and/or NRA, right to early termination, compensation)? Y/N

As general national legislation already covers non-conformance with the contract terms, 25 of the NRAs (AT, BE, BG, CH, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HU, IE, LT, LU, MT, NL, NO, PT, RO, SE, SK and UK) did not introduce any specific remedy.

However, in order to foster end-user rights, five NRAs (HR, IT, LV, PL and SI) have introduced additional remedies for end-user complaints in case of non-conformance of the internet access service with the contract terms.

[10] increase in the data as compared to the previous reporting period due to a new statistical registration

Question 23. Do you currently provide any internet access service quality monitoring tool for consumers to use? Y/N

- If yes, briefly explain this tool, and say whether you consider it as certified according to Article 4(4) and in line with Net Neutrality Guidelines, para. 161.
- If not, please outline any plans you may have for setting up such a tool.
- Is this tool used by the NRA to investigate any potential deviations in speeds or any other contractual parameter or – beyond the scope of Article 4(4) – for detecting infringements of the Regulation (e.g. throttling, blocking)?

For monitoring the performance of their internet access services, end-users could use the measurement tool made available by the respective NRAs. Indeed, 19 NRAs (AT, CY, CZ, DE, DK, EL, HR, HU, IT, LT, LU, LV, NL, NO, PT, RO, SI, SK and UK) have introduced such a monitoring tool during the reporting period or had already one in place before, whereas 10 NRAs (BE, BG, EE, ES, FI, FR, IE, MT, PL and SE) do not have such a monitoring tool in place.

All of the reported monitoring tools measure the speed of end-user's individual internet access service in fixed and/or mobile networks. The monitoring mechanisms also allow users to measure the quality of service parameters (generally: latency, jitter, packet loss).

In this context, one NRA (FR) mentioned that it is currently collaborating with the measurement ecosystem[11] to enhance the quality of the measurements on a whole. A draft version of a code of conduct which contains transparency criteria (on which tools must commit to communicate) and best practices regarding test protocol, has been published by the respective NRA. The NRA has also co-constructed with the ecosystem a technical solution, consisting of an API developed in the ISP modems, which will allow measurement tools to characterize the end user environment and could be used as a complement to the future QoS measurement tool developed by BEREC.

Four NRAs (HR, DE, IT and RO) consider their monitoring tool as certified according to Art. 4(4) of the Regulation and Net Neutrality Guidelines (para. 161). Three respondents (PT, SI and UK) mentioned that they have not yet certified a tool or that a possible certification is under discussion, whereas nine NRAs (AT, CZ, DK, EL, LT, LU, NL, NO and SK) do not consider their monitoring tool as certified.

Based on the information received, it could be concluded that some NRAs not having set up a national system are supporting and/or contributing to the BEREC project regarding the BEREC QoS measurement tool. Moreover, two NRAs (CZ and SI) also mentioned its participation in the MoQoS project. An NRA (BE) reported that it will launch a non-certified application to monitor the quality of the internet access service, whereas another NRA (PL) indicated that the project of implementing a certified measurement mechanism is ongoing.

Four NRAs (HR, HU, IT and LV) reported that they are using the tool to investigate any potential deviations in speeds or any other contractual parameter, or – beyond the scope of article 4(4) – for detecting infringements of the Regulation (e.g. throttling, blocking), whereas nine NRAs (DK, EL, LT, NL, NO, RO, SE, SI, and SK) indicated not to do so. One NRA (IE) highlighted

[11] The mentioned measurement ecosystem consists of ISPs, developers of measurement tools, academics and consumer associations.

that it has a tool at its disposal, which could be used in enforcement cases if the NRA ever gets any enforcement powers.

7 Article 5(1)

Question 24. Did you impose any QoS requirements on any ISP under the Regulation (EU) 2015/2120 (other than definition of contractual speeds)? Y/N

If yes, which requirements were imposed?

All NRAs responded negatively to this question.

Question 25. What approach have you taken to measure the **availability of high quality internet access services:**

- market survey without requesting information from ISPs,
- information request from ISPs,
- analysis of complaints and end-user reporting
- technical network monitoring
- other, please specify _____

Is there any change compared to the previous period? Y/N

Through the NRA responses we understand that the majority of them measure the availability of high quality internet access services through information request from ISPs.

