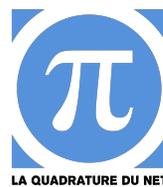


POLICY ANALYSIS OF BEREC DRAFT GUIDELINES

22 June 2016

Supported & co-drafted by:



Executive Summary	3
Scope	4
Zero-Rating.....	5
Summary of the Guidelines	5
Analysis	6
Provisions on commercial practices.....	6
Application Bundling	8
Traffic Management	9
Summary of the Guidelines	9
Analysis	11
Proportionality of traffic management measures	11
Differences in class-based traffic management	13
General Remarks	15
Specialised Services.....	15
Summary of the Guidelines	15
Analysis	17
Reclassification of online services as specialised services	17
Quality deteriorations of the internet access service	18
Transparency.....	20
Summary of the Guidelines	20
Analysis	21
Supervision and Enforcement.....	22
Summary of the Guidelines	22
Analysis	22

Executive Summary

The draft Guidelines of BEREC¹, which are open for public consultation, contain three outstanding issues that still need to be resolved. However, in general, they are a big step towards delivering real net neutrality. BEREC has done an excellent job at navigating the pitfalls left by the legislator and has produced a set of rules that clarify and balance net neutrality safeguards with the practical needs of the telecom industry. The Guidelines also create the right foundation for the roll-out of 5G technology by ensuring that high internet speeds and low latency are delivered in a sustainable and neutral way to the benefit of the European people and economy.

Concerning the issue of zero-rating (key paragraphs: 28–45), the Guidelines need to provide legal certainty, a harmonised application of the Regulation² and an investment-friendly climate. The current proposal fails to deliver this. The Regulation allows the prohibition of harmful commercial practices, like certain forms of zero-rating, but the Guidelines lack predictable, bright-line rules on this issue. They rely instead on a case-by-case approach which is likely to cause lengthy ex-post reviews, enormous competitive distortions and severe interference in consumer choice.

On traffic management (key paragraphs: 46–94), the application-agnostic nature of the internet is not protected well enough. The Guidelines still allow for a class-based system of Quality of Service (QoS) at the discretion of the Internet Service Provider (ISP). This leaves far too much power in the hands of the ISP, brings considerable risks of competitive distortions and discrimination, which would undermine future innovation.

Specialised Services (SpS) are defined in a solid way that should provide a clearer basis for Regulation (key paragraphs: 84–123). However, the current text has two outstanding issues: First, the quality requirements of such a service can be set by its provider instead of being based on objective technical characteristics, as the Regulation requires. Second, the Guidelines permit specialised services to cannibalise the bandwidth of Internet Access Services (IAS). This would create wrong incentives for ISPs to sell the same network capacity twice to the same end-user, instead of expanding capacity.

¹ See http://berec.europa.eu/eng/news_consultations/ongoing_public_consultations/3771-public-consultation-on-draft-berec-guidelines-on-implementation-of-net-neutrality-rules

² Regulation 2015/2120 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. Available online at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&from=EN>

Finally, we want to congratulate BEREC on its clear and strong solution on sub-internet offers and a potential third category of access services outside of the scope of the Regulation. We hope this balanced solution survives the pressures of the decision-making process.

Scope

With regard to the definition of Internet Access Services laid down in paragraphs 13–18 of the Guidelines, we welcome the specification that sub-internet services remain within the scope of the Regulation and are clearly prohibited, as explained in Paragraph 17. We want to use this opportunity to highlight that the relevant provision which prohibits “services other than internet access services” to be “offered or usable as a substitute of internet access services” has been part of the Regulation throughout all stages of the legislative process. This legislative history suggests the clear intention to prohibit sub-internet services.³

Furthermore, we welcome the clarification in Paragraph 18 that “*services where the amount of reachable end-points is limited by the nature of the terminal equipment*” may not be used to circumvent the Regulation. We want to highlight in this regard that there is no legal basis in the Regulation for a third category of access service besides “internet access service” or “services other than internet access services” (“specialised services”). We note, however, that e-book readers commonly offer internet browser functionalities which include connectivity to virtually all end-points in the internet. Yet, e-book readers sometimes limit the amount of reachable end-points, although this cannot be seen as a limitation by the of the terminal equipment. Therefore devices such as e-book readers can be used to circumvent this Regulation and this makes them an unsuitable example that contradicts the whole logic of Paragraph 18. Consumer electronics present an inherent demarcation problem in this regard and BEREC should clarify this aspect.

³ For a more detailed analysis of relevant provisions on sub-internet offers in the Regulation, see EDRis first input to the BEREC process page 14 and 15 https://edri.org/files/BEREC_Hearing2015_EDRiposition.pdf

Zero-Rating

Key articles of the Regulation: 3(1), 3(2); Recital 7

Key paragraphs of the Guidelines: 28–45

Summary of the Guidelines

The Guidelines do not prohibit zero-rating. Rather, they call for a case-by-case assessment of whether a *material reduction* of the end-user rights of Article 3(1) takes place (Paragraph 44).

For this assessment, zero-rating schemes are more likely to be prohibited if they (paragraphs 42–44):

- Privilege specific apps or services, rather than categories of traffic.
- Are carried out by ISP and/or CAPs with stronger market positions.
- Circumvent the aims of the Regulation, in particular to: “guarantee the continued functioning of the internet ecosystem as an engine of innovation”.
- Affect business & consumer end-user rights, i.e.: reduce the range and diversity of content and applications in practice; incentivise users to use certain platforms and/or materially reduce end-user choice.
- Affect CAP end-user rights, i.e.:
 - materially discourage CAPs from entering the market;
 - force CAPs to leave the market;
 - bring other material harms to competition on the CAP market;
 - affect ‘the continued function of the internet ecosystem as an engine of innovation’;
 - allow ISPs to ‘pick winners and losers’; and/or
 - create administrative or technical barriers for CAPs to enter into agreements.
- Occur on a large scale and without alternative offers available
- Affect freedom of expression and/or media pluralism.

In addition, the Guideline introduces the following principles

- Zero-rating schemes where non-zero-rated applications are blocked or throttled after the data cap is reached are prohibited (Paragraph 38).
- Reverse zero-rating (‘premium pricing’), where certain categories of data carry a *higher price*, are likely to be prohibited (Paragraph 45).
- The lower the data cap, the stronger the influence of zero-rating on user choice is likely to be (Paragraph 45).
- Zero-rating is distinguished from generic application bundling, which is *prima facie* permitted (i.e. access to a premium service, with equal treatment and rating of all traffic used: for example, ISP subscriptions include a free Spotify premium account). (Paragraph 33).

- In addition, the Guidelines clarify that not all factors that limit end-users choice should necessarily be deemed to limit end-user rights under Article 3(1). Instead, restrictions would need to result in the end-users' choice being materially reduced for them to be considered a contravention of the end-users' rights (Paragraph 42)

Analysis

Provisions on commercial practices

The lack of a clear prohibition on zero-rating is a missed opportunity. The Guidelines should prohibit all harmful forms of differential pricing (including zero-rating), as the Indian and the Dutch net neutrality laws have done. Thus, the Guidelines should prohibit all forms of application-specific differential pricing (i.e. ISPs charging different prices for traffic from certain applications in a class than for others in the same class, or charging different prices for traffic from different classes of applications), and zero-rating for a fee, where CAPs can pay to have their content zero-rated. These forms of zero-rating and differential pricing enable ISPs to restrict user choice and distort competition between CAPs, thus violating the net neutrality principle, the goal of this Regulation and the rights of end-users under Article 3(1).

We welcome the clear ban in Paragraph 38 on technical discrimination in conjunction with zero-rating offers, most notably blocking or slowing down of non zero-rated traffic once the data limit is reached.

We welcome the degree of detail, which the current Guidelines display on the issue of zero-rating. They include many important factors, which, in the context of a case-by-case approach, are crucial. In particular, we welcome the inclusion of:

- A categorical prohibition of zero-rating schemes where non-zero-rated traffic is blocked or throttled after the data cap is reached (Paragraph 38).
- The distinction between, and inclusion of, the rights of consumers & businesses as end-users on the one hand, and the rights of CAP as end-users on the other (Paragraph 43).
- The acknowledgement of administrative barriers as a restriction of CAP rights (Paragraph 43).
- The inclusion of freedom of expression, media pluralism and 'the continued functioning of the internet ecosystem as an engine of innovation' (Paragraph 43).
- The greater scrutiny of zero-rating for individual applications (Paragraph 45).
- The greater scrutiny of zero-rating applied by ISPs *and* CAPs with dominant market positions (Paragraph 43).

Although the Guidelines list sensitive criteria to assess zero-rating offers, the criteria are incomplete: they lack criteria that cover the detrimental effect of zero-rating for a fee. This type of zero-rating is particularly harmful because it enables a two-sided market that always favors incumbent CAPs and ISPs, increases the costs of market entry and stifles innovation.

By leaving the assessment of the legality of most forms of zero-rating to case-by-case determinations, the Guidelines ultimately fail to deliver a safeguard or predictability regarding the legality of any given zero-rating offer. This problem will be amplified when 31 enforcement agencies (28 EU countries, Iceland, Norway and Lichtenstein) adopt varying regulatory assessments. This will lead to a fragmentation of the digital single market.

In addition, the Guidelines' case-by-case approach has the following disadvantages:

- The multitude of norms and factors will create lasting legal uncertainty, for both CAPs and ISPs.
- Without bright-line rules, the costs of regulatory action will increase, and lengthy case-by-case reviews will lack an exemplary or normative effect
- The case-by-case approach will require extensive monitoring and will result in complex, costly and time-consuming litigation.
- The unpredictability of the legality of commercial practices will reduce the ability of startups to attract investment and hence stifle innovation.