Approach	NRAs	Number
Market survey without requesting information from ISPs (e.g. checking ISP's offers on their web pages)	AT, CY, EE, HU, IT, MT, PT, SE, UK	**9**
Information request from ISPs	AT, BE, BG, CY, DK, EE, EL, FI, FR, HR, IE, IT, LT, LV, MT, NL, PT, SE, SK, UK	**20**
Analysis of complaints and end-user reporting	BG, CY, DK, EL, FI, HR, IE, IT, LV, MT, PT, RO, UK	**13**
Technical network monitoring	AT, BE, CZ, EL, HU, IE, IT, LT, LV, NO, PL, PT, UK	**13**

Table 13. Approach of NRAs regarding the availability of high quality internet access services

Other than that, it seems that a few NRAs (CZ and DE) use broadband measurement mechanisms measuring the exact performance of multiple parameters, while PL purchases reports from tests carried out by the consumers.

Out of the 29 respondents, only 4 NRAs (CZ, NO, PT and UK) reported that they have changed their approach compared to the previous period.

Question 26. If you performed measurements of internet access service quality, please report the main findings in relation to the provisions of the Regulation.

Almost half (15 out of the 29) NRAs reported that either they (themselves) perform measurements of internet access service quality in the fixed and mobile networks or they use the measurements from crowdsourcing tools to evaluate the compliance of the ISPs with the Regulation. CZ did not provide particular findings. In IT the freely distributed software allows the end user to obtain a certificate to be used to complain against the operator and, if the measured quality is below the contractual terms again after 45 days, to void the contract without penalties or to obtain from the ISP a speed upgrade or a better tariff in case of discrepancy in the performance. The remaining 13 NRAs (AT, DE, EL, FR, HR, HU, LT, LV, NO, PL, PT, RO and UK) indicate that there has been an overall steady increase in the network speeds and capacity or at least there has been no degradation compared to the previous reporting period. This increase has been mainly attributed to the expansion of the optical fibre networks, as well as the broader use of LTE technology (in mobile networks). It is clear that in most cases there is still significant room for improvement in the respective KPIs, but it seems that the ISPs have managed to improve the overall performance of their networks despite the ever increasing consumer demand.

Question 27. Have you taken any other steps to ensure compliance with **Articles 3 and 4** according to **Article 5(1)** not mentioned elsewhere in this questionnaire? Y/N

If yes, which?

All NRAs but one (AT) have taken no other steps to ensure compliance with the above articles. AT however have issued two formal decisions for this reason:

- Automatic disconnect of IP connections of end-users every 24 hours. (violation of Art 3(1)) and
- Assignment of a public IPv4 Address only in case the end-user pays an additional fee (violation of Art 3(1)).

8 Article 6

Question 28. What rules on penalties to infringements of **Articles 3, 4, and 5** pursuing to **Article 6** of Regulation (EU) 2015/2120 do you apply?

24 of the NRAs (BE, BG, CY, CZ, DE, DK, EE, EL, FI, FR, HR, HU, IT, LT, LU, LV, MT, NO, PL, RO, SE, SI, SK and UK) stated that they impose fines in cases of infringements of the abovementioned articles. These fines vary in size ranging from 200 Euros (SK) to 3 million Euros (GR) according to the national regulation/legislation, or they may be defined as a percentage of the annual turnover of the relevant ISP, ranging from 2% up to 10%.

Other penalties are non-monetary and range from requesting the ISP to discontinue a specific offer or activity to suspending the license of the ISP to provide electronic communications services in the event of highly severe and repeated infringements.

Annex I: Abbreviations for countries

Throughout the report we have used Eurostat country codes as abbreviations for the country names (http://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Country_codes). The country codes for the NRAs to the questionnaire are shown in the following table.

Austria	AT	Latvia	LV
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Norway	NO
Czech Republic	CZ	Poland	PL
Denmark	DK	Portugal	PT
Estonia	EE	Romania	RO
Finland	FI	Slovakia	SK
France	FR	Slovenia	SI
Germany	DE	Spain	ES
Greece	EL	Sweden	SE
Hungary	HU	The Netherlands	NL
Ireland	IE	UK	UK
Italy	IT		