Furthermore, to fulfil the goal of this Regulation to “*guarantee the continued functioning of the internet ecosystem as an engine of innovation*”, NRAs have to ensure clarity and predictability of the underlying conditions of that internet ecosystem and the legality of business models that affect the level playing field for end-users in the digital single market.

Moreover, BEREC's mandate pursuant to Article 5(3) is to contribute to the “consistent application of this Regulation”. A strictly case-by-case approach falls short of this goal, since the legality of each zero-rating offer will have to be assessed individually by 31 enforcement agencies. This legal uncertainty discourages long-term planning and innovation, and is therefore detrimental to investment in the European startup economy.

To ensure legal certainty and predictability for the single market, BEREC should tighten its reading of Recital 7, in accordance with Article 3(2), to clearly forbid all forms commercial practices that restrict end-user choice. For example, the Guidelines could greatly contribute to the protection of end-user

rights *and legal certainty* by clarifying that zero-rating of only some applications in a class and zero-rating for a fee (i.e. where application providers pay to have their data zero-rated) are prohibited.

Article 5(1) gives the national regulators the right to enforce Article 3. Article 3(2) restricts commercial practices that limit end-user rights of Article 3(1). The ability of a CAP to provide a service on the internet and the freedom of users to use an online service are restricted by application-specific differential pricing and zero-rating for a fee (see definitions above). Therefore regulators have the duty and the right to prohibit practices which limit the rights of end-users.

In Paragraph 39 and 40, the current Guidelines would curtail the strong mandate of Article 3 and equate the word “limit” from Article 3(2) with the terms from Recital 7 “end-users’ choice is materially reduced in practice” and “undermine the essence of the end-users’ rights”. However, Recital 7 does not restrict the mandate for regulatory intervention in that way. It only provides a minimum requirement when NRAs “should be empowered to intervene” and “should be required [...] to intervene”. Moreover, Recital 7 states that commercial practices “should not limit the exercise of those rights [of end-users]” and we argue that the language of the Recital calls for categorical prohibitions of harmful *types* of commercial practices, instead of singular cases in a case-by-case assessment.

Application Bundling

The Guidelines correctly distinguish zero-rating from application bundling (Paragraph 33) and we agree with BEREC that it is not prohibited under the Regulation. However, Paragraph 33 goes further by claiming that ‘An ISP may bundle the provision of the IAS with an application. For instance, a mobile operator may offer free access to a music streaming application for a period of time to all new subscribers (as opposed to zero-rating, which is explained in paragraphs 37-40). Lacking further qualification, this statement goes too far, since application bundling can also have implications in other areas of EU law including competition law, freedom of expression and media pluralism.

Traffic Management

Key articles in the Regulation: 3(3) + recitals 8-15

Key paragraphs in the Guidelines: 46-94

Summary of the Guidelines

The Regulation distinguishes between 'reasonable' traffic management measures, which are permitted to be applied on a daily basis, and measures going beyond that which may only be applied under specific circumstances.

Reasonable traffic management

Paragraph 58 of the Guidelines sets up the conditions for the assessment of the Article 3(2) traffic management measures.

Firstly, there has to be a legitimate aim for this measure, as specified in the first sentence of Recital 9, namely contributing to an efficient use of network resources and to an optimisation of overall transmission quality. Furthermore:

- The traffic management measure has to be suitable to achieve the aim (with a requirement of evidence to show it will have that effect, and that it is not manifestly inappropriate);
- The traffic management measure has to be necessary to achieve the aim;
- There is not a less intrusive and equally effective alternative way of achieving this aim (e.g. equal treatment without categories of traffic) with the available network resources;
- The traffic management measure has to be appropriate, e.g. to balance the competing requirements of different traffic categories or competing interests of different CAPs.

In line with the above, Paragraph 63 states that differentiation of categories of traffic can be done on the basis of application layer protocol or generic application type, and may occur only in so far as (Paragraph 63):

- The category is linked to objectively different QoS requirements.
- Applications with equivalent QoS requirements are handled agnostically in the same traffic category.
- Justifications are specific to the objectives that are pursued by implementing traffic management measures based on different categories of traffic.

The Guidelines also note that these measures should only be applied as long as necessary: "*where traffic management measures are permanent or recurring, their necessity might be questionable and*

NRAs should, in such scenarios, consider whether the traffic management measures can still be qualified as reasonable within the meaning of Article 3(3) second subparagraph” (Paragraph 70).

Regarding Deep Packet Inspection, the Guidelines note that only monitoring of the IP packet header and transport layer protocol header is permitted (Paragraph 66).

The Guidelines also address encrypted traffic: *‘the mere fact that network traffic is encrypted, should not be deemed by NRAs to be an objective justification for different treatment by ISPs’*. (Paragraph 57) and *‘Encrypted traffic should not be treated less favourably by reason of its encryption’* (Paragraph 61).

Measures going beyond reasonable traffic management

Article 3(3) of the Regulation permits ISP intervention going beyond ‘reasonable’ measures under three conditions, which can be summarised as: (a) compliance with legal obligations, (b) preservation of network integrity and security, and (c) mitigation of the effects of exceptional or temporary congestion and prevention of impending network congestion. This analysis focuses on ground (c), as it carries the greatest risk of abuse as regards net neutrality.

The Guidelines note that these exceptional measures require a strict interpretation and are not used to circumvent the general rules on blocking, throttling and discrimination (Paragraph 86). More concretely, they lay out the following requirements:

- **Necessity and proportionality:** congestion can be dealt with under 3(3)(c) when application-agnostic congestion management is not sufficient. Similarly, throttling of traffic is preferred over blocking of traffic (paragraphs 87 & 88).
- In line with the above, equivalent categories of traffic must be treated equally, meaning that anti-congestion measures cannot target individual applications (Paragraph 87).
- 3(3)(c) measures must be localised. Any throttling action should be limited to the section of the network where congestion occurs, if possible (Paragraph 87).
- 3(3)(c) measures must be temporary. This provision may not be used to treat ‘recurrent and more long-lasting network congestion’. 3(3)(c) measures cannot function as a ‘substitute for more structural solutions such as expansion of network capacity’ (Paragraph 89).

Analysis

Proportionality of traffic management measures

On traffic management, the Guidelines rightly emphasise the precedence of application-agnostic traffic management practices under Article 3(3) over application-specific traffic management practices. However, BEREC is only putting this emphasis on the more exceptional forms of traffic management. More so, the reasonable types of traffic management are based on narrow categories although the legislator intended them to be defined on broad quality of service categories.

The Regulation gives precedence to application-agnostic network management practices over application-specific network management practices, both in Article 3(3), subparagraph 2 and subparagraph 3. While paragraphs 87 and 88 of the guidelines explicitly state this for Article 3(3), subparagraph 3, the Guidelines are less explicit on Paragraph 63 with respect to Article 3(3), subparagraph 2. This needs to be clarified.

Article 3(3), subparagraph 3 makes clear that measures that differentiate among applications or classes of applications (i.e. application-specific measures) go beyond those described in subparagraph 2 and do not constitute reasonable network management. Thus, as a general rule, Article 3(3), subparagraph 3 requires that any traffic management under Article 3(3), subparagraph 2 needs to be application-agnostic. Paragraph 71 of the Guidelines recognizes this when it states, quoting Article 3(3), subparagraph 3, that “*under Article 3(3) second subparagraph, inter alia the following traffic management measures are prohibited: [...] discrimination between specific content, applications or services, or specific categories thereof.*”

However, this rule - that application-agnostic traffic management has precedence - also applies to traffic management measures under Article 3(3) subparagraph 2 differentiating among classes of traffic based on objectively different quality of service requirements of the traffic. According to the Regulation, such measures can only be used if the problem at hand cannot be addressed by application-agnostic traffic management measures.

Traffic management measures that differentiate among classes of traffic based on objective technical requirements entail many risks for users and CAPs. They allow ISPs to distort competition by offering priority to some classes of applications but not others; they risk harming CAPs by unintended misclassification of applications; they always risk discriminating against encrypted or anonymised traffic; they also make it harder for small businesses, start-ups, and entrepreneurs to get the class of service they need; these traffic management measures are less transparent and create uncertainty

about the performance of particular applications in any particular network; this also makes enforcement more time-consuming and costly; and, finally, they can undermine the right of individual users to utilise the capacity of their IAS based on their own QoS requirements (user-controlled).

Furthermore, a range of application agnostic measures has proven their efficiency in practice.

Under very limited circumstances, Article 3(3), subparagraph 2 allows ISPs to adopt measures that differentiate among categories of traffic based on “objectively different technical quality of service requirements of specific categories of traffic,” but only if:

- this is necessary to improve the overall quality and user experience – but often, class-based traffic management will harm the user experience, so this requirement will not normally be met;
- this goal cannot be met in an application-agnostic way – but at least in fixed networks, application-agnostic traffic management measures (including user-controlled quality of service) will be able to achieve the same goal, but in a way that is less harmful to innovation and user choice; and
- the measures are not maintained longer than necessary.

In a nutshell, Article 3(3), subparagraphs 2 and 3 establish a three-level hierarchy from less to more intrusive traffic management practices that always have to be considered from the perspective of proportionality.

According to Article 3(3), subparagraph 2 and Recital 9, reasonable traffic management must be proportionate. Article 3(3), subparagraph 3 establishes the same requirement.

As recitals 1 and 3 make clear, the goal of the Regulation is to “protect end-users and the continued functioning of the internet ecosystem as an engine of innovation.” The principle of proportionality needs to be applied in light of these goals. In practice, this means that a measure is not proportionate if there is an alternative measure that is less burdensome for users and innovation in content, applications and services. BEREC correctly follows this interpretation in Paragraph 87 and 88 of the Guidelines when interpreting Article 3(3), subparagraph 3, but does not explicitly state the same principle for Article 3(3), subparagraph 2. This is even more surprising since BEREC has interpreted the requirement for traffic management to be proportionate to indicate a preference for application-agnostic traffic management in its 2011 Guidelines on Network Neutrality and Quality of Service: “It [i.e. the traffic management practice] should also be *proportionate*, leading to as few side effects as possible. For example, if it is possible to manage congestion by throttling traffic, then it is less

proportionate to block it, and if it is possible to use application-agnostic methods, then it is less proportionate to use application-specific methods.” (page 52 of the 2011 Guidelines)

The explanation of the term “proportionate” in Paragraph 58 points in a similar direction: Application-specific network management is not proportionate if application-agnostic measures are available, because:

- If application-agnostic measures are available, class-based traffic management is not “necessary” (paragraph 58 of the Guidelines)
- Class-based traffic management creates many harmful conditions for competition, users, and CAPs, so they will not be “appropriate” (as defined in Paragraph 58 of the Guidelines) if an application-agnostic measure is available.

Thus, using traffic management measures that differentiate between objectively different categories of traffic to optimise the overall transmission quality and user experience is neither proportionate nor necessary (Recital 9: “Such measures should not be maintained for longer than necessary.”), if it is possible to reach these goals in an application-agnostic way (including responding to user-controlled QoS information provided by the end-user in accordance with Paragraph 61), and the Guidelines should say so explicitly. In any case, the limitation that such measures may not be maintained for longer than necessary makes the legislator’s intention clear – namely that they may not be an integral part of network design.

Finally, Recital 9 only seems to allow traffic management measures that differentiate among objectively different classes of traffic if these measures are used to “optimize overall quality and user experience” (and if they are necessary and proportionate to reach that goal.) The various negative consequences of such measures for users, described above, suggest that such measures will often fail to meet that goal.

Differences in class-based traffic management

The Guidelines suggest in Paragraph 63 that under Article 3(3), subparagraph 2, ISPs could define classes based on application-type or even based on application-layer protocol. Categories only have to be “linked” to categories based on QoS requirements. That interpretation is contrary to the text of Article 3(3), subparagraph 2, which requires classes to be defined based “*on objectively different technical quality of service requirements of specific categories of traffic*”, NOT based on application-type.

On the one hand, Paragraph 63 states that ISPs may differentiate categories of traffic based on application layer protocol or generic application types. However, Recital 9 of the Regulation deals with traffic management in cases in the absence of congestion and states that “differentiation should [...] be permitted only on the basis of objectively different technical quality of service requirements (for example, in terms of latency, jitter, packet loss, and bandwidth)”.

Defining classes based on application-layer protocols will often exclude applications with similar technical requirements. For example, different video applications may use different transport-layer and application-layer protocols, but have the same technical requirements. Innovation in application layer protocols (HLS, MPEG-DASH) are less likely when these advancements risk misclassification of the application.

Similarly, defining classes based on application-type makes it easier for ISPs to distort competition among classes of applications (e.g., by providing low-delay only to some delay-sensitive applications). Defining classes by reference to technical characteristics makes it clear that any application with these or similar characteristics belongs to the class.

Therefore, BEREC should clarify that classes should not be defined so narrowly as to facilitate the differentiation among classes as a vehicle to discriminate among different types of applications.

We would conclude that Paragraph 63 is out of line with the definition of ‘reasonable traffic management’ as defined in the second subparagraph of Article 3(3). As a result, it is overly permissive of non-agnostic traffic management which discriminates on the basis of categories of applications.

The correct interpretation (based on Recital 9, the interpretation in Paragraph 71 and most importantly the intended difference in terminology of the legislator in the second and third subparagraphs of Article 3(3)) should emphasise that reasonable traffic management must differentiate at a ‘higher level’ than application-type (protocol, functionality). It should not focus on *categories of applications*, but focus instead on *categories of objective QoS-requirements* such sensitivity to delay, jitter, loss and latency.

The added workload on NRAs to regulate cases of class-based traffic management disputes is another reason to simplify the Guidelines, in order to maintain a manageable workload for NRAs.

General Remarks

We recommend BEREC to add to the Guidelines on traffic management a definition of the term application-agnostic (i.e. criteria not based on specific applications, on categories of applications or on criteria that depend on an application's characteristics) in order to ensure a unified understanding of the concept including examples of the various forms this type of traffic management entails (e.g. consumption-based, user-controlled, etc.).

Paragraph 85 of the Guidelines is crucial to prevent overreaching application of measures for the mitigation of "impending network congestion". These cases have to be limited to exceptional, temporary cases of imminent congestion.

Paragraph 79-83 provides a balanced and practical approach to treating security incidents pursuant to Article 3(3)(b). However, Paragraph 81 is not in line with the Regulation. It allows ISPs to apply pro-active security measures while the Regulation clearly only allows re-active measures in Article 3(3) subparagraph 3 "only for as long as necessary". Specifically, the continuous pro-active security monitoring allowed by Paragraph 81 will involve processing of personal data to a greater extent than allowed by Article 3(4). Similarly, the concept of "blocking lists from recognised security organisations" (Paragraph 82) requires further definition. It is important that these organisations are independent, unbiased, and reliable, and that their lists provide objective, verifiable information. If such quality safeguards are not included, Paragraph 82 could enable arbitrary or abusive censorship by unaccountable private entities and thus restrictions of the freedom of speech and the freedom of information without legal basis. As recognised in Recital 33, any interpretation of the Regulation must be in line with primary EU law, particularly, in this case, Article 52(1) of the Charter.

Specialised Services

Key articles in the Regulation: 3(5) + recitals 16-19

Key paragraphs in the Guidelines: 84-123

Summary of the Guidelines

ISP and CAPs are permitted to offer services other than IAS where the optimisation they offer is necessary to offer a specific QoS required for the content application or service. NRAs are required to verify the extent to which this optimisation is objectively necessary for the features of these applications. This function should enable a corresponding QoS assurance to be given to the end-users as opposed to granting "*general priority over comparable content, applications or services available*

via the internet access service and thereby circumventing the provisions regarding traffic management measures applicable to the internet access services”.

The defining features of specialised services are that they are services other than IAS and that the optimisation is objectively necessary to meet the required QoS for those services. Key conditions set out for the provision of such services are that the network capacity is sufficient to provide the specialised service in addition to any IAS provided. These services must not be usable as replacements for IAS and must not be detrimental to the availability or general quality of the IAS for the end-user.

According to recital 16, the service shall not be used to circumvent the provisions regarding traffic management measures applicable to IAS.

In their assessment of compliance of specialised services with Article 3(5), the NRAs should apply the approach set out in articles 104-111. It can be summarised as follows:

- 104: Providers of specialised services must be able to specify the Quality of Service (QoS) requirements of their service, as well as contractual requirements and the “specific level of quality” which the service provides. It should be demonstrated that this specific level of quality cannot be assured over the IAS.
- 106: The specialised service must be offered through a connection that is logically separate from the IAS. The ‘specific level of quality’ cannot be provided by simply granting general priority over comparable content.
- 107: Optimised delivery must be objectively necessary to ensure one or more specific and key features of the applications, and to enable a corresponding quality assurance to be given to end-users. The NRA should assess whether the service in question requires a level of quality that cannot be assured over an IAS.
- 108: The status of specialised services is temporary and must be re-assessed over time, to see if the requirements of the application in question can also be assured by improving general standards of IASs (so that the application does not meet the conditions for being a specialised service any more).
- 111: Business customers often request services relating to virtual private networks (‘VPN’). The term VPN can be used in relation to two different types of services:
 - “VPN Applications”: typically used in the context of teleworking. In this case, business traffic is typically encrypted and uses IAS on both ends. This would therefore not be a specialised service.

- “VPN Network service”: In this case, a VPN network is typically used to provide a private connection between a number of sites typically implemented in parallel through common infrastructure with IAS. These are considered specialised services (as long as they comply with the requirements of the Regulation).

Analysis

Reclassification of online services as specialised services

The Guidelines clarify what qualifies as a specialised service and which requirements have to be met for the provisioning of such a service. BEREC makes clear that the goal of such services cannot be to circumvent the non-discrimination provisions of the Regulation. The regulators have to deliver a solid differentiation of the two types of access services, namely concrete examples of legitimate specialised services and the creation of meaningful bright-line rules that allow for innovation while protecting the open internet. Otherwise, the Regulation’s ban on selling preferential treatment to CAPs for a fee would become meaningless.

The current version of the Guidelines falls short of this goal.

The text of Article 3(5) is clear: to qualify as a specialised service under the Regulation, the service needs to be optimized for specific content, applications, or service, “where the optimisation is necessary in order to meet the requirements of the content, application or service for a specific Quality of Service”. Recital 16 clarifies that the NRA has to verify whether such optimisation is “objectively necessary”.

When an application can function over the open internet, it does not require the quality optimisation which characterises specialised services. The Guidelines should therefore include the following definition as a “bright-line” rule: If an application can objectively function on the normal internet, then the optimisation is not “necessary to meet the requirements of the application for a specific level of quality.” This definition ensures that ISPs cannot use the provision of specialised service to offer preferential treatment to normal internet applications for a fee. If the category of the application could function on the normal internet, for example by using adaptive video bitrate and buffering video instead of constant video bitrate for ultra high-definition video, the optimisation is not objectively necessary for “key features” of that application (Recital 16) and the same principle has to apply.

The Guidelines contradict the Regulation on this point. Paragraph 102 suggests that the provider of the specialised service (the CAP or the ISP) can define the quality requirements. Paragraph 104 can be read in a way that the contractual assurances of a certain quality can make the optimisation “necessary”. In both cases, this would give ISPs or CAPs the power to circumvent the Regulation’s ban on offering better treatment to internet applications for a fee by unilaterally defining quality requirements that are higher than what the normal internet can offer. This directly contradicts the Regulation’s focus on whether the optimisation is “objectively necessary” to meet an application’s requirements. Both of these readings are not in line with Article 3(5) and Recital 16. Recital 16 only allows “corresponding quality assurances to be given to the end-user” after the objective assessment of the application’s requirements for a specific quality of service by the NRA, because the two criteria are linked with “and” and not with “or”.

The focus on the current development state of the internet access market in Paragraph 108 creates an incentive for ISPs to offer stagnating IAS quality and provision less network capacity, because new services which require a higher quality of service could be exclusively offered as lucrative specialised services. This perverse incentive, as well as the strong emphasis on a case-by-case rule in Paragraph 108, are another argument to tighten the “necessity” requirements of Article 3(5) with a strong definition that excludes all services which could function over the open internet.

We acknowledge that BEREC has laid a solid foundation for the implementation of Article 3(5) in Paragraph 101, 106 and 107. However, we stress the necessity to unmistakably clarify the nature and relationship of services in IAS and specialised services by adding a clear definition that covers the meaning of Article 3(5). Otherwise, the damage done by misclassified services could seriously harm the goals of this Regulation in an irreparable way.

Quality deteriorations of the internet access service

Regrettably, there is another major point at which the Guidelines contradict both themselves and the Regulation. In Paragraph 118, instead of requiring additional capacity to be provided over which specialised services can be run, the Guidelines suggest an incomprehensible regime of allowing specialised services to cannibalise capacity from the IAS of the subscriber. According to the Guidelines, this double-selling of capacity is only limited by the minimum quality assured in the contract of the subscriber.

If the quality of the IAS is reduced by the provisioning of a SpS up to the point where only the absolute minimum remains, then the requirement of Article 3(5) to uphold the “general quality of the IAS for

the end-user” is no longer met. Paragraph 118 of the Guidelines is not in line with Article 3(5) of the Regulation. This argument is amplified by the legislative history of this Article 3(5). In the final triologue negotiations of 6 July 2015, the legislator decided to delete the word “other” from this provision, amending it as follows: “and shall not be to the detriment of the availability or general quality of internet access services for other end-users.” This amendment shows that the requirement to uphold the general quality of the IAS is also intended to apply to the end-user receiving the SpS in question.

We recognise that there may be special situations where extra network capacity for the specialised service cannot technically be provided, such as xDSL connections where the total bandwidth of the connection is limited by the distance to the telephone exchange, and where a detrimental effect to the IAS of the end-user may be unavoidable if specialised services such as linear IPTV are to be offered. However, Paragraph 118 is not limited to situations where cannibalising the bandwidth of the IAS for the specialised service is unavoidable for purely technological reasons. Paragraph 118 should at the very least make it clear that specialised services cannot be used for double-selling of the network capacity offered to the end-user, except in narrowly defined situations where no alternative exists due to the technical deficiencies of the network technology used for the IAS.

BEREC is overstepping its mandate, since Paragraph 118 contradicts an article which was intentionally changed by the legislator to express the opposite meaning of what Paragraph 118 currently says.

Paragraph 118 is not following the stated logic of the Guidelines in paragraphs 113 and 117, which makes the provision of SpS dependent on sufficient network capacity to provide them in addition to any IAS and states that it cannot be do the detriment of the availability and general quality of the IAS.

Paragraph 118 also contradicts Article 4 of the Regulation, on transparency. When the SpS reduces the IAS quality up to the point where only the minimum bandwidth is available, this contradict the obligation to provide the average bandwidth at least during off-peak hours and 90% of time over peak hours, or 95% over the whole day (Paragraph 145). As a result, the definition of normally available and maximum speed in Article 4(1)(d), including their implementation in paragraphs 142 and 144, are no longer met and the internet access product does no longer fulfill the requirements of the contract or the Regulation.

Furthermore, the minimal speed is not a requirement for the specification of mobile internet access service and therefore specialised services could completely cannibalize mobile internet access

services. We also want to highlight that the decision of BEREC to choose the minimum speed, instead of the normally available speed in Paragraph 118 is unintelligible from our perspective and not following the intention of the legislator in the Regulation.

Transparency

Summary of the Guidelines

Key articles: Article 4(1), Recital 18

Key paragraphs in the Guidelines: 124-163

Providers of internet access services shall ensure that any contract which includes internet access services specifies at least the following:

- a. information on how traffic management measures applied by the ISP may impact on the quality of the IAS and on the privacy of end-users' data;
- b. a clear and comprehensible explanation as to how any volume limitation, speed and other quality of service parameters may in practice have an impact on internet access services, and in particular on the use of content, applications and services;
- c. a clear and comprehensible explanation of how any services referred to in Article 3(5) to which the end-user subscribes might in practice have an impact on the internet access services provided to that end-user;
- d. a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services in the case of fixed networks, or of the estimated maximum and advertised download and upload speed of the internet access services in the case of mobile networks, and how significant deviations from the respective advertised download and upload speeds could impact the exercise of the end-users' rights laid down in Article 3(1);
- e. a clear and comprehensible explanation of the remedies available to the consumer in accordance with national law in the event of any continuous or regularly recurring discrepancy between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated in accordance with points (a) to (d).

The section addresses the need for clearly stating the conditions under which the IAS is contracted to the end-user as a means of ensuring the protection of their personal rights as well as clear statement as to the simply shows what the quality of the service they may expect under the contract.

The provisions on safeguarding of the open internet should be complemented by effective end-user provisions which address issues particularly linked to IAS. These provision should apply in addition to provisions set out in the Directive 2002/22/EC of the European Parliament and of the Council and Member States regarding the safeguarding of the open internet by enabling end-users to make informed choices.

NRAs should ensure that ISPs adhere to certain good practices regarding the information:

- should be easily accessible and identifiable for what it is;
- should be accurate and up to date;
- should be meaningful to end-users, i.e. relevant, unambiguous and presented in a useful manner;
- should not create an incorrect perception of the service provided to the end-user;
- should be comparable at least between different offers, but preferably also between different ISPs, so that end-users are able to compare the offers (including the contractual terms used by different ISPs) and ISPs in such a way that it can show differences and similarities.

Minimum speed: The lowest speed an ISP should undertake to deliver to end-user except in the exceptional circumstances of interruptions to the service of the ISP

Maximum speed: This speed should be achieved at least once a day

Normally available speed: This is the speed that end-users can expect to receive over specified times of the day, as specified under Article 5(1). An example is that speed should be available over of non-peak hours and 90% over peak hours or 95% of the whole day

Advertised speed (148): Advertised speed is the speed an ISP uses in its commercial communications, including advertising and marketing, in connection with the promotion of IAS offers. In the event that speeds are included in an ISP's marketing of an offer (see also Paragraph 139), the advertised speed should be specified in the published information and in the contract for each IAS offer.

Analysis

We welcome the transparency rules as a clear and proportionate implementation of the Regulation. We recommend that BEREC clarify in Paragraph 124 that the information provided by the ISP according to Article 4(1) has to be published on the website of the ISP.

In order to allow for informed consumer choice, we would recommend BEREC to require with regard to Paragraph 131 that the ISP informs the user about the definitions used to classify congestion as impending, exceptional or temporary (similar to Paragraph 180).

Furthermore, we would welcome BEREC strengthening its very meaningful recommendation to the NRAs in Paragraph 145 to define the normally available speed the same way BEREC did, by replacing “could” with “should”.

Supervision and Enforcement

Key articles of the Regulation: 5

Key paragraphs in the Guidelines: 164-182

Summary of the Guidelines

This chapter outlines the various powers and competences which NRAs have in order to enforce the Regulation. It sets out a general approach which includes (I) supervision, (II) enforcement, and (III) reporting.

The NRA powers include

- requesting information from ISPs (paragraphs 166-167 and 181)
- conducting technical traffic management research (Paragraph 168)
- Monitoring IAS performance (user-level and market-level assessments (paragraphs 171-172)
- Monitoring transparency requirements (Paragraph 174)
- Setting requirements and imposing orders and prohibitions regarding QoS and non-discrimination of IAS (paragraphs 175-178)

NRAs are also required to submit annual reports to BEREC (paragraphs 179-180).

Sanctions for violation of the Regulation are defined by national law and therefore fall outside the scope of the BEREC Guidelines.

Analysis

We welcome the clear rules on supervision and enforcement set out by BEREC in the Guidelines. They should provide sufficient means for competent and well-intending NRAs to enforce the Regulation.

However, almost all of this section is phrased in terms of powers/competences/discretions for NRAs, rather than duties/responsibilities/obligations. In light of the funding and capacity situations under which some NRAs have to fulfill their duties, a clear mandate which also requires the NRA to act within a certain timeframe would ensure a higher and more equal level of enforcement throughout the digital single market.

Particularly, in light of the newly created requirement of ISPs to deliver their contractually agreed minimum, average and maximum speeds, the upcoming reform of the telecoms package needs to include more robust powers for NRAs to enforce these requirements and properly monitor developments in the quality of IAS.